Standard 7: Facilities and Equipment

Adequate facilities and equipment must be available for the teaching and learning requirements of the program. Use of facilities and equipment should be monitored and regular assessments of adequacy made through consultations with faculty, staff and students.

The scales below ask you to indicate whether these practices are followed in your institution and to show how well this is done. Wherever possible evaluations should be based on valid evidence and interpretations supported by independent opinions

Good Practices Relating to This Standard	**Is this true? Y/No/NA**	**How well is this done? (enter stars)**
7.1 Policy and Planning Planning processes for the provision of facilities and the acquisition and maintenance of equipment must include consultation with program representatives to ensure clear specification of program requirements. Plans for provision must appropriately balance program requirements with institutional policies to ensure compatibility of systems and resources available.		
7.1.1 Equipment acquisitions meet program requirements and are also consistent with institutional policies to achieve compatibility of equipment and software systems across the institution. Coordinate w/ Dr. Des		
7.1.2 Teaching staff are consulted before major equipment acquisitions to ensure that current and anticipated emerging needs are met. Coordinate w/Antonio & Dr. Des		
7.1.3 Equipment planning provides for acquisition, servicing and replacement according to a planned schedule. Coordinate w/Antonio		
Overall Assessment		
Comment _____ _____		
Priorities for Improvement _____ _____		
Independent Opinion ***Comment*** **7.1 Policies are in place for acquisition and maintenance of equipment needed by PMU programs.**		

7.2 Quality and Adequacy of Facilities and Equipment
Facilities and equipment must be of good quality with effective strategies used to evaluate their adequacy for the program, their quality and the services associated with them.

7.2 1 Facilities meet health and safety requirements and make adequate provision for the personal security of faculty, staff and students.
7.2.2 Quality assessment processes include both feedback from principal users about the adequacy and quality of facilities, and mechanisms for considering and responding to their views.
7.2.3 Standards of provision of teaching, laboratory and research facilities are adequate for the needs of the program and benchmarked through comparisons with other comparable institutions. (This includes such things as classroom space, laboratory facilities and equipment, access to computing facilities and associated software, private study facilities, and research equipment.
7.2.4 Adequate facilities are available for confidential consultations between faculty and students)
7.2.5 Provision is made for students, faculty and staff with physical disabilities or other special needs. Coordinate with Dr. Des & Antonio

Overall Assessment

Comment

_____

_____

Priorities for improvement

_____

_____

Independent Opinion
Comment
7.2 The evidence is that most equipment meets needed quality standards.

~~**7.3 Management and Administration**~~
~~Management and administration of facilities, equipment and associated services must be efficient and ensure maximum effective utilization of facilities provided.~~

~~7.3.1 A complete inventory is maintained of equipment used in the program that is owned or controlled by the institution including equipment assigned to individual faculty or staff for teaching and research.~~
~~7.3.2 Services such as cleaning, waste disposal, minor maintenance, safety, and environmental management are efficiently and effectively~~

~~carried out.~~

~~7.3.3 Provision is made for regular condition assessments, preventative and corrective maintenance, and replacement.~~

~~7.3.4 Effective security is provided for specialized facilities and equipment for teaching and research, with responsibility between individual faculty, departments or colleges, or central administration clearly defined.~~

~~7.3.5 Effective systems are in place to ensure the personal security of faculty, staff and students, with appropriate provisions for the security of their personal property.~~

~~7.3.6 Arrangements are made for shared use of underutilized facilities with adequate mechanisms for security of equipment.~~

Overall Assessment

Comment

_____

_____

Priorities for improvement

_____

_____

Independent Opinion

Comment

7.3 The management of installed facilities is mostly in the hands of the programs. Utilization of certain services and facilities not in the programs is sometimes burdened by delays in acquisition and commissioning.

7.4 Information Technology

Computing equipment and software and related support services must be adequate for the program and managed in ways that ensure secure, efficient and effective utilization.

7.4.1 Computing equipment is available and accessible for faculty, staff and students and the adequacy of this provision is regularly assessed. Link to Weekly ITD Classroom and Labs Report (Print all links request for purchase and all reminder letters for Purchasing). Deployment of Banner Electronic purchasing module will enable us to move from 4 to 5.	Y	4
7.4.2 Institutional policies governing the use of personal computers by students are complied with.	Y	5
7.4.3 Technical support is available for teaching staff and students using information and communications technology. University Help Desk system used to track and trace support request to successful resolution. Aging reports are required to move service level from 3 to 4. **Action Plan 1** (See Appendix A) Summary: Evaluate cost effective commercial	Y	3

package solution for service desk software, point person is Abdulaziz. Recommendation to Eng. Yamani through CIO due by January 31, 2012.

7.4.4 Opportunities are available for teaching staff input into plans for acquisition and replacement of IT equipment for use in the program. **Action Plan 2** (See Appendix B) Summary: Part 1 is a faculty orientation program completed. Link to presentation on faculty orientation; Part 2 conduct faculty survey. Link to survey instrument; Part 3 is work with Learning Resource Center to establish faculty forum for education equipment and software suggestions, input, discussion. CIO to coordinate with Director of LRC and College Deans not later than March 31, 2012. CIO and Team Lead of MIS to finalize faculty satisfaction survey not later than October 26, 2011.

Y | 2

7.4.5 Security systems are in place to protect privacy of personal and sensitive personal and institutional information, and to protect against externally introduced viruses. Based upon 20 years in IT Services, current CIO believes the level of security at PMU is higher than any institution he has ever worked for and it suitable for financial institution such as Bank.

Y | 5

7.4.6 Compliance with a code of conduct relating to inappropriate use of material on the internet is checked and instances of inappropriate behavior dealt with appropriately. Security system proactively monitors abuse of systems, log attempts to compromise security, and proactively disable access to system when abuse detected.

N/A |

7.4.7 Training programs are available for faculty and staff to ensure effective use of computing equipment and appropriate software for teaching, student assessment, and administration. IT supports Learning Resource Center by providing subject matter expert trainer who participates in professional development for all employees (faculty and staff). Also IT supports the Student Affairs Division with student orientation and other training required to help students use systems and services. Example of Student Orientation.

Y | 4

Overall Assessment | 3.83

Comment

_____

_____

Priorities for improvement

_____

_____

Independent Opinion

Comment

7.4 The campus including classrooms and teaching laboratories have excellent information technology infrastructure. The campus computer network is being upgraded to accommodate growing

demand.

Overall Assessment of Facilities and Equipment

7.1 Policy and Planning

7.2 Quality of and Adequacy of Facilities

7.3 Management and Administration

7.4 Information Technology

Combined Assessment Independent Opinion:
Comment
Facilities and infrastructure are either excellent or planned to be upgraded to meet program needs.

Independent Opinion

Comment

_____

_____

Indicators Considered

_____

_____

_____

Priorities for Improvement

_____

_____

_____

_____

Appendix A: Action Plan for Commercial Service Desk System

Reference Question: 7.4.3 Technical support is available for teaching staff and students using information and communications technology.

ACTION PLAN FOR CONTINUOUS IMPROVEMENT:

Evaluate cost effective commercial package solution for service desk software, point person is Abdulaziz.

Mr. Abdulaziz to gather functional requirements, survey current market options to meet these requirements, select vendors for Request for Proposals (RFP), create and process RFP through ETA office.

Recommendation to Eng. Yamani through CIO due by January 31, 2012.

Appendix B: IT Governance for Instructional Technologies

Reference Question: 7.4.4 Opportunities are available for teaching staff input into plans for acquisition and replacement of IT equipment for use in the program.

ACTION PLAN FOR CONTINUOUS IMPROVEMENT

Part 1: Faculty Orientation Program (COMPLETED September 2011)

Faculty orientation program completed to include coverage of the follow content areas.

Starting With 20 Minutes on the Basics
Who Do I Call When I Have A Problem?
One Stop Shop: X8888 Is Also the Number You Call for all Engineering and Technical Affairs (Which Includes IT and Facilities and Maintenance)
Demo of Outlook E-Mail, Web Site, Call! (2 Minutes)
Using My Computer from Work
Wired in Your Office (2 Minutes)
Wireless in Common Areas at Campus (2 Minutes)
Using a USB Flash Drive
Getting Access to the Local Network Server (2 Minutes)
Applications on My Computer - Faculty Laptops (2 Minutes)
Accessing the Required Documents through the Intranet (5 Minutes)
Introduction to IPT (10 Minutes)
IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long) -- Continued
10 Minutes: Using My Computer from the Compound
Getting Internet via STC or Mobily (5 Minutes)
Online Banking (5 Minutes)
5 Minutes: Getting and Setting Up My PMU E-Mail Account:
Outlook & Web Mail
My Banner Faculty Self-Service Account: Getting and Setting Up and Submitting Grades!
IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long) -- Continued
20 Minutes: My Banner Faculty Self-Service Account
Introduction to Banner (2 Minutes)
Login In to Faculty Self-Service for the First Time (2 Minutes)
Introduction to Your Self-Service Banner Session and Main Menu (4 Minute)
Introduction to Your Faculty Schedule (6 Minutes)
Detailed Schedule
Week at a Glance
Master Class Schedule
Start With the End in Mind: How to Submit Student Grades at the End of Semester in Banner (6 Minutes)
ITD-Classroom Services 4 PMU Faculties (1 Time for 1 Hr Long)
Two Groups - Male and Female (1 Hr Long)
Traditional 20 Minutes
Smart 20 Minutes
Enhanced 20 Minutes
Traditional Classrooms: 20 Minutes

Instructor Work Station
Projector
Smart Board & Promethean Active Boards (Female)
Smart Classrooms: 20 Minutes
Instructor Podiums
Projectors
Review after the Walk Through:
YouTube Playlist: Smart Classroom Basics at PMU
Google Presentation: Overview of Smart Classrooms at PMU
Enhanced Classrooms: 20 Minutes
Instructor Podiums
Projectors
Video Conferencing
ITD-College Blackboard for Beginners (ITD Will Be Doing 3 Times for 1 Hr)
ITD Will Be Doing Three Level I Sessions:
Getting and Setting Up
Accessing URL
Login
Changing password
Introduction to Syllabus, Hours, Assignments, Presentations
Later Topics Will Include:
Level II: Tracking Assignments & Grade Book
Level III: Assessments & Tests
Level IV: Working With Instructional Multimedia

Part 2: Conduct Faculty Survey.

DRAFT COMPLETED in October 2011 of IT Department Services at PMU Survey Instrument (Multiple Choice and Free From Responses). The following questions will be asked to ascertain satisfaction levels and to provide input for ongoing improvements in services delivered by ITD:

Academic Computer Services

1) I am kept well informed of IT matters important to faculty. [Code: ITD-1-001] Satisfaction Level

2) PMU provides adequate technology equipment and software needed to do my job well [Code: ITD-1-002] Satisfaction Level

3) Technology equipment in classrooms where I typically teach function adequately [Code: ITD -1-003] Satisfaction Level

4) I am satisfied with the response from the ITD when I need help [Code: ITD -1-004] Satisfaction Level

5) The IT system is up and running whenever I need it. [Code: ITD -1-005] Satisfaction Level

6) IT delivers promised services in a timely manner [Code: ITD -1-006] Satisfaction Level

7) IT Services helps you use technology effectively [Code: ITD -1-007] Satisfaction Level

8) The IT services as a whole are valuable to me. [Code: ITD -1-008] Satisfaction Level
Sub-Category [Edit] [Add Question] [Move/Copy Questions] [Archive Questions]

General Support

1) Ability to get through to a person [Code: ITD -2-001] Satisfaction Level

2) Timeliness of initial response to your inquiry [Code: ITD -2-002] Satisfaction Level

3) Ability to solve a problem [Code: ITD -2-003] Satisfaction Level

4) Turnaround time for resolving your problem [Code: ITD -2-004] Satisfaction Level

5) How satisfied are you with problem resolution overall? [Code: ITD -2-005] Satisfaction Level

6) Regarding the Help Desk -- How do you rate the timeliness in getting requests filled? [Code: ITD -2-006] Satisfaction Level

1) How satisfied are you with the SPEED of PMU Webmail? [Code: ITD -3-001] Satisfaction Level
2) How satisfied are you with the FEATURES of PMU Webmail? [Code: ITD -3-002] Satisfaction Level
3) How satisfied are you with the EASE OF USE of PMU Webmail? [Code: ITD -3-003] Satisfaction Level
4) How satisfied are you with the RELIABILITY of PMU Webmail? [Code: ITD -3-004] Satisfaction Level

5) How satisfied are you with the amount of email storage space provided at no charge by PMU? [Code: ITD -3-005] Satisfaction Level

6) How satisfied are you with PMU email overall? [Code: ITD -3-006] Satisfaction Level

Calendaring

1) How satisfied are you with how the calendar performs on your mobile device? [Code: ITD -4-001] Satisfaction Level
2) How satisfied are you with how the calendar performs for importing or combining calendars from different devices?
[Code: ITD -4-002]
Satisfaction Level

3) How satisfied are you with how the PMU calendar performs overall? [Code: ITD -4-003] Satisfaction Level

Mobile Devices

Admin Imports Setup Survey Reports Help Database

1) Which of the following mobile devices do you currently use or intend to use within the next six months for work or study? iPhone? [Code: ITD -5-001]
Usage in next 6 months

2) Use iPad? [Code: ITD -5-002] Usage in next 6 months

3) Use iPod Touch? [Code: ITD -5-003] Usage in next 6 months

4) Use a Blackberry? [Code: ITD -5-004] Usage in next 6 months

5) Use Android device? [Code: ITD -5-005] Usage in next 6 months

6) Use Palm OS device? [Code: ITD -5-006] Usage in next 6 months

7) Use other cell phone with internet access? [Code: ITD -5-007] Usage in next 6 months

8) How important is it to have the following available on your smart phone or other mobile device? Email? [Code: ITD-5-008]Importance Level

9) PMU Directory on Smart Phone? [Code: ITD -5-009] Importance Level

10) Smart Phone -- Class schedules? [Code: ITD -5-010] Importance Level

11) Smart phone - Calendar? [Code: ITD -5-011] Agreement Level

12) How satisfied are you with using the following via your mobile device? Email? [Code: ITD -5-012] Satisfaction Level

13) Mobile device -- calendar? [Code: ITD -5-013] Satisfaction Level

14) Mobile device for public PMU websites and applications? [Code: ITD -5-014] Satisfaction Level

15) Which applications, if any, would you like to be more mobile-friendly at PMU? [Code: ITD -5-015] Long Answer

Telephone Services

1) How satisfied are you with these aspects of PMU telephone services -- Placing an order? [Code: ITD -6-001] Satisfaction Level

2) Order completion and delivery? [Code: ITD -6-002] Satisfaction Level

3) Problem resolution? [Code: ITD -6-003] Satisfaction Level

4) Voicemail? [Code: ITD -6-004] Satisfaction Level

5) How important would the following service and feature improvements be for your PMU work? Ability to schedule calls forwarding of your PMU work number through a web interface? [Code: ITD -6-005] Importance Level

6) Ability to set your office desk and cell telephones to ring simultaneously? [Code: ITD -6-006] Importance Level

7) Ability to set your office desk and cell telephones to ring sequentially? [Code: ITD -6-007] Importance Level

8) Delivery of voicemail messages and faxes to your email? [Code: ITD - 6-008] Importance Level

9) Ability to make or receive calls from your computer (Softphone)? [Code: ITD -6-009] Agreement Level

10) Ability to modify phone features through a web interface? [Code: ITD -6-010] Importance Level

11) How important will the following devices be to your work requirements within the next one to two years? [Code: ITD-6-011]

Importance Level

12) Importance of a WiFi VoIP phone that works only on campus? [Code: ITD -6-012] Importance Level

13) Importance of a cell phone used only for telephone calls? [Code: ITD -6-013] Importance Level

14) Importance of a Smart Phone (eg. iPhone, Blackberry, Android,Windows Mobile Device etc.? [Code: ITD -6-014] Agreement Level

15) Importance of a Tablet Device (eg. Galaxy or iPad)? [Code: ITD -6-015] Importance Level

IT Services Priorities

1) Email [Code: ITD -7-001] Service Providers
2) Email lists/group discussions [Code: ITD -7-002] Service Providers
3) Calendaring (for your own calendar) [Code: ITD -7-003] Service Providers
4) Meeting/event scheduling with others [Code: ITD -7-004] Service Providers
5) Document sharing [Code: ITD -7-005] Service Providers
6) Instant Messaging [Code: ITD -7-006] Service Providers
7) Video storage/sharing [Code: ITD -7-007] Service Providers
8) Image storage/sharing [Code: ITD -7-008] Service Providers
9) Websites, blogs, wikis [Code: ITD -7-009] Service Providers

10) Of the external providers you use, which do you prefer? [Code: ITD -7-010] Service Providers
11) If there were a contract in place with PMU and Google or Microsoft that safeguarded your privacy and intellectual property, which one would you feel most comfortable using? [Code: ITD -7-011]

Service Providers

Remote Access
1) If you use PMU's VPN, SSL or client-based services for remote access, how satisfied are you with your ability to connect to them to get access to such things as your calendar or PMU folder? [Code: ITD -8-001]
Satisfaction Level

Security

1) Anti-virus/anti-spyware software is set to update itself automatically. [Code: ITD -9-001] Likelihood
2) Anti-virus/anti-spyware scanning of your hard disks is turned on [Code: ITD -9-002] Likelihood
3) Operating system updates are installed automatically. [Code: ITD -9-003] Likelihood
4) Application software updates (such as MS Office) are installed when available. [Code: ITD -9-004] Likelihood
5) Passwords changed every six months. [Code: ITD -9-005] Likelihood
6) Password is required to start/wakeup computer. [Code: ITD -9-006] Likelihood
7) Passwords include random combinations of letters and numerals. [Code: ITD -9-007] Likelihood
8) Hand-held devices such as iPhones will require a password. [Code: ITD -9-008] Likelihood
Sub-Category [Edit] [Add Question] [Move/Copy Questions] [Archive Questions]

Final Questions

1) What is one think IT Services could do that would make it easier for you to work or study? [Code: ITD -10-001] Long Answer
2) What are the two or three most important services IT Services provides you? [Code: ITD -10-002] Long Answer
3) What is one thing IT Services could do to improve the way it communicates about its services? [Code: ITD -10-003] Long Answer
4) Any added comments you may have for IT Services [Code: ITD -10-004] Long Answer

Part 3: Work with Learning Resource Center to establish faculty forum for education equipment and software suggestions, input, and discussion.

CIO and Team Lead of MIS to finalize faculty satisfaction survey not later than October 26, 2011.

CIO to coordinate with Director of LRC and College Deans not later than March 31, 2012.

Table of Contents

7. Facilities and Equipment (Overall Rating 3.83 Stars)

Facilities must be designed or adapted to meet the particular requirements for teaching and learning in the programs offered by the institution, and offer a safe and healthy environment for high quality education. Use of facilities must be monitored and user surveys used to assist in planning for improvement. Adequate provision must be made for classrooms and laboratories, use of computer technology and research equipment by faculty and student and appropriate provision made for associated services such as food services, extra curricular activities, and where relevant, student accommodation.

Explanatory note about administration of arrangements for planning, development and maintenance of facilities and equipment. This should include cross references to other more detailed facilities planning documents.

Description of process for investigation and preparation of report on this standard.
ITD Quality Team of of Member drawned from this Department. ITD collaborated closely with representatives of the Deanship of Quality Accreditation throughout the reporting process with particularly emphasis during self evaluation scale star rating and narrative writing processes.

List of Committee Members and meeting minutes are appended to this report.

Copy of QC Minutes IT June 6.docx -
Inst SS Meet Mins - Fac Equip Dr. Dobe+ April 6.docx -
Q C Meeting Minutes FAc Equip May 4.docx -
DQA Meeting Minutes ITD Oct 8, 2011.docx -
DQA Meeting Minutes ITD Oct 5, 2011.docx
DQA Meeting Mins ITD Sept 28, 2011.docx -

Self Evaluation Scales for Higher Education Institutions

National Commission for Academic Accreditation & Assessment

Self Evaluation Scales for Higher Education Programs

February 2010

Self Evaluation Scales for Higher Education Programs

Contents

Self Evaluation Scales for Higher Education Programs

Introduction

These self evaluation scales are intended to provide guidance to program administrators and staff in higher education institutions in their planning, self-review, and quality improvement strategies.

Evaluations of quality in post secondary education are made with reference to generally accepted standards of good practice that serve as criteria for evaluative judgments. This document draws attention to practices that are commonly followed in high quality institutions and adapted to the particular circumstances of higher education in the Kingdom of Saudi Arabia. The scales call for responses to indicate if those practices are followed and if so how well this is done.

The National Commission for Academic Accreditation & Assessment has been established by the Higher Council of Education in Saudi Arabia with responsibility to establish standards and accredit institutions and programs in post secondary education.

The system for quality assurance and accreditation is designed to support continuing quality improvement and to publicly recognize programs and institutions that meet required quality standards. The objective is to ensure good international standards in all post secondary institutions and in all programs offered in Saudi Arabia.

Students, employers, parents and members of the community should be able to have complete confidence that what has been learned by students, the research conducted, and the services provided are equivalent to good international practice. Accreditation of an institution or a program will give public recognition that these standards have been achieved. Saudi Arabian qualifications should be accepted without question anywhere in the world.

This document provides self evaluation scales dealing with standards for higher education programs. The standards apply to all programs in public and private universities and colleges, including those responsible to the Ministry of Higher Education and to any established or regulated by other ministries or agencies. The only exception is for military education which is administered under different arrangements.

The standards and self evaluation scales for programs have been presented in generic terms that are applicable to all programs. Separate documents that draw attention to specific requirements for certain fields of study are in preparation and details of these can be obtained from the NCAAA.

There is considerable variation in the amount of experience that higher education institutions have had with quality assurance processes and the system of higher education is expanding rapidly. In recognition of this the system for accreditation will be introduced progressively over a transition period of several years. During this time institutions that are well advanced with the introduction of quality assurance systems will be considered first, and others will be evaluated and accredited as their internal quality assurance systems are put in place.

The Commission has developed a set of standards for quality assurance and accreditation of higher education institutions in eleven general areas of activity.

1. Mission Goals and Objectives
2. Program Administration
3. Management of Program Quality Assurance
4. Learning and Teaching
5. Student Administration and Support Services
6. Learning Resources
7. Facilities and Equipment
8. Financial Planning and Management
9. Employment Processes
10. Research
11. Relationships With the Community

These standards are based on what is generally accepted as good practice in higher education throughout the world and adapted to the particular circumstances of higher education in the Kingdom of Saudi Arabia.

The standards are described with several levels of detail. First, there are general descriptions for each of the eleven major areas of activity. Second, these are broken down into sub-standards dealing with requirements within each of the major areas. Third, within each of those sub-standards there are a number of good practices that are carried out in good quality institutions. To evaluate performance in relation to the standards, an institution should investigate whether these good practices are carried out and how well this is done. The self evaluation scales have been prepared to assist in this process. In this document the groups carrying out the evaluations within the institution are asked whether the particular practices are followed, and to rate the quality of these practices in the institution on a five point rating scale. Their judgments of quality MUST be based on appropriate evidence including at least some comparisons with other institutions on important items. The development of internal systems to provide that evidence is an essential requirement for an institution's quality assurance system. Unless adequate sources of evidence are available an institution cannot be considered for accreditation.

To be granted accreditation it is necessary for an institution to provide evidence of good quality performance in relation to all the eleven general standards and with all of the subsections of those standards. There is one exception. A college offering only undergraduate programs is not expected to have any significant involvement in research though teaching staff must have continuing involvement in scholarly activities in their field of study.

It is not expected that an institution or program will achieve a high rating for every "good practice" described within the sub-sections of the standards. They are not a simple check list, and items are not equal in importance. Their importance will vary according to the mission and objectives of the institution and its stage of development. However it is desirable that all are met and some are essential. In the initial stages of the introduction of the quality assurance and accreditation system the Commission will indicate a number of items to which special attention will be given. The judgment about whether accreditation should be granted will be an overall assessment by an experienced peer review panel taking account of the mission, objectives and stage of development of the institution and the priorities identified by the Commission.

A description of the eleven general standards is provided in this document together with some general explanatory notes and comments on possible performance indicators and kinds of evidence that could be considered in determining quality of performance.

Further guidance on the use of the standards for continuing monitoring of performance and preparations for accreditation is given in the *Handbook for Quality Assurance and Accreditation in Saudi Arabia* prepared by the Commission.

Relationships Between Standards for Institutions and Standards for Programs

General standards have been developed for higher education institutions and programs. They cover the same general areas of activity but there are some differences that reflect a total institutional overview on the one hand and the perspective of just one specific program on the other. In addition, some general institutional functions are not considered in a program evaluation.

Activities relating to the standards fall into three categories.

- Those that are institutional and have no impact or only very indirect impact on programs. Examples include the management of extra curricular activities or the attractiveness of buildings and grounds. These are not considered in looking at the application of the standards to programs.
- Those that are general institutional activities with a major impact on programs. Examples would be the provision of learning resources through a library or the processes for employment and promotion of staff. Evaluation of these functions in an institutional evaluation would be broad and consider the quality of management and services provided for the institution as a whole and how effectively they support all programs throughout the institution. In a program evaluation they would be considered from the perspective of the particular program concerned. For example a library might be very good in many ways, but not have the materials to support a particular program. In that case the provision of learning resources might receive a reasonably high rating in

an institutional evaluation but a low rating in an evaluation from the perspective of the program concerned in the program evaluation.

- Those that relate directly to the planning and delivery of programs. Examples would be the appropriateness of intended learning outcomes for students and the quality of teaching in the program. For an institutional evaluation these things should be looked at within all programs, and then a judgment made about strengths and weaknesses in the institution's programs as a whole with the possibility of identifying significant variations between different programs. In an institutional evaluation part of the consideration for teaching and learning should be the effectiveness of processes for ensuring all programs are of good quality, monitoring performance, and supporting improvements in all programs throughout the institution. An evaluation of learning and teaching for an institutional evaluation would normally be done by getting a profile of performance at the level of departments or colleges, and then preparing a report identifying similarities and differences and overall performance for programs in general.

In this document standards have been described dealing with the things that should be considered in relation to evaluation of a program. They include the matters described in the second and third of these categories.

Evidence of Performance

Judgments about quality based on general impressions could be accurate, but they could also be badly distorted for a number of reasons. Consequently general opinions without supporting evidence cannot be relied on in making assessments of quality in relation to specified standards. Because of this it is necessary to consider appropriate forms of evidence whenever a judgment is made about quality of performance in relation to standards.

What is appropriate evidence will vary widely for different things that are evaluated and an important element in any quality assessment is to decide on what kind of evidence is appropriate for the matter being considered.

In many cases several different forms of evidence should be considered to make a reliable judgment, and the evidence will need to be interpreted. For example high average grades in a course could mean that students have achieved very high standards because of excellent teaching. Alternatively they could mean that standards are low and grades have been inflated. To draw valid conclusions it would be necessary to check that tests were sufficiently rigorous and that criteria for allocating grades were appropriate and fairly administered.

Interpretations of evidence can also be unreliable, and to guard against this it is recommended that groups that undertake evaluations in relation to the standards include some people who have been involved in the activity concerned, some who are the recipients of the service provided (eg students, graduates or members of departments who use services provided by central administrative units or centers) and also some who are familiar with that kind of work, but are not directly involved in that service provision. As a further safeguard it is recommended that the final judgments be reviewed and an independent opinion given by someone who has not been involved in the initial evaluation as a check on whether the interpretations seem reasonable in the light of the evidence provided.

Performance Indicators

A wide range of kinds of evidence can be considered. However as part of the evidence to be used decisions should be made about some specific items of information that can be expressed in quantitative terms and used as performance indicators. These should be identified in advance as part of planning processes. For example when major goals or objectives are established specific indicators should be specified so achievement of those goals and objectives can be monitored on a continuing basis. It is also important for an institution to identify some key performance indicators that will be used consistently by departments and colleges throughout the institution to monitor their own performance, provide for comparisons of performance between departments and colleges, and permit university committees and senior administrators to monitor overall institutional quality on a continuing basis.

Data on these indicators should be collected in standard form and retained in a central data base so there can be comparisons within the institution and over time. An evaluation of the effectiveness of these processes

will consider whether appropriate indicators have been identified, whether the data is consistently collected and recorded, and whether the information is used in monitoring and analysing quality of performance.

It is the responsibility of every program to monitor and plan for improvement in relation to its own mission and objectives. However the Commission has also identified certain key performance indicators on which information should collected in all institutions. This requirement has several important objectives. It provides a common set of statistical data that can be used by institutions and by those responsible for programs for comparisons of performance and benchmarking within their own institution and elsewhere within the country. (The Commission will publish information for groups of similar institutions, but individual institutional data will be confidential to each institution) It assists the Commission and other relevant Ministries and organizations in monitoring the quality of performance of the system of higher education as a whole, and it provides a sample of important information about institutions that makes it possible for the Commission to maintain accreditation of institutions in the interval between major external reviews.

These indicators established by the Commission should be used by institutions and program managers as part of their quality assurance processes, but they are also encouraged to add additional indicators which they select for themselves that relate to their own mission and objectives and their priorities for improvement.

Good Practices Relevant to More than One Standard

Within each standard and sub-standard a number of statements are made about things that should be done if the standard (or sub-standard) is being met. Many of these statements appear in several different places. This should not be regarded as unnecessary duplication, but rather as a result of the fact that a number of practices are relevant to more than one standard. For example, an expectation that teaching staff be involved on a continuing basis with scholarly activities that ensure they remain up to date is relevant to Qualifications and Experience of Teaching Staff (Standard 4. 8) and also to Personal and Career Development (Standard 9.3), and an expectation that standards of learning outcomes should be checked against the National Qualifications Framework and standards at other comparable institutions is relevant to the standard for Management of Quality Assurance and Improvement (Standard 3) and also to the sub-standards for Student Learning Outcomes (Standard 4.1) and Student Assessment (Standard 4. 4).

Application of the Standards to Different Types of Institutions.

The standards are designed for all higher education institutions, that is institutions offering programs described as higher education and leading to higher education qualifications in the National Qualifications Framework.

While the general standards for higher education institutions are the same for all there are some important differences in the circumstances of some types of institutions that affect how the standards should be applied.

- There are some differences in the regulations affecting public and private institutions, including some relating to borrowing, fee payments by students and financial management. Consequently some of the standards specified for these matters are not relevant to some institutions.
- There are expectations for universities relating to involvement in research and post graduate study. These should be reflected in the evaluations in standard 10 dealing with research. Although scholarly activities on the part of faculty should be encouraged in all institutions these requirements for research do not have to be met in private colleges that are not part of universities.
- Some institutions are involved in partnership arrangements with other institutions, either within or outside the Kingdom, under which certain elements of program planning and evaluation are shared. If such arrangements exist processes must be followed that ensure that quality is maintained and the requirements of the Saudi Arabian system are met.
- Some institutions offer programs by distance education. This different form of delivery changes the form of interaction between students and institutions and leads to additional requirements for program delivery and support. The special requirements for distance education programs are set out in a different document.

In the self evaluation scales attention is drawn to some of these differences. If a particular practice is not applicable to the institution concerned the item should simply be marked as not applicable (NA).

Notes on What Constitutes a Program

A program is regarded as an integrated package of courses and activities in an academic or professional field leading to a qualification. However organizational arrangements in institutions differ and there are sometimes questions about what should be considered as a program.

A program includes all of the courses a student is required to take, including courses that are required by an institution or a college as well as those required by a department, and including any general education programs as well as those in a professional or academic field. It includes courses that may be offered as service courses by another department or college.

A program offered on both men's and women's campuses is a single program and should be evaluated as such. However since there may be significant differences in facilities, resources, experience of faculty, employment of graduates or other matters evidence should be obtained about what happens on each campus and any differences noted and considered in planning what should be done in response. Program reports should show both the evaluations for each campus and a combined result.

A program offered on a remote as well as on an institution's main campus should be dealt with in the same way.

A program offered either on-campus or through distance education should also be evaluated in the same way, that is, information collected for each mode of delivery and reported in a way that shows any differences found. However there are a number of additional matters that relate to distance education and these must also be considered using the standards for distance education.

A program may have an early exit point, for example it may be possible for students to complete two years of study and receive an associate degree or to continue for several more years and complete a bachelor degree. If this is done it is essential that the associate degree be planned so that it provides a complete and useful qualification in its own right. For example it might include significantly more practical and applied work in the field than students would normally undertake in the first two years of a bachelor degree program. It is not acceptable for such an award to be granted simply because students fail or drop out after the early parts of a longer program.

The distinction between what is regarded as a single program or a cluster of related programs is difficult to define and may be best explained through examples.

A bachelors degree program to prepare a student as a civil engineer would be regarded as a different program from one to prepare a mechanical engineer, even though there may be some courses that are common to both. Similarly, if a student had completed the bachelors degree program and wished to take a post graduate program leading to a masters degree or a doctorate in the same general field, that would be regarded as a separate program. The test in these examples relates to there being a qualification that is regarded as being complete in itself, and in the case of a professional program, qualifying the person who has taken the program for professional practice in the field. The distinction does not necessarily relate to organization of an institution or college into departments. In the particular example given it is likely that a civil engineering department would offer both the undergraduate and the postgraduate programs. It would also be possible if an institution wished to organize itself in that way for a single department to offer programs in both civil and mechanical engineering.

The title of an academic award is not necessarily a useful guide to what should be regarded as a program. For example general titles such as Bachelor of Arts, or Business, or Science, could include many different programs. In an Arts degree there could be programs in history and or social sciences, in psychology, in social work, or many others. A Business degree could include separate programs for accountants, for economists, or for management and administration, and these would be different programs leading to quite different occupational skills.

The programs that have been used in these examples are separate entities, and will be accredited as such. However this does not prevent groups of related programs being considered together by an external review team in the accreditation process provided it is possible for external review panels to include the necessary expertise. A panel might consider an undergraduate and a post graduate program in the same field at the same time. However the institutions self study and the reports of the review panel will deal separately with each program ant it would be possible for one such program to be accredited and not the other.

An equivalent set of standards has been developed for institutions offering post secondary programs in technical education and training. These standards differ from those for higher education institutions because of important differences in the nature of programs and the processes for program development and delivery. The standards for these institutions are set out in another document, *Standards for Accreditation of Technical Education and Training Institutions.*

Using the Self Evaluation Scales

High quality standards can only be achieved by honest evaluation of performance and commitment to improve, and by action planned and taken by those offering the program and providing the services on which it depends. In recognition of this teaching and other staff responsible for various activities should evaluate their own performance in comparison with generally accepted standards of good practice.. Although every effort should be made to form valid and reliable judgments based on evidence, a number of these evaluations will involve subjective judgments and to avoid an illusion of precision and discourage a misleading aggregation of total numbers in a single "quality score" it is recommended that a starring system be used for rating these quality evaluations. It is expected that these self evaluation scales will be used by institutions and by those responsible for programs in their initial quality assessment, their continuing monitoring of performance, and in their more extensive periodic self studies prior to an accreditation review by the Commission.

In this document information about the standards is presented at two levels. The first is a general statement of the standard as it applies to a broad area of activity and the second is a description of why it is important and the kinds of processes that are expected if the standard is achieved.

This explanatory information is followed for each standard by a number of more specific statements of "good practices" that are typically carried out in a high quality institution with scales to indicate whether and how well the practice is followed.. The scales" are presented in groups that deal with major components or sub-sections of the general standards.

The lists of specific practices are intended primarily as a guide for those responsible for particular activities to draw attention to things that are generally regarded as good practice, and to assist them in their self-evaluations.

Some of these statements are relevant to certain institutions but not to others. Where an item is not applicable it should be simply marked NA, and ignored.

For each individual item two responses are called for. The first is to indicate whether the practice is followed in the institution. The possible responses are:

NA -- the practice is not applicable or relevant for the institution or unit making the response.
Y – yes, the practice is followed; or
N – no, the practice is relevant but not followed.

The second response is called for in cases where the practice is relevant to the institution (i.e. a "Y" or "N" response). It involves the use of a five-point rating scale to evaluate on a how consistently and how well the practice is carried out. Stars, rather than a numeric or alphabetic rating scale, are used for this purpose.

The evaluations relate to:

The extent and consistency with which processes are followed;
The quality of the service or activity as assessed through systematic evaluations;
The effectiveness of what is done in achieving intended outcomes.

Using Stars for Evaluations

Performance should be assessed by allocating from zero to five stars in accordance with the following descriptions:

Improvement Required

No Star – The practice is relevant but not followed at all. A zero should be recorded on the scale.

One Star – The practice is followed occasionally but quality of the activity is poor or not evaluated.

Two Stars -- The practice is usually followed but the quality is less than satisfactory.

Good Performance

Three Stars—The practice is followed most of the time. Evidence of the effectiveness of the activity is usually obtained and indicates that satisfactory standards of performance are normally achieved although there is some room for improvement. Plans for improvement in quality are made and progress in implementation is monitored.

High Quality Performance

Four Stars—The practice is followed consistently. Indicators of quality of performance are established and suggest high quality but with still some room for improvement. Plans for this improvement have been developed and are being implemented, and progress is regularly monitored and reported on.

Five Stars—The practice is followed consistently and at a very high standard, with direct evidence or independent assessments indicating superior quality in relation to other comparable institutions. Despite clear evidence of high standards of performance plans for further improvement exist with realistic strategies and timelines established.

Converting Survey Responses to a Starring System.

In a number of cases the individual items refer to evaluations of quality by students, faculty, or other stakeholders. The wording of survey instruments and items in rating scales can influence results significantly and interpretations of the data and independent verification of conclusions is important. However as a general guide where a five point rating scale is used with possibilities of positive and negative assessments evenly balanced, an overall rating from respondents to a survey might achieve star ratings as follows:

Above 4.5	Five stars
3.6-4.5	Four stars
2.6-3.5	Three stars
1.6-2.5	Two stars
1.5 or below	One star

Combining Ratings on Individual Items to Develop a Broader Evaluation

The quality ratings of specific practices can be combined to guide broader judgments about an institution's performance in relation to the groups of items that are shown as components of each general standard, or to each broad standards as a whole. This can be done by averaging the number of stars, ignoring the items marked NA and counting items where the practice is relevant but not followed as zero.

However the individual items are not necessarily of equal importance and if individual items are combined to form an overall assessment consideration should be given to weighting certain items more heavily than others and adjusting the overall rating accordingly. Space is provided on the forms to note when this kind of adjustment is made.

Aggregating Evaluations to Obtain an Institution-Wide Overview

The rating scales are presented in a form that enables them to be used for individual programs and aggregated to give an overview of the quality of programs for a college or for the institution as a whole. When aggregated in

this way the scales should assist in the conduct of an institutional self-study, and provide useful information for external review panels as they carry out their independent institutional reviews.

It is recommended that programs within a department or college be looked at together noting both similarities and any significant differences between them, and then at a second stage the reports on programs within colleges brought together to give an overall picture for the institution. It is possible in these processes to simply work out an average number of stars for various functions. However if there are significant differences the overall average is much less important than variations between programs or colleges. Consequently these variations should be identified and reported on, and considered carefully when suggestions are made for improvements.

Priorities for Improvement

An important outcome of the self-assessment carried out through the use of the rating scales is to identify areas for improvement. It is rarely possible to do everything at once and priorities have to be established. Space is provided on the forms to indicate particular items that are considered the highest priorities for improvement.

Indicators as Evidence of Performance

As far as possible evaluations should be based on direct evidence that practices are followed, and that desired levels of quality are achieved rather than general post hoc impressions. This consideration of evidence need not be a major undertaking but it does require some advance planning and selection of indicators that will be used as evidence of performance. The performance indicators should be specified in advance and data gathered and considered as part of continuing monitoring processes. (This does not preclude consideration of other evidence that may emerge) The document includes space for the selected performance indicators to be noted.

Expected Standards of Performance

It is not expected that every program will rate at the highest level on all dimensions of activity. That would be unrealistic, and setting up such expectations is not the purpose of the document. Instead it is intended to provide descriptive performance standards in many different forms of activity, so there can be a clearer basis for evaluation in relation to generally accepted standards of good practice. This is intended to help those responsible for programs in their self-evaluations and planning for improvement, and to help the institution as a whole to identify areas of relative strength and weakness, and to work towards improvement in spheres of activity that are considered priorities for development.

While the document is intended primarily to assist in evaluations and planning for improvement within institutions it also establishes levels of performance that are considered necessary for accreditation. For this purpose the basis of judgment will be at the level of the broader standards rather than the precise assessment of performance in relation to each individual practice. In general a one or two star rating on a standard is considered unsatisfactory and three stars is a minimum acceptable level of performance. However as noted above not all functions are of equal importance in accreditation judgments and the particular circumstances of an institution, and its strategies for development, will be taken into account.

Relative Importance of Different Standards

The point about some items in the rating scales being more important than others applies to the broader standards as well, and the relative importance will vary for different institutions. The place of research is a good example of this. In some institutions, particularly universities seeking international recognition the quality and extent of participation in research is vitally important and international ratings of universities give considerable weight to research performance. In others, such as a college concentrating on quality of undergraduate programs, research may be of little significance though it is still important that faculty participate in scholarly activities to ensure that their teaching is up to date with latest developments.

The quality of learning and teaching will always be of primary importance since this is normally the primary function of an educational institution. Satisfactory performance in relation to this standard is essential for accreditation.

Independent Verification of Evaluations

Although direct evidence of quality of performance should be obtained wherever possible, many of the judgments have to involve some subjective opinions. When self evaluations are made by an individual or a

group this can mean unduly harsh or overly generous assessments and some action should be taken to correct for this.

Provision is made in the scales for independent opinions to be given by a person familiar with the type of activity, but independent of those responsible for it, and whose judgment is respected. For many items during annual evaluations these independent opinions could be given by a person nominated by a dean or department head, such as a colleague from another department within the institution. For major judgments on important items, for example in a program self study prior to an external review for re-accreditation of a program, greater independence may be required.

Note on Terminology

The term **governing body** is used as a general descriptive title for the highest policy making body or committee in a post secondary institution. This would be the university council in a public university, or a board of trustees in many private colleges.

The term **rector or dean** is used in this document to refer to the head of an institution. Rector is the title normally used in Saudi Arabia for the head of a public university, and dean is typically used as the administrative head of a smaller institution or a private college. The term dean is also used for the head of a college within a university, and a private university or college may use other terms for the administrative head such as president or director. In this document reference is made to rector or dean, and it should be possible from the context of the reference to avoid confusion with the position of dean of a college within a university.

The term **teaching staff** has been used rather than "faculty" to refer to all individuals responsible for teaching groups of students. It includes faculty or equivalent members of staff as formally defined in Ministry regulations but also anyone else who has been given teaching responsibility. It includes tutors or instructors working with groups of students in a distance education or on-campus program, but does not include laboratory assistants or others who assist with the teaching of classes under the direct supervision of others.

Standard 1 Mission Goal and Objectives

The mission of the program must be consistent with that for the institution and apply that mission to the particular goals and requirements of the program concerned. It must clearly and appropriately define the programs principal purposes and priorities and be influential in guiding planning and action.

Main components in this standard:

1.1 Appropriateness of the Mission
1.2 Usefulness of the Mission Statement
1.3 Processes of Development and Review of the Mission
1.4 Use Made of the Mission Statement
1.5 Relationship between Mission, Goals and Objectives.

Comment and General Description of Good Practice

Effective and coordinated planning and development normally requires that a program have a succinct mission statement, summarizing in a few sentences what it is trying to achieve as a guide to detailed planning and development.

The mission statement should establish priorities for development and quality improvement and be key element in the quality assurance process. Consequently it should be prepared in a way that generates a sense of ownership on the part of all those involved with the program, be periodically reviewed as a major policy issue, and consistently referred to as a basis for planning and evaluation. It should be consistent with the charter establishing the institution, and realistic in relation to the capacity of the institution in the environment within which it is operating, but at the same time present challenges for development and improvement.

Goals should be thought of as applications of the mission to specific activities. They establish directions for detailed planning though they are usually expressed in general terms.

Objectives should be linked through strategic planning processes to the mission and goals They should be more specific and include intended results to be achieved within a stated time period.

This standard relates to the way the mission statement has been developed and is expressed, to its effectiveness in guiding the development of the program, and to the relationships between the mission and the goals and objectives.

Evidence and Performance Indicators

Evidence about the quality of the mission could be obtained from examination of the mission statement itself, copies of papers proposing the mission or modifications in it, interviews with teaching and other staff and students to find out how well it is known and supported, and consideration of other reports, proposals and statements to see the extent to which the mission is used as a basis for decisions. Indicators that could be used include responses to questions on surveys to see how well the mission is known and supported, or the proportion of policy decisions that refer to the mission among criteria for the decision made.

Standard 7 Facilities and Equipment

Adequate facilities and equipment must be available for the teaching and learning requirements of the program. Use of facilities and equipment should be monitored and regular assessments of adequacy made through consultations with faculty, staff and students.

The scales below ask you to indicate whether these practices are followed in your institution and to show how well this is done. Wherever possible evaluations should be based on valid evidence and interpretations supported by independent opinions

Good Practices Relating to This Standard	**Is this true? Y/No/NA**	**How well is this done? (enter stars)**
7.1 Policy and Planning Planning processes for the provision of facilities and the acquisition and maintenance of equipment must include consultation with program representatives to ensure clear specification of program requirements. Plans for provision must appropriately balance program requirements with institutional policies to ensure compatibility of systems and resources available.		
7.1.1 Equipment acquisitions meet program requirements and are also consistent with institutional policies to achieve compatibility of equipment and software systems across the institution.		
7.1.2 Teaching staff are consulted before major equipment acquisitions to ensure that current and anticipated emerging needs are met.		
7.1.3 Equipment planning provides for acquisition, servicing and replacement according to a planned schedule.		
Overall Assessment		
Comment_____		
_____		
Priorities for Improvement_____		
_____		
Independent Opinion		
Comment_____		
_____		
7.2 Quality and Adequacy of Facilities and Equipment Facilities and equipment must be of good quality with effective strategies used to evaluate their adequacy for the program, their quality and the services associated with them.		
7.2 1 Facilities meet health and safety requirements and make adequate provision for the personal security of faculty, staff and students.		
7.2.2 Quality assessment processes include both feedback from principal users about the adequacy and quality of facilities, and mechanisms for considering and responding to their views.		
7.2.3 Standards of provision of teaching, laboratory and research facilities are adequate for the needs of the program and benchmarked through comparisons with other comparable institutions. (This includes such things as classroom space, laboratory facilities and equipment, access to computing facilities and associated software, private study facilities, and research equipment.		
7.2.4 Adequate facilities are available for confidential consultations between faculty and students)		
7.2.5 Provision is made for students, faculty and staff with physical disabilities or		

other special needs.

Overall Assessment

Comment_____

_____

Priorities for improvement_____

_____

Independent Opinion

Comment_____

_____

7.3 Management and Administration

Management and administration of facilities, equipment and associated services must be efficient and ensure maximum effective utilization of facilities provided.

7.3.1 A complete inventory is maintained of equipment used in the program that is owned or controlled by the institution including equipment assigned to individual faculty or staff for teaching and research.

7.3.2 Services such as cleaning, waste disposal, minor maintenance, safety, and environmental management are efficiently and effectively carried out.

7.3.3 Provision is made for regular condition assessments, preventative and corrective maintenance, and replacement.

7.3.4 Effective security is provided for specialized facilities and equipment for teaching and research, with responsibility between individual faculty, departments or colleges, or central administration clearly defined.

7.3.5 Effective systems are in place to ensure the personal security of faculty, staff and students, with appropriate provisions for the security of their personal property.

7.3.6 Arrangements are made for shared use of underutilized facilities with adequate mechanisms for security of equipment.

Overall Assessment

Comment_____

_____

Priorities for improvement_____

_____

Independent Opinion

Comment_____

_____

7.4 Information Technology

Computing equipment and software and related support services must be adequate for the program and managed in ways that ensure secure, efficient and effective utilization.

7.4.1 Computing equipment is available and accessible for faculty, staff and students and the adequacy of this provision is regularly assessed. Y 4

7.4.2 Institutional policies governing the use of personal computers by students are complied with. Y 5

7.4.3 Technical support is available for teaching staff and students using information and communications technology Y 3

7.4.4 Opportunities are available for teaching staff input into plans for acquisition and Y 2

replacement of IT equipment for use in the program.

7.4.5 Security systems are in place to protect privacy of personal and sensitive personal and institutional information, and to protect against externally introduced viruses.	Y	5
7.4.6 Compliance with a code of conduct relating to inappropriate use of material on the internet is checked and instances of inappropriate behavior dealt with appropriately.	N/A	
7.4.7 Training programs are available for faculty and staff to ensure effective use of computing equipment and appropriate software for teaching, student assessment, and administration	Y	4
Overall Assessment		3.83

Comment_____

_____

Priorities for improvement_____

_____

Independent Opinion

Comment_____

_____

_____

Overall Assessment of Facilities and Equipment

7.1 Policy and Planning

7.2 Quality of and Adequacy of Facilities

7.3 Management and Administration

7.4 Information Technology

Combined Assessment

Comment _____

_____

_____

Independent Opinion

Comment_____

_____

Indicators Considered _____

_____

_____

_____

Priorities for Improvement _____

_____

_____

_____

_____

Evidence of Process of Investigation

جامعة الأمير محمد بن فهد
PRINCE MOHAMMAD BIN FAHD UNIVERSITY
Quality Center

Quality Center Meeting Minutes

Date: April 6, 2011

Topic: NCAAA Institutional Self Study

Participants: Facilities and Engineering: Dr. Dobe, Quality Center, R. Davis

Areas of discussion: Section H - 7 of Facilities and Equipment

- Review of Evaluation Scales – most pertinent pages
- Review of Standards with particular attention to key pages as marked on document
- Review of Scales and Self Study with attention given to pgs 5-5 of Scales for Star Rating, process for Scaling, and overview of the range covered in the whole of the H – 7 section
- Discussion of evidence trail
- NCAAA Institutional guidelines for access to NCAAA documents and call-outs for hard and soft copies

Tasks assigned (with target dates if given):

- May 4, 2011 as target completion date

Key Questions/Areas for follow-up (with responsible parties if assigned):

- Absence of Mr. Naimi for much of this cycle may require expansion of Facilities and Equipment Quality Committee

جامعة الأمير محمد بن فهد
PRINCE MOHAMMAD BIN FAHD UNIVERSITY
Quality Center

Quality Center Meeting Minutes

Date: May 4, 2011
Topic: Facilities and Equipment
Participants: Dr. Dobe (Fac & Equip), Mr. Davis (QC)
Areas of discussion: Prepare electronic packets for Fac/Equip team, Process for completing Scales and SS Report, KPI's, Evidence binder (digitize flip-chart pages), submission process

Tasks assigned (with target dates if given):

- Fac & Equip Quality Team to continue processes

Key Questions/Areas for follow-up (with responsible parties if assigned):

جامعة الأمير محمد بن فهد
PRINCE MOHAMMAD BIN FAHD UNIVERSITY
Quality Center

Quality Center Meeting Minutes

Date: June 6, 2011

Topic: NCAAA KPIs and Inst Self Study Section

Participants: Dr. Dobe, Mr. Jessie (IT), Randy Davis (QC)

Areas of discussion:

- KPI's to infuse data into Self Study documentation and the KPI submission process
- IT and QC representative completing collaboratively the KPI document
- PMU and IT Strategic Plans review and integration into KPI report
- IT: "Total PMU Expenditures per PMU Student" QC liaised with Budget/Finance to procure Annual IT Expenditure Report and alerted Budget/Finance to other PMU entities needing same or similar reports asap.

Tasks assigned (with target dates if given):

- Team to complete KPIs this week
- On track to complete NCAAA Self Study Section by June 20

Key Questions/Areas for follow-up (with responsible parties if assigned):

- Concerns expressed regarding how to best complete the Facilities and Technical Equipment Self-Study section as Dr. Dobe is an IT specialist.

	Deanship of Quality and Accreditation Meeting Minutes	
Date:	Sept 28, 2011	
Topic:	NCAAA Inst Self Study: ITD	
Participants:	Dr. Dobe (ITD), Randy Davis (DQA)	
Areas of Discussion:	NCAAA Inst Self Study Report/Self Evaluation Scales Star Rating Process Review (DQA KPIs & ITD Strategic Plan were completed in soft & hard copy Spring 2011): • ITD will continue with process by convening full teams to address Self Study Report Star Rating process • Particular attention given to obtaining full and well-informed input via review of Star Rating Criteria displayed in conference room with particular attention given to delineations between each level of Star Rating --- ITD to use Star Rating process as an opportunity to teach the required processes to ensure comprehensive input and participation in addition to developing a high level of understanding of overall processes & PMU, ITD policies and responses of ITD department • Particular attention given to full understanding of each sub-standard • Document gathering process, review of documents • Team input into Strengths and Areas Offering Room for Improvement Narratives • SMART Plans to remediate weaknesses • DQA representative to assist as requested by ITD in future processes	
Tasks assigned (with target dates if given):	ITD requests extension of deadline until Oct 15, 2011	
Key Questions /Areas for follow-up (with responsible parties if assigned):		

	Deanship of Quality and Accreditation Meeting Minutes	
Date:	Oct 5, 2011	
Topic:	NCAAA Inst Self Study: FAc/Equip (ITD Specific)	
Participants:	DR. Dobe and Mrs. Maazam, Abdulaziz, Alsghar, Garret and Mario (ITD),Randy Davis (DQA)	
Areas of Discussion:	NCAAA Inst Self Study: Section 7, Fac/ Equip (ITD) • Review of Self-Eval Scales / Star Rating Criteria • Review of FAc / Equip Sections – noting areas for collaboration between LRC, Eng Antonio and ITD • Selected sub-standards that are ITD specific • Completed Star Rating, noted document collection to be completed, began Strength and Opportunities for Improvement Narratives, began Action Plans with Responsible Parties and Timeframes. • Process and Responsible Parties for soft and hard copy production.	
Tasks assigned (with target dates if given):	• Soft copy and hard copy of ITD specific sections and related sub-sections to be readied by Oct 15, 2011 per previous agreement	

	Deanship of Quality and Accreditation Meeting Minutes	
Date:	October 8, 2011	
Topic:	NCAAA Inst Self Study:	
Participants:	Dr. Dobe (ITD),Randy Davis (DQA)	
Areas of Discussion:	NCAAA Inst Self Study: Follow-up on Self Eval Scales meeting of Wed: • Hyper-Links • Action Plans	
Tasks assigned (with target dates if given):	• Mr. Mario to continue to print and bind hard copies. • ITD to complete Inst Self Study doc for submission	
Key Questions/ Areas for follow-up (with responsible parties if assigned):		

Key Questions/ Areas for follow-up (with responsible parties if assigned):	• Particular areas needing coordination between LRC/Dr. Rice and Eng. Antonio of Fac/ Equip have been denoted for follow-up • Team members have been appointed to particular Action Plans and will follow-up as required to ensure full process documentation and completion of planned processes.	

Standard 7 Facilities and Equipment

Adequate facilities and equipment must be available for the teaching and learning requirements of the program. Use of facilities and equipment should be monitored and regular assessments of adequacy made through consultations with faculty, staff and students.		
The scales below ask you to indicate whether these practices are followed in your institution and to show how well this is done. Wherever possible evaluations should be based on valid evidence and interpretations supported by independent opinions		
Good Practices Relating to This Standard	**Is this true? Y/No/NA**	**How well is this done? (enter stars)**

1. **Policy and Planning**

Planning processes for the provision of facilities and the acquisition and maintenance of equipment must include consultation with program representatives to ensure clear specification of program requirements. Plans for provision must appropriately balance program requirements with institutional policies to ensure compatibility of systems and resources available.

1. Equipment acquisitions meet program requirements and are also consistent with institutional policies to achieve compatibility of equipment and software systems across the institution. Coordinate w/ Dr. Des
7.1.2 Teaching staff are consulted before major equipment acquisitions to ensure that current and anticipated emerging needs are met. Coordinate w/Antonio & Dr. Des
7.1.3 Equipment planning provides for acquisition, servicing and replacement according to a planned schedule. Coordinate w/Antonio

Overall Assessment

Comment_____

_____

Priorities for Improvement_____

_____

Independent Opinion

Comment_____

_____

2. **Quality and Adequacy of Facilities and Equipment**

Facilities and equipment must be of good quality with effective strategies used to evaluate their adequacy for the program, their quality and the services associated with them.

7.2 1 Facilities meet health and safety requirements and make adequate provision for the personal security of faculty, staff and students.
1. Quality assessment processes include both feedback from principal users about the adequacy and quality of facilities, and mechanisms for considering and responding to their views.
2. Standards of provision of teaching, laboratory and research facilities are adequate for the needs of the program and benchmarked through comparisons with other comparable institutions. (This includes such things as classroom space, laboratory facilities and equipment, access to computing facilities and associated software, private study facilities, and research equipment.
3. Adequate facilities are available for confidential consultations between faculty and students)
4. Provision is made for students, faculty and staff with physical disabilities or other special needs. Coordinate with Dr. Des & Antonio

Overall Assessment

Comment_____

_____

Priorities for improvement_____

_____

Independent Opinion

Comment_____

1. ~~**Management and Administration**~~
~~Management and administration of facilities, equipment and associated services must be efficient and ensure maximum effective utilization of facilities provided.~~

1. ~~A complete inventory is maintained of equipment used in the program that is owned or controlled by the institution including equipment assigned to individual faculty or staff for teaching and research.~~
2. ~~Services such as cleaning, waste disposal, minor maintenance, safety, and environmental management are efficiently and effectively carried out.~~
3. ~~Provision is made for regular condition assessments, preventative and corrective maintenance, and replacement.~~
4. ~~Effective security is provided for specialized facilities and equipment for teaching and research, with responsibility between individual faculty, departments or colleges, or central administration clearly defined.~~
5. ~~Effective systems are in place to ensure the personal security of faculty, staff and students, with appropriate provisions for the security of their personal property.~~
6. ~~Arrangements are made for shared use of underutilized facilities with adequate mechanisms for security of equipment.~~

Overall Assessment

Comment_____

_____

Priorities for improvement_____

_____

Independent Opinion

Comment_____

_____

7.4 Information Technology

Computing equipment and software and related support services must be adequate for the program and managed in ways that ensure secure, efficient and effective utilization.

Y

4

7.4.1 Computing equipment is available and accessible for faculty, staff and students and the adequacy of this provision is regularly assessed. Link to Weekly ITD Classroom and Labs Report (Print all links request for purchase and all reminder letters for Purchasing). Deployment of Banner Electronic purchasing module will enable us to move from 4 to 5.

Y

5

1. Institutional policies governing the use of personal computers by students are complied with.

3

Y

2. Technical support is available for teaching staff and students using information and communications technology. University Help Desk system used to track and trace support request to successful resolution. Aging reports are required to move service level from 3 to 4. **Action Plan 1** (See Appendix A) Summary: Evaluate cost effective commercial package solution for service desk software, point person is Abdulaziz. Recommendation to Eng. Yamani through CIO due by January 31, 2012.

2
Y
3. Opportunities are available for teaching staff input into plans for acquisition and replacement of IT equipment for use in the program. **Action Plan 2** (See Appendix B) Summary: Part 1 is a faculty orientation program completed. Link to presentation on faculty orientation; Part 2 conduct faculty survey. Link to survey instrument; Part 3 is work with Learning Resource Center to establish faculty forum for education equipment and software suggestions, input, discussion. CIO to coordinate with Director of LRC and College Deans not later than March 31, 2012. CIO and Team Lead of MIS to finalize faculty satisfaction survey not later than October 26, 2011.
5
Y
4. Security systems are in place to protect privacy of personal and sensitive personal and institutional information, and to protect against externally introduced viruses. Based upon 20 years in IT Services, current CIO believes the level of security at PMU is higher than any institution he has ever worked for and it suitable for financial institution such as Bank.
N/AA/
5. Compliance with a code of conduct relating to inappropriate use of material on the internet is checked and instances of inappropriate behavior dealt with appropriately. Security system proactively monitors abuse of systems, log attempts to compromise security, and proactively disable access to system when abuse detected.
4
Y
6. Training programs are available for faculty and staff to ensure effective use of computing equipment and appropriate software for teaching, student assessment, and administration. IT supports Learning Resource Center by providing subject matter expert trainer who participates in professional development for all employees (faculty and staff). Also IT supports the Student Affairs Division with student orientation and other training required to help students use systems and services. Example of Student Orientation.

3.83

Overall Assessment

Comment_____

_____

Priorities for improvement_____

_____

Independent Opinion

Comment_____

_____

_____

Overall Assessment of Facilities and Equipment

7.1 Policy and Planning

7.2 Quality of and Adequacy of Facilities

7.3 Management and Administration

7.4 Information Technology

Combined Assessment

Comment _____

_____

_____

Independent Opinion

Comment_____

_____

Indicators Considered_____

_____

_____

_____

Priorities for Improvement_____

_____

_____

_____

_____

Appendix A: Action Plan for Commercial Service Desk System

Reference Question: 7.4.3 Technical support is available for teaching staff and students using information and communications technology.

ACTION PLAN FOR CONTINUOUS IMPROVEMENT:

Evaluate cost effective commercial package solution for service desk software, point person is Abdulaziz.

Mr. Abdulaziz to gather functional requirements, survey current market options to meet these requirements, select vendors for Request for Proposals (RFP), create and process RFP through ETA office.

Recommendation to Eng. Yamani through CIO due by January 31, 2012.

Appendix B: IT Governance for Instructional Technologies

Reference Question: 7.4.4 Opportunities are available for teaching staff input into plans for acquisition and replacement of IT equipment for use in the program.

ACTION PLAN FOR CONTINUOUS IMPROVEMENT

Part 1: Faculty Orientation Program (COMPLETED September 2011)

Faculty orientation program completed to include coverage of the follow content areas.

Starting With 20 Minutes on the Basics
Who Do I Call When I Have A Problem?
One Stop Shop: X8888 Is Also the Number You Call for all Engineering and Technical Affairs (Which Includes IT and Facilities and Maintenance)
Demo of Outlook E-Mail, Web Site, Call! (2 Minutes)
Using My Computer From Work
Wired in Your Office (2 Minutes)
Wireless in Common Areas at Campus (2 Minutes)
Using a USB Flash Drive
Getting Access to the Local Network Server (2 Minutes)
Applications on My Computer - Faculty Laptops (2 Minutes)
Accessing the Required Documents Through the Intranet (5 Minutes)
Introduction to IPT (10 Minutes)
IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long) -- Continued
10 Minutes: Using My Computer From the Compound
Getting Internet via STC or Mobily (5 Minutes)
Online Banking (5 Minutes)
5 Minutes: Getting and Setting Up My PMU E-Mail Account:
Outlook & Web Mail
My Banner Faculty Self-Service Account: Getting and Setting Up and Submitting Grades!
IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long) -- Continued
20 Minutes: My Banner Faculty Self-Service Account
Introduction to Banner (2 Minutes)
Login In to Faculty Self-Service For the First Time (2 Minutes)
Introduction to Your Self-Service Banner Session and Main Menu (4 Minute)
Introduction to Your Faculty Schedule (6 Minutes)
Detailed Schedule
Week at a Glance
Master Class Schedule
Start With the End in Mind: How To Submit Student Grades at the End of Semester in Banner (6 Minutes)
ITD-Classroom Services 4 PMU Faculty (1 Time for 1 Hr Long)
Two Groups - Male and Female (1 Hr Long)
Traditional 20 Minutes
Smart 20 Minutes
Enhanced 20 Minutes
Traditional Classrooms: 20 Mins
Instructor Work Station
Projector
Smart Board & Promethean Active Boards (Female)
Smart Classrooms: 20 Mins
Instructor Podiums
Projectors
Review After the Walk Through:
YouTube Playlist: Smart Classroom Basics at PMU
Google Presentation: Overview of Smart Classrooms at PMU
Enhanced Classrooms: 20 Mins
Instructor Podiums
Projectors

Video Conferencing
ITD-College Blackboard for Beginners
(ITD Will Be Doing 3 Times for 1 Hr)
ITD Will Be Doing Three Level I Sessions:
Getting and Setting Up
Accessing Url
Login
Changing password
Introduction to Syllabus, Hours, Assignments, Presentations
Later Topics Will Include:
Level II: Tracking Assignments & Grade Book
Level III: Assessments & Tests
Level IV: Working With Instructional Multimedia

Part 2: Conduct Faculty Survey.

DRAFT COMPLETED in October 2011 of IT Department Services at PMU Survey Instrument (Multiple Choice and Free From Responses). The following questions will be asked to ascertain satisfaction levels and to provide input for ongoing improvements in services delivered by ITD:

Academic Computer Services

1) I am kept well informed of IT matters important to faculty. [Code: ITD-1-001] Satisfaction Level

2) PMU provides adequate technology equipment and software needed to do my job well [Code: ITD-1-002] Satisfaction Level

3) Technology equipment in classrooms where I typically teach function adequately [Code: ITD -1-003] Satisfaction Level

4) I am satisfied with the response from the ITD when I need help [Code: ITD -1-004] Satisfaction Level

5) The IT system is up and running whenever I need it. [Code: ITD -1-005] Satisfaction Level

6) IT delivers promised services in a timely manner [Code: ITD -1-006] Satisfaction Level

7) IT Services helps you use technology effectively [Code: ITD -1-007] Satisfaction Level

8) The IT services as a whole are valuable to me. [Code: ITD -1-008] Satisfaction Level
Sub-Category [Edit] [Add Question] [Move/Copy Questions] [Archive Questions]

General Support

1) Ability to get through to a person [Code: ITD -2-001] Satisfaction Level

2) Timeliness of initial response to your inquiry [Code: ITD -2-002] Satisfaction Level

3) Ability to solve a problem [Code: ITD -2-003] Satisfaction Level

4) Turnaround time for resolving your problem [Code: ITD -2-004] Satisfaction Level

5) How satisfied are you with problem resolution overall? [Code: ITD -2-005] Satisfaction Level

6) Regarding the Help Desk -- How do you rate the timeliness in getting requests filled? [Code: ITD -2-006] Satisfaction Level

1) How satisfied are you with the SPEED of PMU Webmail? [Code: ITD -3-001] Satisfaction Level
2) How satisfied are you with the FEATURES of PMU Webmail? [Code: ITD -3-002] Satisfaction Level
3) How satisfied are you with the EASE OF USE of PMU Webmail? [Code: ITD -3-003] Satisfaction Level

4) How satisfied are you with the RELIABILITY of PMU Webmail? [Code: ITD -3-004] Satisfaction Level

5) How satisfied are you with the amount of email storage space provided at no charge by PMU? [Code: ITD -3-005] Satisfaction Level

6) How satisfied are you with PMU email overall? [Code: ITD -3-006] Satisfaction Level

Calendaring

1) How satisfied are you with how the calendar performs on your mobile device? [Code: ITD -4-001] Satisfaction Level
2) How satisfied are you with how the calendar performs for importing or combining calendars from different devices?
[Code: ITD -4-002]
Satisfaction Level

3) How satisfied are you with how the PMU calendar performs overall? [Code: ITD -4-003] Satisfaction Level

Mobile Devices

Admin Imports Setup Survey Reports Help Database

1) Which of the following mobile devices do you currently use or intend to use within the next six months for work or study? iPhone? [Code: ITD -5-001]
Usage in next 6 months

2) Use iPad? [Code: ITD -5-002] Usage in next 6 months

3) Use iPod Touch? [Code: ITD -5-003] Usage in next 6 months

4) Use a Blackberry? [Code: ITD -5-004] Usage in next 6 months

5) Use Android device? [Code: ITD -5-005] Usage in next 6 months

6) Use Palm OS device? [Code: ITD -5-006] Usage in next 6 months

7) Use other cell phone with internet access? [Code: ITD -5-007] Usage in next 6 months

8) How important is it to have the following available on your smart phone or other mobile device? Email? [Code: ITD-5-008]Importance Level

9) PMU Directory on Smart Phone? [Code: ITD -5-009] Importance Level

10) Smart Phone -- Class schedules? [Code: ITD -5-010] Importance Level

11) Smart phone - Calendar? [Code: ITD -5-011] Agreement Level

12) How satisfied are you with using the following via your mobile device? Email? [Code: ITD -5-012] Satisfaction Level

13) Mobile device -- calendar? [Code: ITD -5-013] Satisfaction Level

14) Mobile device for public PMU websites and applications? [Code: ITD -5-014] Satisfaction Level

15) Which applications, if any, would you like to be more mobile-friendly at PMU? [Code: ITD -5-015] Long Answer

Telephone Services

1) How satisfied are you with these aspects of PMU telephone services -- Placing an order? [Code: ITD -6-001]

Satisfaction Level

2) Order completion and delivery? [Code: ITD -6-002] Satisfaction Level

3) Problem resolution? [Code: ITD -6-003] Satisfaction Level

4) Voicemail? [Code: ITD -6-004] Satisfaction Level

5) How important would the following service and feature improvements be for your PMU work? Ability to schedule call forwarding of your PMU work number through a web interface? [Code: ITD -6-005]

Importance Level

6) Ability to set your office desk and cell telephones to ring simultaneously? [Code: ITD -6-006] Importance Level

7) Ability to set your office desk and cell telephones to ring sequentially? [Code: ITD -6-007] Importance Level

8) Delivery of voicemail messages and faxes to your email? [Code: ITD - 6-008] Importance Level

9) Ability to make or receive calls from your computer (Softphone)? [Code: ITD -6-009] Agreement Level

10) Ability to modify phone features through a web interface? [Code: ITD -6-010] Importance Level

11) How important will the following devices be to your work requirements within the next one to two years? [Code: ITD-6-011]

Importance Level

12) Importance of a WiFi VoIP phone that works only on campus? [Code: ITD -6-012] Importance Level

13) Importance of a cell phone used only for telephone calls? [Code: ITD -6-013] Importance Level

14) Importance of a Smart Phone (eg. iPhone, Blackberry, Android,Windows Mobile Device etc.? [Code: ITD -6-014] Agreement Level

15) Importance of a Tablet Device (eg. Galaxy or iPad)? [Code: ITD -6-015] Importance Level

IT Services Priorities

1) Email [Code: ITD -7-001] Service Providers
2) Email lists/group discussions [Code: ITD -7-002] Service Providers
3) Calendaring (for your own calendar) [Code: ITD -7-003] Service Providers
4) Meeting/event scheduling with others [Code: ITD -7-004] Service Providers
5) Document sharing [Code: ITD -7-005] Service Providers
6) Instant Messaging [Code: ITD -7-006] Service Providers
7) Video storage/sharing [Code: ITD -7-007] Service Providers
8) Image storage/sharing [Code: ITD -7-008] Service Providers
9) Websites, blogs, wikis [Code: ITD -7-009] Service Providers
10) Of the external providers you use, which do you prefer? [Code: ITD -7-010] Service Providers
11) If there were a contract in place with PMU and Google or Microsoft that safeguarded your privacy and intellectual property, which one would you feel most comfortable using? [Code: ITD -7-011]

Service Providers
Remote Access

1) If you use PMU's VPN, SSL or client-based services for remote access,how satisfied are you with your ability to connectto them to get access to such things as your calendar or PMU folder? [Code: ITD -8-001] Satisfaction Level

Security

1) Anti-virus/anti-spyware software is set to update itself automatically. [Code: ITD -9-001] Likelihood
2) Anti-virus/anti-spyware scanning of your hard disks is turned on [Code: ITD -9-002] Likelihood
3) Operating system updates are installed automatically. [Code: ITD -9-003] Likelihood
4) Application sofware updates (such as MS Office) are installed when available. [Code: ITD -9-004] Likelihood
5) Passwords changed every six months. [Code: ITD -9-005] Likelihood
6) Password is required to start/wakeup computer. [Code: ITD -9-006] Likelihood
7) Passwords include random combinations of letters and numerals. [Code: ITD -9-007] Likelihood
8) Hand-held devices such as iPhones will require a password. [Code: ITD -9-008] Likelihood
Sub-Category [Edit] [Add Question] [Move/Copy Questions] [Archive Questions]

Final Questions

1) What is one think IT Services could do that would make it easier for you to work or study? [Code: ITD -10-001] Long Answer
2) What are the two or three most important services IT Services provides you? [Code: ITD -10-002] Long Answer
3) What is one thing IT Services could do to improve the way it communicates about its services? [Code: ITD -10-003] Long Answer
4) Any added comments you may have for IT Services [Code: ITD -10-004] Long Answer

Part 3: Work with Learning Resource Center to establish faculty forum for education equipment and software suggestions, input, and discussion.

CIO and Team Lead of MIS to finalize faculty satisfaction survey not later than October 26, 2011.

CIO to coordinate with Director of LRC and College Deans not later than March 31, 2012.

Section 7.4

Information Technology

Computing equipment and software and related support services must be adequate for the program and managed in ways that ensure secure, efficient and effective utilization.

7.4.1 Computing equipment is available and accessible for faculty, staff and students and the adequacy of this provision is regularly assessed.

STAR: 4

Strengths:

In order to ensure that computing equipment is available and accessible for faculty, staff and students and the adequacy of this provision is regularly assessed, ITD produces and maintain**s a** Weekly ITD Classroom and Labs Report. This live on-line reporting system allows for the linkage of purchasing requests and the on-going updating of repair status. Artifact of this live process are extracted as example here:

- P.O. #08-Y11-0329-ITIS
- P.O. #09-Y11-0394-ITIS

Opportunities for improvement:

Deployment of Banner Electronic purchasing module will enable us to move from 4 to 5.

Action Plan:

N/A

PMU IT Facilities Weekly Inspection Report - Latest Updates - PMU AV SYSTEM INSPECTION

	LOCATION	SYSTEM DESCRIPTION	STATUS	PLAN OF CORRECTIVE ACTION	HELPDESK TICKET #	Person to Whom Ticket is Assigned	Update Remarks
1	AUDITORIUM	**Lighting system**	spot lights failiar	Follow up with Engineering Dep.	12998		
			busted moving head .1unit	Follow up with Engineering Dep.	12999		
			one bulb of wall lights doesn't work				
			All other lights working fine				
		Audio System	Works fine				
		Video System	indoor camera no:2+4 need Brackets to give full coverage, also camera 5 ,4 Fiber connector need to re termination.	- we contact with a Fiber network company to solve the problem ,waiting for approval regards PMU prosdure .			
			-	RFQ (Brackets) has been set waiting for approval			
		Digital Signage System	working fine				
			Busted Moving Head Spotlight. 1 pc.	for replacement of busted Moving headlights	12999	AV Team	As per Eng'g Dept. They're still waiting for the scaffolding to erect inside the auditorium for replacement of busted lights. update 10/23/11 updated by francis labnao
			Busted Moving Head Washlight. 3 pcs.	for replacement of busted Moving washlights	13000	AV Team	As per Eng'g Dept. They're still waiting for the scaffolding to erect inside the auditorium for replacement of busted lights. update 10/23/11 updated by francis labnao
		Lighting System	Busted Par 54 Spot lights. 16 pcs	for replacement of busted Par 54 Spot lights.	12998	AV Team	As per Eng'g Dept. They're still waiting for the scaffolding to erect inside the auditorium for replacement of busted lights. update 10/23/11 updated by francis labnao
		Public Address and Paging System	Installation of some speakers and cabling were still not yet done by the contractor	To follow up to the contractor.	13006		
		Translation	Working fine				
		Panel Desk Discussion	Working fine				
		Panel Discussion (VIP chair mic's)	Working fine				
		Wired and wireless Mic's	Working fine				
		Video Conferencing	Working fine				
		Video Presentation	Working fine				
		Live event video streaming	Working fine				
		Control System	Working fine				
2	MALE LECTURE HALL	Audio Visual System with Video Conferencing	AV System are working fine but the Control room AC doesn't work for almost a month now.	Already reported to Engg. Dept. to this issue.	13039	AV Team	Still waiting the purchasing dept for the spare part of AC Compressor. 10/23/11
3	FEMALE LECTURE HALL	Audio Visual System with Video Conferencing	Busted Projector Lamp	RFQ for the Busted lamp	13001	AV Team	Pending from the purchasing department.
			Working fine				
4	Dr. Issa's OFFICE	Audio Visual System with Video Conferencing	Working fine				
5	Dr. Issa's Conference Room	Audio Visual System with Video Conferencing	Working fine				
6	Admin bldg VIP Room	Audio Visual with Video Conferencing	Touch Panel doesn't work	To follow up to the contractor. c/o ENPRO	13002	AV Team	
		Discussion System	Working fine				
7	Data Center	Digital Signage	Working fine				
8	Data Center	MATV Live Video Streaming	Working fine				
9	Vice Rector Conference Room	Audio Visual System with Video Conferencing	Working fine				
10	Admin Building	CCTV System	Server at the admin building are working fine. 6 camera outside admin bldg doesn't work due to power problem.	To check by Vendor (ENPRO) for their outside camera.	13003	AV Team	As per ATCO there's a power going to the parking cctv camera. Already coordinated to ENPRO regarding this issue. update by francis labnao 10/15/12 @ 10am
11	Main Campus	CCTV System	All camera are already installed but some cameras are not working due to unavailability of network switches and patch panel in the warehouse and chiller plant communication rooms.	Working on progress RFQ-IT-2011-PCNC9S	13005	AV Team	
			Working fine				
12	Main Cafeteria	Audio Visual System	Working fine				
		MATV System	Satellite signal doesn't work	For re-allignment of satellite dish			Already informed/email to vendor (ENPRO) send their technical team to fix satellite dish. updated by. francis labnao 11/15/12 @ 10am
13	Sport Center	Audio System	Working fine				
14	Mosque	Audio System	Working fine				
15	LRC EMBA Rm.	Audio Visual System	Working fine				

PMU IT Facilities Weekly Inspection Report - Latest Updates - Male A Wing

	Wing	Room Type Code	Room No.	Type Of Room	Status	Plan of Corrective Action	Help Desk Ticket	Person to Whom Ticket is Assigned	Updated Remarks
1	A	A	G053	Eng. Lab	Robotel Hubs Not Working - DynEd Only Works in Internet Mode				
2	A	LAB	G055	Eng. Lab	Robotel Hubs Not Works - DynEd Only Working in Internet Mode				
5	A	T.C.	F139	Student Club	Desktop PC is up and running, but Projector needs better cable	Change the VGA cable to EXTRON's cable		AV Team (pending with purchasing Dept.)	
4	A	T.C.	F138	Student Support Center	Configured with New Standard Desktop Image, tested and working fine.				
3	A	SCR	G056	Smart classroom with Video Conf.	Working Fine				
6	A	T.C.	F140	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
7	A	T.C.	F141	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
8	A	T.C.	F142	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
9	A	T.C.	F143	Traditional Classroom	Desktop PC is up and running, but projector lamp needs replacement	P.O. #08-Y11-0329-IT	11943	AV Team (pending with purchasing Dept.)	updated as of 9-28 @ 3:00 PM by Mr. Garret & Mr. Mario
10	A	T.C.	F144	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
11	A	T.C.	F145	Traditional Classroom	Desktop PC is up and running, but projector lamp needs replacement	P.O. #08-Y11-0329-IT	11944	AV Team (pending with purchasing Dept.)	updated as of 9-28 @ 3:00 PM by Mr. Garret & Mr. Mario
12	A	T.C.	F146	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
13	A	T.C.	F147	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
14	A	T.C.	S134	Traditional Classroom	Desktop PC is up and running, but Projector needs better cable		11950	AV Team (pending with purchasing Dept.)	
15	A	T.C.	S135	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
16	A	T.C.	S136	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
17	A	T.C.	S137	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
18	A	T.C.	S138	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
19	A	T.C.	S139	Traditional Classroom	Desk top running but need beter cable	Change the VGA cable to EXTRON's cable	11946	AV Team (pending with purchasing Dept.)	
20	A	T.C.	S140	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
21	A	T.C.	S141	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
22	A	T.C.	S142	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.	Smart Board Needs Cleaning (Report to Auxiliary Services Dept.)			
23	A	T.C.	S143	Traditional Classroom	Desktop PC is up and running, but projector lamp needs replacement	P.O. #08-Y11-0329-IT	11945	AV Team (pending with purchasing Dept.)	updated as of 9-28 @ 3:00 PM by Mr. Garret & Mr. Mario
					Prepared By : Omar Ghuweir				

PMU IT Facilities Weekly Inspection Report - Latest Updates - Male B Wing (SABIC 1st Fl)

No.	Wing	Alias	Room No.	Type Of Room	Status	Plan of Corrective Action	Help Desk Ticket	Person to Whom Ticket is Assigned	Updated Remark
1	B	SCR	G038	Smart Classroom	Working Fine				
2	B	LAB	G039	Chemistry LAB	Working Fine				
3	B	SCR	G040	Smart Classroom	Working Fine				
4	B	SCR	G041	Smart Classroom	Working Fine				
5	B	LAB	G042	Math LAB	Working Fine				
6	B	LAB	G043	Physical LAB	PC, Projector and Smartboard installed				Installed New Optiplex 790 desktop. Win Xp configuration in progress. Updated by Garret as of Oct. 18, 2011 @ 12:00 NN
7	B	LAB	F148	Eng. LAB	Configured with New Standard Desktop Image, tested and working fine.				Configured additional Optiplex 790 Desktop with Win XP SP3. Tested and working fine. Updated as of oct-17, 2011 @ 3:00 PM by Garret . From 16, now we have a total of 18 PCs in this lab including the instructor's PC.
8	B	LAB	F149	E-Portfolio	Configured with New Standard Desktop Image, tested and working fine.				Configured additional Optiplex 790 Desktop with Win XP SP3. Installed, Tested and working fine. Updated as of oct-17, 2011 @ 3:00 PM by Garret . From 16, now we have a total of 17 PCs in this lab including the instructor's PC.
9	B	T.C.	F150	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
10	B	LAB	F151	Micro Stodio for E-Portfolio	Desktop PC configured, Audio, Video, Lighting Set up & Visual Communicator software set up and configuration completed, tested and working fine.				
11	B	T.C.	F152	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
12	B	T.C.	F153	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
13	B	T.C.	F154	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
14	B	T.C.	F155	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
15	B	T.C.	F156	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
16	B	T.C.	F157	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
17	B	LAB	S144	LAB	Configured with New Standard Desktop Image, tested and working fine.				
18	B	T.C.	S145	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
19	B	T.C.	S146	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
20	B	T.C.	S147	Traditional Classroom	Working fine	Already replaced the projector from Omar's office and New Lamp		AV Team (Done)	Updated as of 10-23 @ 12:30 PM by Francis Labnao
21	B	T.C.	S148	Traditional Classroom	Working fine	Already replaced the projector from Omar's office and New Lamp	11953	AV Team (Done)	Updated as of 10-23 @ 12:30 PM by Francis Labnao
22	B	T.C.	S149	Traditional Classroom	Working fine	Already replaced the projector from Omar's office and New Lamp	11954	AV Team (Done)	Updated as of 10-23 @ 12:30 PM by Francis Labnao
23	B	T.C.	S150	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
24	B	T.C.	S151	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
25	B	T.C.	S152	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.	Already replaced the busted lamp to a new lamp.	11955	AV Team (pending with purchasing Dept.)	updated as of 10-24 @ 11:23 AM by Francis Labnao

PMU IT Facilities Weekly Inspection Report - Latest Updates - Male C Wing

No.	Wing	Alias	Room No.	Type Of Room	Status	Plan of Corrective Action	Help Desk Ticket	Person to Whom Ticket is Assigned	Updated Remark
1	C	T.C.	G026	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
2	C	T.C.	G027	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
3	C	SCR	G028	Smart CR \ W V.C.	Working Fine				
4	C	T.C.	G029	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
5	C	LAB	G030	Writing Lab Lab	All 7 PC's were Configured with New Standard Desktop Image, tested and working fine.				
6	C	T.C.	G031	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
7	C	T.C.	G032	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
8	C	T.C.	G033	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
9	C	T.C.	G034	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
10	C	LAB	F086	Computer Lab	Working Fine	Already replaced the busted projector lamp VT 85LP	# 12604	Francis	updated as of 10-22 @ 2:300 PM by Francis Labnao
11	C	T.C.	F087	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
12	C	T.C.	F088	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
13	C	SCR	F089	Smart CR	Working Fine				
14	C	T.C.	F090	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
15	C	SCR	F091	Smart CR	Working fine				
16	C	SCR	F092	Smart CR	Working Fine				
17	C	LAB	S084	Lab	Working Fine				
18	C	T.C.	S085	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
19	C	T.C.	S086	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
20	C	LAB	S087	Lab	Working Fine				
21	C	T.C.	S088	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
22	C	LAB	S089	Lab.	Working Fine				
23	C	SCR	S090	Smart CR	Working Fine				

PMU IT Facilities Weekly Inspection Report - Latest Updates - Male D Wing

No.	Wing	Room No.	Type Of Room	Status	Plan of Corrective Action	Help Desk Ticket	Person to Whom Ticket is Assigned	Updated Remark
1	D	G017	Traditional Classroom	No Projector, Configured with New Standard Desktop Image, tested and working fine.	P.O. #08-Y11-0329-IT	12142	AV Team (pending with purchasing Dept.)	updated as of 9-28 @ 3:00 PM by Mr. Garret & Mr. Mario
2	D	G018	Smart CR	No projection screen – (Being utilized as Temporary storage of Maintenance Dept)	Need to install projection screen	12143	AV Team (pending with purchasing Dept.)	
3	D	G019	Circuit Lab	Working Fine				
4	D	G020	Physics LAB	Working Fine				
5	D	G021	Physics LAB	Working Fine				
6	D	G022	Smart Classroom	No Projection Screen – (Being utilized as Temporary Bookstore storage)	Need to install projection screen	12144	AV Team (pending with purchasing Dept.)	
7	D	F058	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
8	D	F059	Smart CR	MatLab - COE – up and running. Projector not working		13408		Replaced busted Infocus lamp. Updated as of Oct. 31, 2011 @ 11: 00am by Francis Labnao
9	D	F060	Smart CR	Labview Academy – COE – up and running				
10	D	F061	Signal Processing LAB	COE – Up and running				
11	D	F062	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
12	D	F063	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
13	D	F064	Vacant LAB	Pc, projector and Smartboard installed	Win XP configuration in progress			Installed New Desktop and Win XP Configuration in progress. Updated as of Oct. 18, 2011 @ 12:00 NN by Garret
14	D	S053	Robotics LAB	Working Fine				
15	D	S054	Smart CR	Working Fine				
16	D	S055	Traditional Classroom	PC and Projector installed	Need to install Smartboard			Installed New Desktop and Win XP Configuration in progress. Updated as of Oct 18, 2011 @ 12:00 NN by Garret
17	D	S056	Mechanics LAB	Working Fine				
18	D	S057	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
19	D	S058	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.				
20	D	S059	Embedded Systems Lab	Working Fine				

PMU IT Facilities Weekly Inspection Report - Latest Updates - Male E Wing

No.	Wing	Room No.	Type Of Room	Status	Plan of Corrective Action	Help Desk Ticket	Card Read Status		Updated Remark
1	E	G010	STC	OK					
2	E	G011	Datacenter	OK					
3	E	G012	Technical Support Office	OK					
4	E	G013	Purchasing Dept Office	OK					
5	E	G014	ATCO Office	OK			Yes	No	
6	E	G015	Utility – Storage	Ok					
7	E	F051	Traditional Classroom	Only was Smart Board Installed	ROOM BEING UTILIZED AS STORAGE BY MAINTENANCE DEPARTMENT				
8	E	F052	Traditional Classroom	College of Engineering , Support Center- OK					
9	E	F053	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.Projector not working.	Defective Projector was removed and need to replace the new one	13408			Replaced new NEC projector.. Updated as of Oct. 31, 2012 @ 11: 00am by Francis Labnao
10	E	F054	SUN LAB	Working Fine					
11	E	F055	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.					
12	E	F056	Smart Classroom	Configured with New Standard Desktop Image, tested and working fine.					
13	E	F057	Comp Lab (Thin Client)	Configured with New Standard Desktop Image, tested and working fine.					
14	E	S046	VACANT Lab	PC, Projector and Smartboard installed	Win XP configuration on progress				Installed New Desktop and Win XP Configuration in progress. Updated as of Oct. 18, 2011 @ 12:00 NN by Garret
15	E	S047	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.					
16	E	S048	Traditional Classroom	Working Fine	Already replaced the projector and New lamp.				Updated as of 10-22 @ 8:30 PM by Mr. Francis Labnao
17	E	S049	Networking Lab	Working Fine					
18	E	S050	Traditional Classroom	Configured with New Standard Desktop Image, tested and working fine.					
19	E	S051	Smart CR,General Purpose Lab	Working Fine					
20	E	S052	Traditional Classroom	Only PC & projector was installed	Need to install Smartboard. Win Xp configuration on progress				Installed New Desktop and Win XP Configuration in progress. Updated as of Oct. 18, 2011 @ 12:00 NN by Garret

Section 7.4.2

Institutional policies governing the use of personal computers by students are complied with

STAR: 4

Strengths:

Through the application of IT Dept. Policies, ITD ensures that personal computer usage by students is governed by institutional policy. Periodic audits are used to document compliance.

Opportunities for improvement:

Provide documentation of on-going system of compliance audits in order to generate/ demonstrate on-going feedback loop for continuous improvement.

Action Plan:

Initial audit documentation to be provided not later than 31 January 2012.

جامعة الأمير محمد بن فهد

PRINCE MOHAMMAD BIN FAHD UNIVERSITY

Information Technology Policies

Prince Mohammad Bin Fahd University
Al Khobar, Saudi Arabia

Last Updated: November 12, 2011

PMU IT Policies Index

Policy 01: Customer Support

Customer Support Policy Statement

The Information Technology resources and services of Prince Mohammed Bin Fahd University are provided for the advancement of the University's educational, research, and service objectives. They are offered primarily to facilitate the University's academic and business purposes.

University Service Desk

To ensure support for all students, faculty and staff members, ITD has established a customer service desk commonly known as helpdesk. In order to help our customers, ITD provides a service desk (Helpdesk) software package to track and trace all IT and facilities issues to successful resolution and ensure customer satisfaction. Requests for the provisioning of new services are also handled by service desk.

IT Equipment Refresh

Personal computers in labs and classrooms, as well as faculty computers, are on a 3-5 year replacement cycle.

Applicability

IT Policies are applicable to all students and employees (faculty, administrators, and staff) and any others who are extended the privilege of using IT resources and services for the purpose of achieving the educational objectives of PMU and its students. All such persons accessing and using IT resources and services are subject to the applicable provisions of the University Statutes, University Code of Conduct, and Handbook for Administrators, Student Handbooks, and all other policies and procedures established by administrative offices of PMU.

Policy 02: Acceptable Use

Introduction

This Functional Policy covers the responsibilities for users at PMU. PMU will take reasonable precautions to ensure that the University complies with Saudi Arabian laws where applicable and where such laws exist.

It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.
Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as network link
- All management information systems
- All business activities supported by ITD Group.
- All of the above are either owned or leased by the ITD Group and under the PMU-ITD possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy,

and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy Statements govern the Responsibilities for Users Functional Policies listed in this document:

- All relevant statutory, regulatory and contractual requirements must be explicitly defined by the HR Department and technical requirements must be explicitly defined and documented by PMU for each information system.
- Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products;
- Important records of PMU must be protected from loss, destruction and falsification;
- Controls must be applied to protect staff personal information in accordance with relevant legislation;
- Management must authorize the use of information processing facilities and controls must be applied to prevent the misuse of such facilities;
- Controls must be in place to ensure compliance of Information systems with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls. This must be regularly reviewed;
- Where action against a person or organisation involves the law, either civil or criminal, the evidence presented must conform to the rules for evidence laid down in the relevant law;
- This must include compliance with any published functional policy or code of practice for the production of admissible evidence.

Use of the Internet/Intranet – Internet Crime

Current Legislation

The Saudi Arabian Communications and Information Technology Commission announced the issuance of e-crimes and e-transaction acts, Both acts were issued on 27’th of March, 2007. E-crimes act was issued to combat information

electronic crimes, by defining those crimes and penalties upon them. E-transactions act was issued to regulate electronic transactions and electronic signatures in a policy frame work, and combat any misuse of them by defining responsibilities, and penalties.

University Directive

All users must comply with the following functional policies:

Internet/Intranet Functional Policy

Hacking and Cracking into Computer systems

- No employees will participate or be party to any kinds of hacking or cracking into computer systems.
- No user is allowed to gain access to PMU computer networks and systems without prior permission from the designated authority within PMU.
- No vendor or third party is permitted to perform penetration testing on any of PMU systems and network without written approval from PMU.
- All users are allowed to perform only authorized transactions on PMU systems and the Internet/Intranet.

Creating and distribution of Malicious (dangerous) code

Dangerous code can be classified as any computer program (code) that causes destruction or harm to a computer system.

- All users must ensure they have Anti-virus software enabled on their computers. If in doubt, user should contact ITD.
- It is the users responsibility to check all external material for viruses – this includes e-mails with attachments and disks from external sources.
- It is prohibited for employees to create and distribute dangerous code – of any form within PMU and associated parties.

Internet Fraud

- Users are not permitted to use the PMU network or computer systems to perform a transaction they are not authorized to perform.
- All transactions will be logged and will be used in the event of any illegal misconduct.
- All users must always represent themselves as themselves when communicating and operating on PMU systems and network. Misrepresenting yourself is classified as a fraudulent event.
- Users are not allowed to create personal web pages using PMU facilities (systems, network or computers).
- Users must report suspected fraud to PMU\ITD immediately – this can be done anonymously.
- Users are not permitted to operate an independent web page – running an online business for personal gain is forbidden using PMU facilities .

Theft of Information

- Users must only access information which they have authorized access to.
- No information is allowed to be given to an external party unless written permission is given by PMU management.
- All information created and used in the course of the users employment remains the sole property of PMU.
- Theft of information includes the copying of software and using it without a legal license.
- This is forbidden at PMU and can be classified as a serious act of misconduct within the organization.
- All users of software must strictly abide by copyright laws and restrictions detailed by the software manufacturer. Users must not copy software from the Internet. This includes the use of freeware and shareware (certain terms and conditions normally apply). All users must contact PMU\ITD if such software is required to perform their job.

Use of Electronic Mail (e-mail)

Electronic Mail (E-mail) Functional Policy

E-mail Content

- Unacceptable e-mail content must not be acquired, possessed, sent

or shown to other employees. For definition of Unacceptable e-mail, refer to the “Expressly Prohibited Use” section in the Electronic Mail Usage Functional Policy document.

- If users are found creating, reading or distributing such mail, they will be penalized accordingly. Refer to section 9 of this document for penalties.
- All e-mail attachments must be scanned for viruses.
- Misrepresentation of one self is prohibited within PMU– employees should always represent themselves as they are.

Representing PMU

- The use of email to create contracts for and on behalf of PMU is strictly prohibited. PMU Management or the HR Department of PMU must approve all contracts.
- E-mails must not contain any information, views or opinions of the employee's that could create a negative corporate image for PMU.
- All employees have a disclaimer attached to each e-mail. This disclaimer must expressly disclaim the employee's authority to act for or bind the employer.

Defamation

Defamation is defined as "The unprivileged publication of a statement which exposes a person to contempt, hatred, ridicule or obloquy". Defamation usually consists of written or spoken works but can also include graphics – cartoons or pictures, voice or video conferencing facilities where word is not used.

- Defamation of any person, whether they are employed by PMU or not, is strictly prohibited. This includes written, spoken or graphically representation – unacceptable e-mail content.
- Defamation will lead to a severe disciplinary action.

Copyright

Current Legislation

- In Saudi Arabia, copyright protection is afforded solely under the Copyright Act. The Copyright Act recognizes the following types of work, which are eligible for protection:
    - Literary, musical and artistic work;

- Sound recordings, cinematographic films, sound and television broadcasts and programme-carrying signals;
- Published editions; and
- Computer Programs.

- Computer databases (tables and the data) are protected as literary works.
- Internet web sites are multimedia products containing written texts, photographs, pictures, etc. and all should be assumed a copyright. Web sites can also be seen as computer programs.
- Infringement of the Copyright Act falls into the following categories:
    - Infringement by reproduction;
    - Infringement by publication;
    - Infringement by public performance;

Software Management Functional Policy

Software Copyright

- All users must be aware of and understand the software copyright and acquisition standards, and non-compliance to the software and standards will cause PMU to take the required disciplinary action against staff who breach them.
- PMU must maintain proof and evidence of ownership of licenses, master disks, policy's, etc.
- PMU must implement controls to ensure that any maximum number of users permitted is not exceeded.
- All users must comply with the terms and conditions for software and information obtained from the networks.
- All employees must conform to the Copyright Act as described above.
- Employees are not permitted to load an illegal copy of software on any PMU computer or related facilities.
- The viewing, discussion or distribution of pornography material either by using the facilities of PMU, being on or off the University premises, or during work hours is forbidden.
- PMU will monitor Internet web site access and logs will be maintained for 3 months.

Safeguarding of Organizational Records

- Important records of organization are protected against loss, destruction and falsification.
- Some records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Examples of this are records, which may include evidence that PMU

operates within statutory or regulatory rules, or to confirm the financial status of an organization with respect to shareholders, partners and auditors.

- The time period and data content for national law or regulation may set information retention.
- Records are categorized into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details.
- Consideration are given to the possibility of degradation of media used for storage of records.
- Storage and handling procedures are implemented in accordance with manufacturer's recommendations.
- Data storage systems are chosen such that required data can be retrieved in a manner acceptable to a court of law, e.g. all records required can be retrieved in an acceptable time frame and in an acceptable format.
- The system of storage and handling is ensure clear identification of records and of their statutory or regulatory retention period.
- To meet these obligations, the following steps are in process:
    - Guidelines on the retention, storage, handling and disposal of records and information;
    - A retention schedule identifying essential record types and the period of time for which they retained;
    - An inventory of sources of key information and
    - Appropriate controls to protect essential records and information from loss, destruction and falsification.

Penalties

Depending on the number of offenses made and on the severity of the offense or non-compliance with the provisions covered in this document, the corresponding penalty will be applied at the discretion of the PMU Rector based on the University's By-Laws and Procedures

Internet and Intranet usage

Introduction

This Functional Policy covers PMU's Internet and Intranet usage.
Communications and operational management of information resources and systems are essential to maintaining a high level of service to PMU clients and customers. Therefore, security requirements will be developed and implemented to maintain control over communications and operations
It is each user's responsibility and obligation to ensure that all IT resources

are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU

All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Computer, Network and Telephone Usage Functional Policies:

- Independent review of information security in the organisation must be done on a regular basis;
- The security requirements of an organisation outsourcing the management

and control of all or some of PMU's information systems, networks and/or desktop environments must be addressed in a contract agreed between the parties;

- Relevant information security roles and responsibilities must be documented in job definitions where appropriate;
- All Employees and third parties such as contractors, consultants, business partners and outsourced staff must sign a confidentiality agreement as part of their initial terms and conditions of employment;
- Aspects related to information security must be addressed in the Organization's standard employee's terms and conditions of employment and for third parties, with a formal contract with the PMU;
- Users of information services must be required to note and report any observed or suspected security weaknesses in or threats to systems or services;
- The violation of organisational security policies, functional policies and procedures by employees must be dealt with through a formal disciplinary process;
- Capacity demands must be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage is available;
- ITD must implement detection and preventive controls to protect information and information processing facilities against malicious software and appropriate user awareness procedures;
- Authorized PMU employees must be provided with Internet access for academic and business use;
- Content scanning must only be enforced in checking for malicious software, viruses, etc.;
- Functional policies for the use of the Internet and intranet must be implemented and controls put in place to reduce security risks created by the Internet and intranet usage;
- The implementation of the E-mail, Internet and Intranet policy is aimed at ensuring that all employees and independent contractors are made aware of the disciplinary sanctions that PMU must impose on any unauthorised and/or unacceptable use of these services;
- Employees of and independent contractors to PMU are specifically warned that personal criminal and/or civil action may be taken by PMU in the event of their breach of this policy;
- The allocation of passwords must be controlled through a formal management process;
- An intrusion detection system must be in place to detect unauthorised use of PMU networks;

All users must have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual.

Internet and Intranet Usage Functional Policies

- Access to the Internet: Access to the Internet is provided to all employees and students. Guests of the university will be provided Internet access at the discretion of the university.
- Acceptable and Unacceptable Use of the Internet/Intranet
- In an open plan office users must be aware of unauthorized users reading information displayed on their screen.

University Use

PMU sees the Internet/Intranet as significant tools for business benefit and for achieving required business objectives, i.e. The Internet can be used to access a wealth of information and resources, while the Intranet is one of the most effective ways of making PMU information available internally to the organization.

These services do however offer the opportunity for abuse of resources and inappropriate use of these mediums could expose PMU to significant risks. Therefore Internet/Intranet facilities will only be available to users after formal contracting of the Internet/Intranet functional policy. Any exceptions will be filed.

- Unauthorized attempts to break into any computer;
- Theft or copying of electronic files without permission; and
- Sending or posting company files outside the company or inside the company to unauthorized personnel.

Personal Use

PMU understands that many users work at non-traditional times, for example outside working hours and that these activities infringe on “personal time”. PMU therefore allows incidental and infrequent personal use of the Internet/Intranet within the Constraints on Personal Use noted below.

Constraints on Personal Use

Incidental and infrequent personal use of PMU's Internet/Intranet during or outside normal work hours are allowed on condition that:

- It does not consume significant amounts of the user’s workday.
- It does not consume substantial amounts of PMU bandwidth in such a way

that it negatively impacts upon PMU systems, either directly or indirectly. PMU bandwidth could be impacted by distribution of for example the following:

    - Attachment types such as JPEG, JPG, AVI, etc; or
    - Chain letters, jokes, bitmaps, etc.
- It does not expose PMU to a noticeable increase in costs.
- It does not expose PMU to reputation or financial risks.

Expressly Prohibited Use

In order to prevent loss and the possibility of PMU being in violation of regulatory and statutory requirements the following Internet/Intranet related activities are prohibited within PMU:

- Carrying of any obscene, defamatory or discriminatory material.
- Material containing derogatory racial, gender, religious or hate-oriented comments;
- Libelous remarks about products or other companies,
- Defamatory remarks, including defamation of character; or
- Discriminatory language or remarks that would constitute harassment of any type.

Password Management

Internet/Intranet access to General Support systems and Public data shall require a password. All password creation and usage must be in accordance with those stated in
PMU General Security Guidelines Functional Policy.

Downloading content

Users are permitted to download content from the Internet/Intranet. The downloading of content from the Internet/Intranet must however be in accordance with the following:

- Users downloading large volumes should consider scheduling these for transmission after normal working hours.
- When non-text files (databases, software object code, spreadsheets, formatted word-processing package files, etc.) are downloaded from non-PMU sources via the Internet, the following conditions must be adhered to:

- Files must be screened with approved virus detection software prior to being used (opened);
- Whenever an external provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed up. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine;
- Downloaded files must be decrypted and decompressed before being screened for viruses;
- The use of digital signatures to verify that unauthorized parties have not altered a file is recommended, but this does not assure freedom from viruses.

Representing PMU

Vicarious Liability:

Users must be aware that in using PMU Internet/Intranet facilities they are representing PMU. It is therefore important that the use of Internet/Intranet must be in accordance with the following:

- Users should consciously build and preserve PMU image when using the Internet/Intranet.
- Users may indicate their affiliation with PMU in mailing lists (list servers), chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an electronic mail address. In either case, whenever users provide an affiliation, they must also clearly indicate the opinions expressed are their own, and not necessarily those of PMU.
- Users can indicate that opinions expressed are their own by the use of a disclaimer stating the following:
  "Any opinions, presented explicitly or implied, are solely those of the author's and do not necessarily represent those of the Organization's."

Information Protection

In this subsection, “proprietary information” refers to information that is “confidential” and/or “critical”.

As information is very valuable to PMU, users should observe the following before considering sending information over the Internet:

- Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, PMU proprietary information must not be sent over the Internet unless it has first been encrypted by approved methods.
- User IDs and passwords, and other parameters that can be used to gain access to PMU information must not be sent over the Internet in readable form.
- PMU software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-PMU party for any purposes other than business purposes expressly authorized by management.
- Users should not allow others to use their user IDs and passwords when connecting to Internet sites requiring authentication (e.g. Gartner research database). If a user has no option but to allow this, the user must understand that he/she is the responsible party.

Expectation of Privacy

- Individual Practices: On the Web, one of the real dangers is a possible loss of privacy or leakage of information about user activities. Employees should be aware of the following issues relating to their privacy when surfing the web:
- When you visit a Web site, the site you are visiting can identify where your Internet connection originates. For example, if you use the Web from work, your activities can be identified as coming from PMU.
- Web sites can log all of your activity including any personal data you provide. The web site owner can associate you with this data on future visits. They may want to use this information to give you a better web experience, or they may be collecting competitive information, or both. Some web sites do not respect data privacy laws and may make the information collected from you available to other organizations. Should any of the events mentioned takes place, the Legal Department must be informed immediately.
- PMU Practices: The Internet connection provided to employees is a PMU resource. Activities may be subject to monitoring, recording, and periodic audits to ensure they are functioning properly and to protect against unauthorized use. Users must therefore note the following:

- PMU reserves the right to monitor sites (e.g. duration and content) visited by users and to detect security violations.
- PMU reserves the right to examine and access all information, created, stored or communicated using PMU information systems whenever warranted by business need or requirements.
- PMU will disclose information obtained through such examinations to appropriate third parties, including law enforcement agencies.
- Internet users expressly consent to such monitoring, recording and examination.

Internet Integrity

When using the Internet all users must comply with the following:

- All information taken off the Internet should be considered suspect until confirmed by separate information from another source.
- Before users release any internal PMU information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed.

Electronic Fraud

- Impersonation: Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any PMU electronic communications system is forbidden.
- Disclaimer of Liability: PMU is not responsible for material viewed or downloaded by users from the Internet or other public communications networks. Users are cautioned that web pages may include offensive, sexually explicit, and/or other inappropriate material. Users accessing the Internet and other public communications networks do so at their own risk.

General Information on Wireless Networks:

- Wireless Networking now provides easy, Inexpensive, high bandwidth network services for any organizations which selects this Latest Network technology.
- Approved by IEEE Standards committee the 802.11 further enhanced to 802.11b/g/n specification detailed the frame work necessary for a standard method of wireless network communication.
- Connectivity previously had to creep up with the monopoly held" Wires" ,now the data can Fly thru the walls ,significantly increasing the Network Bandwidth & Performance.
- A recent survey by a leading Security Consulting Company has

reveled that Wireless Networking has indeed increased in the current technology Savvy market by 30% and Wireless Networking is the Future Networking.But as Every Technology has it’s own loopholes , Security is a real cause of Concern for Wireless networks,.

- Access Points communicate with the data freely flowing in the Air vulnerable to penetrate by any unauthorized user.
- Placement of the access points is equally important , As you do your site survey for access point deployment, think about locating the access points toward the center of your building rather than near the windows. Plan your coverage to radiate out to the windows, but not beyond. If the access points are located near the windows, a stronger signal will be radiated outside your building making it easier for people to find you.

Introduction

This functional policy covers PMU's Computer, telephone and network, Mobiles usage. In today's business environment,. Therefore, proper use and protection of PMU resources and information is essential for business operations.

It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All business activities supported by PMU.

All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Computer, Network and Telephone Usage Functional Policies listed in this document:

- Both the wired and wireless networks will be monitored for unauthorized use or devices.

Wireless Network (Wi-Fi) Functional Policy

Technical Functional Policies

Authentication

- All wireless stations (users/devices) must be authenticated to access a WLAN.
- If username and password authentication is used, users/devices must use strong passwords (alphanumeric and special character string at least eight characters in length).
- If a central authentication server or VPN gateway is used in the WLAN architecture, each wireless client must uniquely and successfully authenticate to the WLAN. Strong passwords must be used in this situation
- All wireless device users must be authenticated to access wireless devices and/or the desktop PC synchronization software.
- Wireless handheld devices and synchronization software must require a strong password, or both to authenticate access to the device or software. Users are required to authenticate when operating locally and remotely.
- Wireless device authentication must not be disabled.

Encryption

- All WLAN traffic must be encrypted to limit eavesdropping and ensure confidentiality.
- Wired Equivalent Privacy (WEP) must be enabled using 128-bit key or the strongest encryption available in the 802.11 b/g/n compliant product used.

Access Control

- All access to the WLAN system, including its data and resources, shall be restricted unless authorized by the PMU -ITD. Data traversing wireless networks and data accessible via wireless entry must be protected from unauthorized access, use, modification, or deletion using access control methods.
- Non-PMU employees, excluding approved vendors and contractors, must not have access to WLANs that connect to the PMU Enterprise data network.
- Service Set IDs (SSIDs) must be changed from the factory default to something that is meaningless to outsiders. SSID character strings must not reflect Member or Committee name, location, or product being used.
- Broadcast mode of SSIDs must be disabled in products that permit it so that the client SSID must match that of the access point.
- The authentication server, firewall, and/or VPN gateway must enforce access control mechanisms.

Anti-Virus Software

- Antivirus software at the perimeter will provide protection for handheld devices by scanning all entry ports (i.e, synchronizing, email, and Internet downloading) as data is imported into the device, provide online signature update capabilities, and prompt the user before it deletes any suspicious files.

Personal Firewalls

- It is highly recommended that WLAN client and handheld devices utilize personal firewall software.
- Users that access public wireless networks (e.g., in airports, conference centres, coffee shops) should install personal firewall software on all WLAN client and handheld devices. A personal firewall protects against wireless network attacks and rogue access points (e.g., Ad hoc networks, accidental or malicious association, soft access points) that can be easily installed in public areas.

Physical Security

- Access points must be physically secured upon proper configuration to prevent tampering and reprogramming (i.e., to prevent unauthorized

physical access).

- Access points must be placed in secure areas, such as high on a wall, in a wiring closet, or in a locked enclosure to prevent unauthorized physical access and user manipulation. Devices must not be placed in easily accessible public locations.
- To mitigate eavesdropping, access points shall be placed strategically within the building so that the range does not exceed the physical perimeter of PMU-controlled facilities and allow unauthorized users to eavesdrop near the perimeter. Access points shall be placed to minimize or prevent the distance that the signal can travel outside the area that is under the control of the organization, including buildings, court yards, adjacent parking areas, etc.
- The transmission power of WLAN access points must be restricted to the lowest power required for coverage.
- In the event that the reset function of an access point is used, the device must be restored to the latest security settings.

Logical Security

- All access points shall be logically separated and isolated from the House Enterprise data network, such as on a different segment, in a demilitarized zone (DMZ), or in a virtual LAN (VLAN).
- WLANs must be treated as insecure counterparts to their wired associates. Access to resources on the wired network must be restricted.
- Access points shall be physically situated so that authorized users can connect, yet away from sources of interference such as microwave ovens and Blue-tooth devices.
- To keep interference to a minimum, access point channels shall be at least five channels different from all other nearby access points on different WLANs. Some coordination may be required if multiple WLANs are to be used within close proximity.
- All insecure and nonessential management protocols (Hypertext Transport Protocol (HTTP) and Simple Network Management Protocol (SNMP)) shall be disabled if not used
- SNMP settings must be set to least privilege (read only).
- Web-based management of access points shall be from pre-defined management stations controlled by access lists on the access point. SNMP requests shall only be accepted from specified management devices.
- SNMPv3 products or equivalent cryptographically protected protocol shall be used since they include mechanisms to provide strong security.

Monitoring & Audit

- All wireless LANs and handheld devices must be routinely monitored and security audits performed to verify that security configurations comply with this policy, access points and wireless devices are authorized, and to identify unauthorized activity.
- If DHCP is used in the environment, logs shall be reviewed for static addresses to determine if rogue access points have been installed.
- Access logs and system audit trails shall be routinely monitored.
- The ITD will conduct routine controlled penetration tests or packet sniffing/ wireless traffic analysis on WLANs and within the coverage area
- All access points must have Intrusion Detection Systems (IDS) at designated areas on House property to detect unauthorized access or attack.

Responsibilities

Systems Administrators/Vendors/Users Responsibilities.

- System Administrators / Vendors are required to operate Wireless LANs and devices in a secure manner.
- System Administrator / Vendors job includes proper authorization and termination of access, proper configuration and placement of wireless components and associated security technologies, routine, random, and event-driven maintenance, support monitoring and audit functions, etc.
- System Administrators / Vendors are required to change factory default settings and use strong administrative passwords on all wireless devices to ensure a higher level of security. (On some wireless devices, the factor default password is blank.) All insecure and nonessential management protocols must be disabled.
- To the extent possible, System Administrators / Vendors shall ensure that their wireless implementation and associated security technologies are up-to-date with evolving standards and best practices.
- System Administrators / Vendors are required to maintain a list of authorized wireless device users to enable them to perform periodic inventory checks and security audits.
- Wireless users must only access information systems using approved wireless device hardware, software, solutions, and connections.
- Wireless users must act appropriately to protect information, network access, passwords, cryptographic keys, and wireless equipment.
- Wireless users are required to report any misuse, loss, or theft of wireless

devices or systems immediately to the IT Department. (Planning & Control)

Minimum Security Requirements

There will further addition to the checklist in case of new release, Version or change in Technology. Each point in the section has a check box which needs to be filled with “Y” for available and “N” for not available. Please read the points carefully before filling the check boxes.

Reduce your WLAN transmitter power

This feature not on all and access points, but some allow you lower the power of your WLAN transmitter and thus reduce the range of the signal. Although it's usually impossible to fine-tune a signal so precisely that it won't leak outside your home or business, with some trial-and-error you can often limit how far outside your premises the signal reaches, minimizing the opportunity for outsiders to access your WLAN.

Authentication

Consider using an additional level of authentication, such as RADIUS, before you permit an association with your access points. Cisco access points, for example, can enforce RADIUS authentication of MAC addresses to an external RADIUS server.

Supplement on Email Accounts

Introduction

This functional policy covers PMU's E-mail usage. Communications and operational management of information resources and systems are essential to maintaining a high level of service to PMU Users. Therefore, security requirements will be developed and implemented to maintain control over Electronic Mail Usage.

It is each user’s responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of these Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU which includes

Purpose and Scope

To make a easy and secure policies for electronic mails being used by all PMU personals, to have a organized and professional method to follow in PMU, where it limits the usage, controls the email behaviors etc….

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the email usage

- Email Domain of PMU: <user>@pmu.edu.sa
  (i.e. First letter of the first name then the last name / family name)
- E-mail must only be available to PMU employees and students.
- No offensive material must be sent using E-mail.
- Functional policies for the use of E-mail must be developed and controls put in place to reduce security risks created by electronic mail.
- Content scanning must only be enforced in checking for malicious software, viruses or violations.
- Formal agreements must be established for the electronic or policy exchange of information and software between organizations.
- PMU's policy on Internet, Intranet and E-mail services access and use provides that usage of these services by PMU employees must be compatible with the organisations objectives.
- The implementation of the E-mail, Internet and Intranet policy is aimed at

ensuring that all employees and independent contractors are made aware of the disciplinary sanctions that PMU must impose on any unauthorised and/or unacceptable use of these services.

- The policy is also implemented to minimise the risk of civil and/or criminal liability to the organisation through the unauthorised and/or unacceptable use of the E-mail, Internet and Intranet services
- Every Outgoing email from PMU should have disclaimer

Electronic Mail Functional Policies

Access to E-mail: All requests for e-mail access must be forwarded by HR to ITD Helpdesk for account creation.

Acceptable and Unacceptable Use of E-mail Business Use

E-mail communication enables PMU employees and other types of workers to send messages and memorandum between workers within PMU, and also between PMU, business partners, vendors and required domains, more effectively.
This service does however will not offer the opportunity for abuse of resources and inappropriate use of this medium, which could expose PMU to significant risks. Therefore e-mail facilities will only be available to PMU users by following the formal procedures and by accepting the policy rules.

Conditions on Academic and Business Use

Email usage in PMU for the academic and business use must be within, but not limited to the following conditions:

- Employees may not use e-mail for personal or commercial purposes.
- Access to e-mail from a PMU-owned home-based computer or through PMU-owned connections must adhere to all the same functional policies that apply to use from within PMU facilities.
- Employees shall not allow family members or other non-employees to access PMU e-mail system via linked home computers.
- Disciplinary action may occur after actions including or similar to those stated below of PMU e-mail facilities has occurred:
    - Unauthorized attempts to break into any computer;
    - Theft or copying of electronic files without permission; and
    - Sending PMU files outside the PMU to unauthorized personnel.

Personal Use

PMU understands that many users work at non-traditional times, for example

outside working hours and that these activities infringe on “personal time”. PMU therefore allows incidental and infrequent personal use of e-mail

Conditions on Personal Use

Users may use e-mail for coincidental personal purposes on condition that:

- It does not consume significant amounts of the user’s workday.
- It does not consume substantial amounts of PMU bandwidth in such a way that it negatively impacts upon PMU e-mail system or other PMU users, either directly or indirectly. PMU bandwidth could be impacted by distribution of the following:
- Large e-mail messages. Users should consider using compression utilities such as Zip before sending large e-mail messages.
- Large e-mail attachments can also be placed on shared documents if it is being used for local communication, and pass a hyperlink to access the required files, which will reduce the bandwidth usage drastically.
- Attachment types such as JPEG, JPG, AVI, Chain letters, jokes, bitmaps, etc cannot be circulated using PMU infrastructure services.

Note: There are many free services on the Internet to share images and video files. Do not use university resources to distribute large files to large group of people.

Privacy of PMU E-mails.

As PMU allows the incidental and infrequent personal use of e-mail, users must be aware of the restrictions placed on the privacy of e-mail.

- Electronic mail is private and owned by the sender and each recipient account holder.
- The contents of e-mail will not be monitored, censored, or otherwise examined except:
- With specific authorization from the head of the Department as part of the required system administration;
- Investigations may require the examination and release of any document, including electronic files such as e-mail. Should any PMU user be involved, the ITD Department will act only under the specific instructions from a business unit manager to ensure that individual rights, including rights to privacy and due process are maintained; and
- A special condition exists for users who receive e-mail associated with his/her job responsibilities and where, their direct supervisor or others in the department need to have access to their e-mail. ITD will continue to maintain the privacy of mail

Expressly Prohibited Use

The creation, transmission, receipt or storage of certain content may be in violation of regulatory and statutory requirements and are therefore prohibited within PMU. This content includes, but not limited to the following:

- Unprofessional Threats;
- Pornographic explicit material, but limited to unsolicited SPAMS being spoofed and circulated.
- Material containing derogatory racial, gender, religious or hate-oriented comments;
- Discriminatory language or remarks that would constitute harassment of any type.
- Any other comments that offensively addresses someone's age, political beliefs, national origin, or disability.

E-mail Manners

Any form of communication is most effective if it conforms to etiquette acceptable to both the sender and the recipient of the message. Therefore the following principles should be followed when using e-mail:

- Are concise - long messages often lose their emphasis.
- If you have received a message as a part of a group of recipients consider a reply to only the author rather than to the entire group.
- As with any written form of communication, attention to proper grammar, spelling, etc. will convey your message most effectively.
- Remember that even though the medium is electronic, the recipient of the message is another human.

Unsolicited E-mail

When a staff receives unwanted E-Mail (Junk Mail or SPAM), they must refrain from responding directly to the sender. Instead, they should forward such E-Mail to the IT-Help desk which will forward the case to the appropriate technical resource for remediation.

Representing PMU

Liability

Users must be aware that in using PMU e-mail facilities they are representing PMU.
It is therefore important that the use of e-mail must be in accordance with the following:

- Users should consciously build and preserve PMU image when they use e-mail for communication.When applicable, users should attach the official PMU headers and disclaimers to e-mail. A disclaimer could state the following:
    - This message (including attachments) is intended for the addressee named above. It may also be confidential, privileged and/or subject to copyright. If you wish to forward this message to other, if you are not the addressee named above, you must not disseminate copy, communicate, otherwise use, or take any action in reliance on this message. You understand that any privilege or confidentiality attached to this message is not waived, lost or destroyed because you have received this message in error. If you have received this message in error, please notify the sender and delete from any computer.
- Unless explicitly attributed, the opinions expressed in this message do not necessarily represent the official position or opinions of PMU.
- Whilst all care has been taken, PMU disclaims all liability for loss or damage to person or property arising from this message being infected by computer virus or other contamination.
- The creation of business e-mail is equivalent to the creation of any other PMU document. Therefore, user must use the same degree of care and seriousness associated with the drafting of PMU documents when composing business e-mail messages.
- The quality of written or verbal communications reflects on PMU. Users should always strive to use good grammar, correct punctuation, and acceptable language.
- Users are not allowed to enter into any contractual agreement for or on behalf of PMU using e-mail.

Disclaimer of Liability

PMU is not responsible for material viewed or received by users from the Internet or other public e-mail systems. Users are cautioned that these communications may include offensive, sexually explicit, and/or other inappropriate material. Having an e-mail address may lead to receipt of unsolicited messages containing offensive content.

Electronic Fraud

As electronic fraud may be possible via e-mail, user must adhere to the following:

- Impersonation
    - Impersonation of another user when using e-mail is prohibited within PMU.
    - Users should not allow others to use their e-mail accounts. If a user has no option but to allow this, the user must understand that they will be held responsible for all actions performed on their e-mail account.
- Anonymous E-mail: Anonymous e-mail may be used in the event of:
    - A user reporting an incident due to wrongdoing caused by another PMU user may send anonymous e-mail.
    - Users requesting medical information, without disclosing their identity.

Computer Viruses

A computer virus is a software program intended to damage, delete or perform other harmful actions to a user's data. It is therefore important that users adhere to the following when receiving e-mail from an unknown source:

- Users must ensure that all e-mail attachments are scanned for viruses before opening, using approved PMU anti-virus software.
- Users must immediately report any malfunction that might be related to a computer virus to the IT-Helpdesk
- When accessing public e-mail servers (e.g. hotmail) or when connecting to public SMTP servers from a workstation that is linked to the PMU network, users must ensure that any attachments are scanned for viruses on the user's workstation.
- User must read ands comply with the Protection Against Malicious Software and Viruses Functional Policy

Transmitting Confidential Information

Addressing E-mail

- When a user sends e-mail, it is the user's responsibility to ensure that the e-mail address of the recipient is correct.
- When a user recognizes that a mail item has been incorrectly addressed to him, the user should inform the sender by returning and deleting the mail.
- The user must ensure that their personal information on directories and/or address books is kept up to date.

Information Protection

- Prior to e-mailing or forwarding proprietary data, the e-mail options should be set to confidential. The message should be given the subject confidential.
- Documents containing proprietary information should be individually password protected.
- The sender and receiver should agree on the password by calling in advance. Under no circumstances should sensitive information be sent without a password.
- The sender should also ensure that the receiver is able to retrieve the message from the e-mail address to which it is sent – in terms of the software used to create the e-mail as well as any attached documents.
- The e-mail system should not be used to communicate details of the password.
- The message recipient should be asked to confirm receipt of the document.
    - In this subsection, "proprietary information" refers to information that is "confidential" and/or "critical".

E-mail Software

Only authorized email software may be used, no re-mailer (mail bomber) software will be permitted for any purpose.

Retention of E-mail Messages

E-mail shall be retained for periods that would normally apply to written or facsimiled transactions. Where precise retention periods need to be defined, they should be defined in conjunction with PMU IT Department.

Supplement on Software Copyright Compliance

Introduction

This functional policy covers PMU's Software Licensing and Compliance. This is to ensure that all PMU assets must be accounted for and controlled in the proper manner, for both physical and logical assets. These assets are crucial to PMU's success and must be protected by the proper controls to minimize any risk of harm, disruption of services or disclosure of proprietary information.

It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.Each policy statement is supported by standards and procedures to achieve a complete security framework in the PMU.

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy Statements govern the Functional Policies on Software Licensing and Compliance listed in this document:

- Arrangements involving third party access to organisational information processing facilities must be based on a formal contract that must contain all necessary security requirements accompanied with appropriate responsibility and confidentiality undertaking. Any violations thereto must be dealt with accordingly.
- Owners must be identified for all major assets and the responsibility for the maintenance of appropriate controls must be assigned.
- All Employees and third parties such as contractors, consultants, business partners and outsourced staff must sign a confidentiality agreement as part of their initial terms and conditions of employment.
- Detection and preventive controls to protect information and information processing facilities against malicious software and appropriate user awareness procedures must be implemented.
- Formal agreements must be established for the electronic or policy exchange of information and software between organizations.
- Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly.
- Control must be applied for the implementation of software on all systems.
- All data must be protected and controlled.
- Strict control must be maintained over access to program source libraries.
- The purchase, use and modification of software must be controlled and checked to protect against possible covert channels and Trojan code.
- Controls must be applied to secure outsourced software development.
- Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products.

Software Licensing and Compliance Functional Policies

Protection of Intellectual Property

- All software and/or applications developed for PMU by third parties is the property of PMU. This must be conveyed to all third parties, which develop software or applications for PMU use, to prevent any dispute about ownership of the software once a project is completed.
- Software developed by PMU employees on company time becomes the property of PMU.

User Responsibilities regarding Software Licensing

- Purchase and use of third party software must be in accordance with third party licensing agreements. These agreements may include specific user restrictions such as:

    - The number of copies allowed to be installed;
    - The number of machines the software can be installed on;
    - The number of concurrent users of the software allowed at any one time; and/or
    - The customer support levels (onsite or phone) may also be specified within the agreement.
- Only appropriately licensed software may be placed on or used in a resource. Such software may only be for the purpose of conducting PMU business.
- Employees are to be provided appropriately licensed copies of software necessary to perform their assigned tasks. Employees must not be asked or expected to perform tasks for which appropriately licensed software has not been provided.
- Some software licenses allow for the user to make a copy for home use or home-based business use in conjunction with the business use of the software. A user of licensed software at work should not assume that such provision is in place. Prior to installing copies of software at home, employees must obtain confirmation of their rights in writing from relevant management.
- Internal Audit, in conjunction with ITD, must perform periodic reviews of software usage on PMU PC's, laptops and servers to ensure that it is in compliance with licensing agreements.
- All software found in violation must be removed immediately. Parties responsible for loading and/or using non-compliant software will be subject to corrective actions by management.
- The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased Information Security risks associated with such projects are mitigated using a combination of procedural and technical control techniques

User Responsibilities Regarding Software Copyrights

The unauthorized use, copying, or distribution of copyrighted software is not allowed.
Unauthorized acts include, but are not limited to, the following:
Making extra copies of computer based software for use on other computers unless specifically allowed through a licensing agreement;
Putting copies on a network in unprotected environments where they may be copied by others

To comply with government mandates and to ensure ongoing vendor support, the terms and conditions of all End User License Agreements are to be strictly adhered to:

- Obtaining copies of software from others without paying the appropriate licensing fees;
- Unauthorized distribution of software by electronic mail.
- All users of software on PMU Information Systems must strictly abide by copyright laws and restrictions detailed by the software manufacturer and the Agreements signed therewith.
- A copyright notice must be used to protect software or other copyrighted materials developed by or for PMU.

Obtaining and Using Software

Software Definitions

Software that can be obtained from sources other than ITD can be defined as follows:

- Evaluation Software: Evaluation software is a limited software that has some of its features disabled. This software usually allows the use of a fair number of features in order to entice a user to purchase the full product.
    - Public Domain Software: Public domain software is made available with no restrictions on its distribution or copying. However, unless there is a statement to the effect that the software is in the public domain, the user should assume the author retains the copyright to the software.
    - Freeware Software: Freeware is free and was developed to provide end users with a new application. There are no license restrictions to these programs.
- Shareware Software: Shareware is software that can be downloaded, tried and evaluated for its use, and its full-featured program can be bought at a nominal fee. If not bought, the shareware programs usually either stop functioning after a period of time or they continue working but will never have all of the features that the purchased version would have.
- Application Software: Application software is a software containing business application programs that may have been developed in-house or by a third party or may have been purchased off-the-shelf.

Evaluation and Public Domain Software

Obtaining or downloading of evaluation and public domain software from other than PMU sources is permitted only under the following conditions:

Selecting Business Software Packages

- The software must be required for a legitimate business purpose and approved by management.
- Use of the software must comply with all applicable copyright and license agreements.
- It is recommended that the software be obtained only from known vendors or suppliers, ideally those with whom PMU currently does business, or are considering doing business with.
- At a minimum, an evaluation as to the safety and reliability of the vendor or provider of the software must be performed by the person obtaining the software.
- The person obtaining the software should check it for viruses, trap doors, and other malicious code. A reasonable evaluation must be performed on a single system or in a test environment lab before deploying the software to others.
- If the software is found to be creating security vulnerabilities or causing system or network problems, the problem causing the identified vulnerability must be corrected in a timely manner or the software must be removed immediately.

Freeware and Shareware Software

Obtaining or downloading of freeware and shareware software from other than PMU sources is permitted only if the conditions laid out by this functional policy are adhered to. In addition, the following should be noted:

- Software distributed in this manner is often inadequately tested, e.g., Beta versions of software. The software may not work correctly, or may cause problems with other approved software. ITD has no obligation to support this software or resolve any problems it causes, unless arrangements have been made in advance with ITD Management;
- The supplier or vendor of such software may refuse to make modifications or provide support for the software in the future; and
- Shareware, where required, must be licensed and users must strictly abide by copyright laws and restrictions detailed by the software manufacturer. This includes the terms and conditions when downloading the shareware or freeware.

Purchasing Software

All requests for new applications systems or software enhancements must be presented to management with a Business Case with the business requirements presented in a User Requirements Specification document

- Proof of purchase is required for all licensed software installed on an PMU personal computing device.
- Proof of purchase may be demonstrated by possession of one or more of the following:
- Original purchase order (or a copy of the original purchase order);
- Receipt or packing slip from the vendor;
- Software right to use license; and
- Original serialized software CD or diskette.

Proof of purchase is not required for site-licensed software obtained through authorized procedures. However, users must ensure they are in compliance with the software license before copying or loading site-licensed software.

Proof of purchase must be kept and filed for reference and audit purposes.

Protection of Software

Protection of Computing Software

- CDs and DVDs and other removable media containing software programs must be locked in secure file cabinets when not in use.
- CDs and DVDs and other removable media containing application software programs must be kept under the custody of ITD

Return of Computing Software

- Software stored on PMU personal computing devices must be returned together with the personal computing device to PMU upon termination of employment or work contract.
- Off-site copies, including copies stored on personally owned computers (when permitted by the license agreement) must also be returned (or erased, where appropriate) at the same time.

Policy 03: Data Access

Purpose

Administrative data captured and maintained at PMU are a valuable university resource. To protect PMU sensitive data from unauthorized disclosure and inappropriate use the ERP system contains data from multiple operational areas that need to be integrated in order to support institutional business analysis, reporting, and decision making. The purpose of this ERP Data Policy is to ensure the security, confidentiality and appropriate use of all ERP data which is processed, stored, maintained, or transmitted on PMU computer systems. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental. This policy applies not only to stored information but also to the use of the various computerized systems and computerized programs used to generate or access data, the computers which run those programs including workstations to which the data has been downloaded, and the monitors and printed documents that display data.

Definitions

ERP Data – Any data that resides on, is transmitted to, or extracted from any ERP system, including databases or database tables/views, file systems and directories, and forms.

ERP Security Administrator – An IT professional position in the Office of CIO is responsible for processing approved requests.

ERP System – Human Resources, Finance, Student, Financial Aid, Luminis, Executives reporting tool, Banner Online Reports, ERT and any other interfaces to these systems.

Data Owners - Data Owners are responsible for determining who should have access to data within their jurisdiction, and what those access privileges should be. Responsibilities for implementing security measures may be delegated, though accountability remains with the owner of the data.

Area of Responsibility Data Owner(s)

Student System	:	Student Affairs Dept.
Student Financial Aid System	:	Budget and Accounting Dept.
Finance System	:	Budget and Accounting Dept.
Human Resources System	:	HR Dept.
Faculty Academic	:	Student Affairs Dept.
Accounts Receivable	:	Budget and Accounting Dept.

Data Custodians - Data Custodians oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area. They are responsible for the general administration of user access to data within their area(s) of responsibility. Data Custodians are appointed by the respective Data Owner.

Data Users - Data users are individuals who access ERP data in order to perform their assigned duties or fulfill their role in the PMU.

Query access – Access enabling the user to view but not update ERP data.

Maintenance access – Access enabling the user to both view and update ERP data. This access is limited to users directly responsible for the collection and maintenance of data.

Data Administration

By University policy, certain data is confidential and may not be released without proper authorization. All PMU ERP data, whether maintained in the central database or captured by other data systems, including personal computers, remains the property of PMU. Department heads are responsible for ensuring a secure office environment regarding all ERP data. Department heads will review the ERP data access needs of their staff as it pertains to their job functions before requesting access via the Banner Access Request Form. ERP data (regardless of how collected or maintained) will only be shared among those employees who have demonstrated a job related need to know.

Access to ERP Data

Below are the requirements and limitations for all PMU Divisions/Departments to follow in obtaining permission for access to ERP data. Division/Department heads must request access authorization for each user under their supervision by completing and submitting a Banner

Access Request Form

Approved requests will be forwarded to the ERP Security Administrator for processing. Under no circumstances will access be granted without approval of the appropriate department heads.

Secured Access to Data

ERP security classifications will be established based on job function. Specific capabilities will be assigned to each security classification. Each user will be assigned a security classification. Some users may be assigned several security classifications depending on specific needs identified by their Division/ Department head. The use of generic accounts is prohibited for any use that could contain protected data.

Policy 04: Data Protection

Purpose

To protect PMU sensitive data from unauthorized disclosure and inappropriate use.

Policy

It is the responsibility of each individual with access to sensitive data resources to use these resources in an appropriate manner. Additionally, it is the responsibility of each individual with access to sensitive data resources to safeguard these resources. Methods of safeguarding sensitive data include:

- Sensitive data should not be stored on personal desktop or laptop computers since these computers tend to reside in less secure locations than central servers.
- Access to computers that are logged into central servers storing sensitive data should be restricted (i.e. authenticated logins and screen savers, locked offices, etc.).
- Access to sensitive data resources stored on central servers should be restricted to those individuals with an official need to access the data.
- All servers containing sensitive data must be housed in a secure location and operated only by authorized personnel.
- Copies of sensitive data resources should be limited to as few central servers as possible.
- Sensitive data should be transmitted across the network in a secure manner (i.e., to secure web servers using data encryption with passwords transmitted via secure socket layer, etc.).
- Any accidental disclosure or suspected misuse of sensitive data should be reported immediately to the appropriate University official.

Definiation

Sensitive Data - any information that could cause an individual personal financial harm if disclosed and used improperly. Examples of sensitive data include but are not limited to social security numbers, credit card numbers, computer

passwords, and any personal information flagged for non-disclosure.

Policy 05: System Development Life Cycle (SDLC)

Introduction

This functional policy covers PMU's Systems Development and Maintenance. It is essential that security is built into information systems and not bolted on afterward. Therefore ITD will document the security and control requirements to be determined during system design, development of the system architecture and to be implemented in the final system. Effective security related change control procedures will be in place to ensure changes occur to the system in a controlled and secure environment with minimal risk to the "live" environment.

It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under PMU's possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Systems Development and Maintenance Functional Policies

Roles and Responsibilities

Project Management

The Project Managers responsibilities include, but are not limited to the following:

- Provides overall direction for the project;
- Ensures appropriate representation of affected users and business units if necessary;
- Monitors and controls costs and project timetable; and
- Ensures deliverables are a quality product.
- Ensure adequate implementation of security policies.

Project Planning

Purpose of Project Planning

Planning must be done for development of new systems/applications and for any major and/or minor enhancements to systems/applications.

Creation of Project Plan

Project Plan creation must include consideration for the following:

- The allocation of personnel and information resources needed for analysis, design, implementation, administration, and maintenance.

- The plan must include a discussion of specific goals as an integral part of the system requirements. This must include:
- Documentation of known constraints, which could impede proper development;
- Processes to ensure adequate security has been addressed, such as security reviews.
- All cost estimates must include the cost of analysis, design, implementation, and ongoing administration and maintenance.
- All time estimates must include a reasonable estimate of the time required for a thorough analysis and implementation.
- The planned reporting structure and hierarchy must include the appropriate management levels needed for approval and control throughout the project, including:
- Requirements will be defined, and specifications approved by the Owner prior to acquiring or starting development of any applications; and
- Recoverability processes must be considered during planning since this could influence the selection of computing platforms and database management systems.

Analysis of the System/Application

Purpose of Analysis

Analysis defines the features and functions of the system or application and provides the logical system specifications from which requirements will be defined.

Analysis

The following must be included during the analysis:

- A risk analysis to determine the controls required for the system or application under development or acquired, including:
- Performing a threats and vulnerability analysis. Security vulnerability considerations including those introduced when designing the connectivity or interface with other systems and applications; and
- Performing a business impact analysis. This must include an analysis of the impact on both existing and new systems and of opening new connections
- In defining the required operating environment, existing operating system security controls must be utilized (where available).
- The environment selected must support all requirements of the system or application being developed.

- Where an application or system has no specific requirements, a statement to that effect should be documented and approved by management.
- The analysis must balance user's requirements with required security controls.
- An acquisition vs. development analysis must include specifications for required academic and business need.
- Any Request for Proposal or Request for Information used to solicit vendors must include selection criteria for functionality.

Design of the System/Application

Purpose of Design

- Design uses the logical models from analysis and makes them executable.
- The work done in design provides the basis for actual development of the system or application. System and physical architecture, interfaces, policy processes, and documentation are design components.

Requirements in Design

For all systems designed within or for PMU, requirements must be used, which have been determined in the analysis phase, prior to the application development phase.During the system design phase, Information Owners, PMU and Information Security must determine the proper control environment of the application by using the security specifications of the analysis phase.

Development Environment

Securing Source Code under Development

For securing source code under development the following must be adhered to:

- Source code, including parameter and configuration files, is a valuable information asset and must be protected when in development.
- Access control to the development environment and authorization control for all data and source code files must be implemented.
- Developer access must be restricted to only those resources required to perform established job duties.
- Security audit records capable of providing sufficient information for after-

the-fact investigation of loss, impropriety or other inappropriate activity must be generated and reviewed.
- Source code under development may be at greater risk of being acquired before all copyright protection is in place, thus making it subject to claims of ownership by intruders.
- Programmers must maintain documentation of their program development and changes in order to legally support claims of ownership for software not yet copyrighted.
- Systems/applications documentation must be prepared and maintained throughout the development/maintenance lifecycles to ensure continuity.

Management of Changes to Source Code under Development

Management of changes to source code under development must conform to the following:

- Version control must be utilized for ensuring ongoing management of changes to the source code. An automated process with specific version tracking functionality or a policy procedure may provide version control.
- Source code under development must be backed up and secured from unauthorized access.
- Changes to source code must allow for rollback. Rollback will enable the developer to restore source code to its original state if necessary.
- Changes to source code under development must be part of the change control process.
- System/Application documentation should be updated when changes are made.
- Changes to source code must be evaluated by a second person to review if any inappropriate code has been included (i.e. Trojan horses, etc).

Test vs. Production Environments

The following must be adhered to for the test and. production environments:

- Development and testing must be performed in an environment which is separate from production, either physically or logically, to ensure that testing and production processing cannot impact each other.
- If possible, testing should not involve any components of the production environment, including software, hardware, and network connectivity.
- Testing should be done only with test data; production files and data must never be impacted by the development process.
- If access to production environment is required, such access must be approved by the Information Owner and must be limited to read only.
- Copies of production data may be used for testing, after scrambling where

feasible, if they are controlled to the same degree as in production.

- Sensitive data should be sanitized or deleted from the created test data.
- Production processing must be performed only with production data. Production data must never be impacted by the testing process.
- Development hardware must not be migrated to a production environment until all development and testing is completed and proper signoff was obtained.
- It is recommended that the operating system and all file systems be reinstalled and reinitialised to ensure that all production security controls are in place.
- Measurements need to be in place to ensure that the tested system is transferred to production without any alterations (e.g. using checksums).

Testing of the System or Application

Purpose of Testing

- Testing verifies that the features and functions of the system or application are in line with the development specifications and ensures that its operation is compatible with the environment in which it will run.
- During testing, the test scenarios are designed for unit, system, integration, and acceptance testing.
- All tests are executed and the results are logged and evaluated. All errors must be corrected during testing and before implementation.

Security Requirements for Testing

Security must be integrally included in unit, system, integration, and user acceptance tests. This includes both developed and purchased software. In all cases:

- Test plans must include time and resources to sufficiently test all aspects of the security functionality.
- Scenarios for testing security must be designed in attempt to defeat or circumvent security.
- Testing procedures must be properly documented on the change request forms.
- During integration and acceptance testing, logical access restrictions must ensure that developers have no update access and that the code being tested cannot be modified without written consent of the user.
- Both successful and unsuccessful access attempts must be tested and the appropriate audit logging must be verified.
- The developer must supervise unit testing in the testing environment. The developers manager must then perform an independent review of these results.

- As part of the test, verification must be done to ensure that the newly developed system or application does not introduce vulnerabilities in existing structures, common networks and systems.
- If test data must be transmitted to an external site, other than to the ultimate recipient, to complete a test, all sensitive or proprietary information in the data must be sanitised or deleted.
- If the system or application is intended to execute on more than one type of platform, security must be tested in each of the possible operating environments.
- Testing of security administration functions is required.
- If the software being tested was purchased, it may be advisable to have a technical representative from the vendor onsite during the testing.
- The system or application must be tested when the security function is down to ensure that access is not allowed.
- All testing logs and evaluations must be secured and marked.
- Where a mechanized scanning tool is available, a vulnerability scan must be completed for all new systems prior to being approved for production. The tools used for such scans must not be distributed to the developers or any persons other than security or system administrators.
- All significant modifications, major enhancements and new systems must be integration and acceptance tested prior to installation of the software in production.
- Volume and stress testing for the security functions must be included in the test plan. If possible, maximum user access should be simulated to measure the response of the system.
- Backup and recovery processes for the system or application and for any databases must be tested.
- Disaster Recovery Plans must be tested and updated to ensure changes to systems/applications are adequately addressed.
- All tests performed must be signed off in the test plan/test script by staff who performed the test and must be approved by the Business Owner.

Unit Testing

- The developer will supervise unit testing in the development environment.
- Testing procedures must be properly documented and the developer's manager must perform an independent review of unit test results.
- If problems are noted, the developer will document the problem, make appropriate modifications in the development environment.

Integration Testing

- All significant modifications, major enhancements and new systems will follow integration testing prior to installation of the software in production.
- System stress testing and volume testing must be performed, and in some cases, parallel testing will be required.

- Integration testing must be conducted in a separate, independently controlled environment.
- During integration testing, logical access restrictions must ensure that developers have no update access and that the code being tested cannot be modified without the written consent of the user.
- Copies of production data, sanitized from any customer data, or pre-designed test datasets must be used for testing purposes..

User Acceptance Testing

- All significant modifications, major enhancements and new systems must be acceptance tested by the appropriate users, prior to installation of the software in production.
- The user acceptance plan will include tests of all major functions, processes and interfacing systems.
- Testing procedures must be properly documented on the change request forms.
- During acceptance testing, logical access restrictions must ensure that developers have no update access and that the code being tested cannot be modified without the written consent of the user.
- If problems are noted, the user will document the problem, the developer will make appropriate modifications in the development environment and submit it to CASD for re-testing.

Implementation of the System or Application

Purpose of Implementation

- Implementation installs the system or application into production.
- During implementation, data is converted as needed, and live processing begins.
- Users and operators should be trained before implementation.

Requirements for Implementation

Before moving a system or application into production, the following must be accomplished:

- An operational readiness review must be completed which includes evidence of the following items at a minimum:
    - Compliance with the current PMU IT Architecture;

    - Satisfactory completion of vulnerability scanning, where feasible;
    - Preparation of a Disaster Recovery/Contingency Processing Plan; and
    - Assignment of an appropriate number of qualified System and Security Administrators.
- A backup of all existing files and databases that will be impacted must be done before beginning implementation.
- After successful installation, all developer access must be removed to the production environment.
- If multiple sessions were allowed for any testers or other users, they should be reviewed in production and limited if no longer needed or conflicts with existing access.
- Approval to move software from development to production must be obtained.
- Approval to move software from production to development must be obtained within the formal change management process.
- Security administrators and users must be fully trained on the new functions.
- Any policy security processes required for implementation must be in place.
- Availability of a facility to print security reports, such as:
    - Security violations;
    - User profiles and access rights; and
    - User administration activities.
- Personnel to review and monitor audit intrusion reports must be available and trained.
- For purchased software, a written vendor statement that all security controls have been successfully implemented and are functional must be obtained.
- Only object code should be distributed to end users.
- Rollback plans need to be in place.
- License data on all purchased software distributed must be maintained.
- If the new system or application is replacing an existing system, procedures for maintaining security administration on both systems during the implementation must be established.
- Ensure the correct version is installed (the version that was tested and signed off).
- Ensure the necessary SLA is in place and signed.

Maintenance of Systems or Application

General Maintenance Information

General maintenance information includes:

- Maintenance of systems and applications begins after the system or application is stable and no longer under development and continues over the life of the system.
- It includes day-to-day system/application monitoring, tuning for performance purposes, scheduled and emergency maintenance functions, problem management to correct faults and to adapt to business change, change control for system enhancements, and security administration.
- Maintenance actions must be planned and must sufficiently cover the maintenance of security functionality of systems/applications.

Monitoring of Systems and Applications

Monitoring of systems and applications must be in accordance with the following:

- Systems and applications are only valuable if they are available at the required times. All parties involved must ensure that procedures to support operational monitoring of all production systems and applications are in place.
- Dated and time stamped logs should be produced to aid in evaluating the operations. Examples of areas to monitor include:
    - Outages and downtime;
    - Volume of usage for data and users;
    - General system response time; and
    - System and resource access.

Emergency Maintenance Procedures

Emergency procedures for correcting unpredicted software errors must include:

- The ability to grant sufficient access to enable the maintenance personnel to accomplish the task.
- As soon as the emergency is past, details of the changes implemented must be documented.
- This documentation should include the following details:
    - The change requestor;
    - Authorization for change;
    - Short description of the required change; and
    - The time frame in which the change was required.
- Normal maintenance or change control procedures should be applied retroactively.
- Emergency changes to programs should be made to separate copies of the programs to allow production work to continue.

- After the emergency, implementation approval as used in change management should be utilized.
- If it was necessary to grant special access to production resources, activities must be monitored and logged. After the emergency, all such access must be revoked.
- The installation of any type of back door that circumvents security controls is prohibited.

Policy 06: Change Management

Introduction

Prince Mohammad University relies upon IT services in order to perform its roles of teaching and administration. The inter-dependencies of these systems are complex and the results of change made to any system may have serious consequences.The uncontrolled implementation of changes to University's IT systems, critical systems and underlying infrastructure utilized to perform its core roles presents a significant risk to the University.

Changing system requirements, resolution of known issues, implementation of new services and routine maintenance all require appropriate Change Management. Change management ensures the stability of systems by the identification and mitigation of associated implementation risks, minimization of disruption to Prince Mohammad University's operations caused by system outages,
and improves service and service levels provided to the University.

The Change Management policy is based on the industry best-practice standards of ITIL – the IT Infrastructure Library.

This policy outlines the ITD Change Management process, including its roles and accountabilities.

Purpose

The goal of Change Management at Prince Mohammad University is to ensure that standardized ITIL (IT Infrastructure Library) methods and procedures are used for efficient and prompt handling of all Changes to the IT systems; thus minimizing any undue disruption to IT services delivered to the University.

Change Management also aims to provide the ITD the ability to rapidly adapt as University's requirements change and increase their ability to ensure a customer focused operation is maintained

To ensure that a comprehensive business and technical risk assessment is made for all changes, allows for open communication between key stakeholder and coordination of resources required for successful implementation.

Definitions

PMU: Prince Mohammad University

ITD: Information Technology Department

ITIS: IT Infrastructure Services

Change Management: is the process of developing a planned and documented approach to change in an organization.In the ITIL framework, Change Management is responsible for controlling change to all configuration items within the live environment, test and training environments, and all environments under the control of ITD operations. It is not typically responsible for change within development projects where change requests are managed by the Project Manager.

CAB: The Change Advisory Board. As can be inferred from the name, this body has no governance role, but is tasked with *advising* the Change Manager and Service Owner of the perceived impact of a requested change. This body is made up of a core group with representation from all major systems and the core Services teams, and incorporates required stakeholders depending on the nature of the Request for Change being assessed.

ITIL: The IT Infrastructure Library is a collection of internationally recognized best-practices for delivering IT Services, covering all aspects of service provision, quality assurance, and providing a framework which allows customization of internal processes. It was developed within the British Public sector and has since been revised with commercial input to become the world standard for IT Service Management.

RFC: Request for Change – an electronic form which initiates the Change Management process.

CM Change manager: is a Chair of the CAB meeting and will be responsible to select the CAB members per the nature of the RFC. CM is also responsible for scheduling and publishing approved changes.

Service Owner: is a person or department responsible to provide the service for the business.

Change Management Process Development

Guidance from ITIL

The Change Process at the Prince Mohammad University has been based extensively upon the guidance of the British Government "Information Technology Infrastructure Library" textbooks (ITIL). Wherever possible, this guidance has been followed closely, most notably in the use of the ITIL terminology.

The ITIL texts provide comprehensive guidance as to industry best-practice in this area, and have been widely adopted as standards to ensure IT infrastructure stability and resilience.

ITIL forms the basis of the British Standard BS15000 and International Organization for Standardization ISO20000.

Process Development

The Change Management Process was developed within the ITD and implementation will be staged. The benefit of this approach is to work on the process iteratively, allowing various approached to be trialed before formal adoption

Process Improvement

The Change Management Process will undergo continuous improvement. The primary source of improvements will be the review phase of the process, wherein the Change Advisory Board members analyze and identify process improvements which will enhance success or increase the efficiency of the process.

Constructive feedback is welcomed, and suggestions for improvement will be incorporated wherever value is added.

Change Management Process Notes

Change Process Scope

Currently the scope of this process is limited to ensure a successful staged implementation. All changes to centrally managed IT infrastructure and Systems must follow the PMU Change Management Process.

This scope is further limited to changes for which an outage or noticeable change is visible for clients. This ensures the process is not swamped by minor operational changes, and reduces the bureaucratic overhead of the process.

Integration with the (Purchase Department) Approval Process

Where Purchase Department approval is required for IT equipment or software purchases, an assessment of the impact of the purchase should be sought through the PMU Change Management process. The appropriate place for this integration is prior to distribution of Request for Proposal made by office of CIO

In some instances, assessment may be requested to provide information for inclusion as part of the development of the business case.

Change Type

The type of the changes which follow the Change Process varies. The following categories have defined:

- Pre-approved
- Minor
- Medium
- Major
- Urgent
- Emergency
- Installation
- Evaluation

The type of the Request for Change (RFC) affects the timeline of the request, determines the notifications which must be sent, and the review and closure process to follow.

Pre-Approved Changes

Many changes do not require authorization, and do not need to pass through the formal process. Those changes should still be logged in the normal manner; however they will proceed to the scheduling phase immediately.

This is essential to ensure appropriate change scheduling, and the minimization of impact arising from change conflicts. It also provides and audit trail of

improvement made to systems and services. In CAB review phase the minor or medium changes done frequently can be categorized as Pre-Approved Change.

Minor or Medium Changes

Minor or medium changes follow the standard change process and may affect relatively few clients or cause minimal impact; however they do require proper notification of selected groups of staff or students.

Major Changes

Major changes are designated as such because the affect, or have the potential to affect, large numbers of clients, or will involve lengthy outages of critical systems.

Major changes will typically involve notification of all staff or students and may require authorization by Senior University Management (IT supervisory committee, Communication meeting)

Urgent Changes

Urgent changes are designated as those which are not able to follow the standard change implementation timeline. These may occur due to external factor such as consultant availability or external project critical timelines, possible hardware failure, or simply due to scheduling issue necessitating implementation in conjunction with other previously scheduled changes.

As these changes fall outside the normal change window, a special meeting of the CAB may be held, or consultation prior to approval may be made by email.

All urgent changes will be reviewed by the CAB post-implementation. This will ensure that appropriate measures are taken to reduce or eliminate the requirement for such urgency.

Emergency Changes

Changes may be designated at the time of recording as 'Emergency' changes. These changes will not be required to follow the standard Change Management Process, but instead are automatically approved and proceed directly to implementation. Emergency changes naturally take schedule precedence from all other changes.

All emergency changes are reviewed by the CAB, following implementation.

Installations

All new systems to be commissioned within the IT managed server facilities must be submitted as an RFC. This allows the CAB to assess the request for business and technical risk and ensure appropriate resources are allocated. It also automates the creation of appropriate work requests to ensure all standard tasks for preparation take place.

Evaluations

The process for the evaluation of a new item of equipment or software prior to its sale or support is important in order to ensure support criteria are met. The inclusion of a change type for the evaluation of new equipment etc reflects this importance, although it constitutes a variation on the standard process.

Request for evaluation are circulated to a number of key areas of ITD, to ensure appropriate checks take place prior to introduction.

The Change Advisory Board

Overview

The Change Advisory Board (CAB) is the body responsible for the assessment of changes to determine their risks and impact, and authorization of RFC implementation or otherwise.

Given the complexity of computing environment a CAB has to be developed which has the depth to ensure accurate assessment and identification of risk and impact , both from a business viewpoint , and technical and support issues. The method chosen in this instance has been to establish a "core" CAB of relevant staff from the IT infrastructure services and mission critical MIS system, which will almost always be involved in change assessment, and then bring other appropriate stakeholders into the assessment when required.

The members of the core CAB:

- Change Manager
- Infrastructure Supervisor
- MIS Supervisor
- Academic Supervisor

- Business Representative

In essence the CAB has a dynamic membership so we do not waste the time of those that particular changes do not impact upon. This follows the industry best-practice guidance provided by ITIL.

Additional CAB members relevant to each change are added to the group based on the services affected by a particular RFC. In particular this includes the service owners of all affected services. A further list of stakeholder for inclusion in the assessment includes representation from all service units and academic colleges and is built in consultation with those units. It may include a technical support of management staff with vested interest in the service

These stakeholder will be given the opportunity to submit an assessment of relevant changes, however they will not be required to attend the regular CAB meetings , although they are welcome to do so.

CAB Responsibilities

- The responsibilities of the CAB members are:
- Identification of business , technical and support risks associated with the implementation of the RFC
- Identification of the direct or indirect costs and resource requirements
- Identification of impact on any other University services
- Identification of impact on PMU operations not directly associated with the change
- Circulation of assessment and collation of responses from team members
- Timely response to requests for assessments
- Assisting the Change Manager with authorization of RFCs

CAB Meetings

The CAB will meet weekly to perform authorization, review and closure of RFCs. The Change Manager is responsible for scheduling and rescheduling the meeting.

Time frame

As the CAB meets weekly, impact on timeframe for implementation should be minimal, given appropriate planning prior to RFC initiation.

Agenda

The CAB meeting will be chaired by the Change Manager, and will follow a standard agenda.

Authorization

Discuss RFCs in assessment phase
Approve or Reject RFCs

Scheduling

Schedule changes
Ensure ITS Change Calendar is updated

Notifications

Ensure all RFCs include proper notification
Emergency and Urgent RFC Review

Closure

Close all outstanding completed RFCs

Review

Review failed changes
Improve the IT Change Management Process

The agenda of RFCs for assessment will be circulated to CAB members and notified via email prior to each meeting.

Urgent Meetings

An ad-hoc urgent CAB meeting may be called as and when required for urgent changes. This may be conducted via email if required.

Quorum

For IT infrastructure changes, a quorum of four CAB members must be present

in order to authorize any RFC. In the absence of sufficient CAB members, all changes may be deferred until a time a quorum can be obtained or referred to Service Owner, IT Directors, and Chief Information Officer to authorize.

Authorization

For an RFC to be authorized, it must be approved unanimously by the CAB, having taken into account the assessments submitted. Should a unanimous decision be unachievable , the RFC will be referred to Service Owner , IT Director or Chief information officer for a final decision.

Reporting

An essential element of the Change Management Process is the requirement to ensure the IT supervisory Committee and Senior Management are well informed about all Changes relating to mission critical systems, especially those for which they have delegated accountability.

The Department heads and Service Owner identified for each MIS system are to be included in automated reporting. The Forward Schedule of Changes will also be circulated to ITD Management and Senior Administrators monthly.

Process Overview

Initiation / Recording

Due to the variety of the changes that may be required, specific Request for Change forms is designed to suit the type of change. They are as follows (see Appendix A for templates):

The proper recording of changes is essential to this process. All changes must be submitted either electronically or by tools approved by PMU.

RFCs must be filled out in full and include the following information:

Initiator	The person requesting the change should fill in their userid. All communication with the initiator will then be made by email
Service Affected	To identify the Owner and stakeholders of the

	service which are to be consulted and given the opportunity to take part in the RFC assessment.
Requested Date	This indicates the data and time on which the initiator wishes to implement the change. Both date and time are required to assess the impact of outages.
Critical Date	In most cases the requested date will become the implementation date. The exception to this is when the request conflict with higher priority change already in the system, or when another critical date is indicated by the assessment. The critical date should be the date by which this change must be implemented. It will be used to resolve scheduling conflicts only
Change Description	Describe the requested change in detail, providing as much information as required for other staff to understand and make an appropriate assessment. This change description should include details of the implementation plan, if appropriate.
Reason for Change	Why is this change being requested? Is It to fix a known problem? If so provide the provide the problem number.

Who will this Change effect?	The RFC initiator should provide their assessment of the impact of this change. Which clients will be affected? Will other services be affected? Which staff will be required for the implementation? The CAB will ensure appropriate representatives from this list provided are advised of the change and allowed an opportunity to provide their assessment.
Length of an outage	If there is to be an outage associated with this Change, please indicate the length. Approximation should be accompanied with some explanation.
Back out plan	If the change implementation fails, what plans have been made to reverse the change? These plans

	should be comprehensive, as in the case of a failed change, they will be reviewed by the CAB to identify area for improvement.
Change Type	Indication of the type of RFC: Pre-Approved , Minor , Medium , Major , Urgent or Emergency
Notification Text	What message should be sent to the clients?

Filtering

It is essential that indicated fields are filled in, and the system/CM will not save the requests without identification of the initiator, change description, requested date and back-out plan.

The above filtering can be done at form level or by using tools approved by PMU. policy Filtering of RFC also takes place to ensure changes are not submitted to the process which are erroneous and frivolous or requested by unauthorized staff.

Initial errors in the completion of the RFC form must be quickly identified, as must any missing information. RFC record may be updated by the Change Manager, CAB members, or the RFC initiator. All changes made will be logged to ensure proper audit trail.

Inputs

Completed RFC form

Output

Filtered and corrected RFC

Roles and responsibilities

Responsibility for filtering the RFC form and ensuring accurate information has been recorded lies with the Change Manager. In the absence of the Change Manager this responsibility lies with the members of the core CAB.

Assessment

Assessment is one of the key phases of the process. Request for change will be forwarded via email to the CAB members for their assessment. The CAB is responsible for assessing the RFC and providing their assessment of:

- Business and technical risks associated wit the RFC
- Impact on any other PMU Services
- Impact on PMU operations not directly associated with the change
- Direct or indirect Costs and resource requirement

Email notification will be sent to all core CAB members , the Service Owner , and identified service stakeholders following successful RFC and collation of responses from other affected colleagues (where necessary). The notification of assessment can be forwarded to other staff members if required.
CAB members have a responsibility to ensure they respond to requests for assessment in a timely manner. Should no response be submitted, it will be assumed that no impact is foreseen in their area and therefore they approve the RFC.

Requests for further Information

CAB members may also use email to request more information from the initiator. The initiator may respond by email. Following response, the CAB will be informed of both the question and the answer provided to assist with their assessment. This will highlight areas of the RFC where clarification is required and may also result in revisions to components of the process itself.

Inputs

RFC

Outputs

CAB assessment
Assessed change for authorization

Roles and Responsibilities

The change Advisory Board members have a responsibility to assess all RFCs to the best of their ability and knowledge.

Assessment should be provided within two working days of notification

Categorization

Taking place in parallel with the assessment phase the RFC is categorized on a number of aspects.

Source

The source of the change is categorized in order to identify whether the RFC is the result of a fix to a known problem, a new service, an installation, a patch or upgrade, or a client requested enhancement.

Service

It is important that the service to be changed is identified, as this allows the identification of relevant stakeholders who would then be requested to take part in the assessment.

Impact

The impact of the change is the extent to which it affects PMU's operations, based roughly on the number of clients affected by the change, or the business critical nature of the services affected.

Urgency

Urgency provides an indication of the extent to which delay of implementation can be tolerated

Priority

The combination of Impact and Urgency allows us to priorities RFCs appropriately; ensuring resources are targeted where they are most needed and eliminating scheduling conflicts.

Scale

The scale of the change gives the CAB an indication as to the level of authorization required.
These categorizations are important to monitor the nature of changes, and to ensure efficiency of the process. They also contribute to the approval and scheduling phases of the process.

Authorization

Following assessment by the CAB, the RFC will proceed to authorization.
All RFCs are authorized by the CAB during the weekly meeting or by special arrangement if the RFC is designated urgent. Authorization will be based upon the collected assessment made by the CAB members , and will balance the expected benefits of implementation with the business and technical risks identified, the urgency of the change and the predicted impact on clients or PMU operations.

All changes to centrally managed IT infrastructure will be authorized by the CAB itself. In the case of RFCs which are for MIS systems, a recommendation for approval or rejection, and the CAB assessments will be forwarded to the Service Owner or appropriate authority for formal sign-off. Those changes which will impact on several critical MIS systems will be referred to higher authorities depending on the scale of the change.

For an RFC to be authorized, it must be approved unanimously be the CAB, having taken into account the assessments submitted. Should a unanimous decision be unachievable, the RFC will be referred to the Service Owner, ITIS Director or CIO for a final decision.

Following the CAB meeting the appropriate RFC will be updated, setting its status to Approved or Rejected, and specifying any points noted by the CAB during the discussion.

Approval of the RFC will result in the notification of the CAB members, the Service Owner, the Initiator, ITIS Director and CIO

Rejection of the RFC will result in notification of the initiator with the reason for rejection.
No unauthorized RFCs will be implemented. The decision of the CAB or Service Owner will be final. The RFC may be re-submitted provided that all the issues resulting in the rejection have been mitigated.

Inputs

• CAB assessments
• RFC

Outputs

• Recommendations for approval or rejection to the Service Owner.
• Approval or rejection notification to the Initiator,
• Notification to ITD Management
• Notification to Service Owner
• Notification to CAB members

Scheduling

Proper scheduling is important to ensure change implementations do not conflict and cause undue impact on the PMU operations.

The IT change calendar should be published on the Intranet. This should be the definitive source of change schedule information, and is updated automatically directly from the Change process.

Changes requested for implementation within the same time period are rescheduled based on the impact and urgency of each change

Input

Approved Changes
Existing Change Schedule

Output

Updated Change Schedule

Roles and responsibilities

Scheduling is the joint responsibility of the Initiator, the Service Owner and the Change Manager.

Notification

All notification to Clients should be broadcasted. This ensures consistency and reliability in notification process and content. This is especially important where outages may affect client operations, or where an outage to normal service is involved.

All notification will include reference to the appropriate RFC and links to the ITS change Calendar.

Notifications will only be sent following proper change authorization.

No change notification to be sent by any other party.

All RFCs which are rescheduled must be notified to clients, firstly to inform them of the cancellation of the original change or outage window, and then to provide details for the updated schedule.

Inputs

Scheduled Change
Notification text via RFC

Outputs

Notification to appropriate client groups

Roles and responsibility

Responsibility for notification lies with the IT help Desk / or the Change Manager.

Implementation

- From a change management point of view, the implementation of the change should follow the plans provided as part of the RFC.
- Success or failure of the implementation must be promptly reported to the IT
- Helpdesk, as must any known issues created by the implementation.
- Following the scheduled date of implementation, an email message will be sent to the initiator requesting a status update.
- On the requested implementation date, a problem record will be created and all incidents attributed to this implementation will be recorded efficiently which will provides raw data for change review phase.

Inputs

Authorized and Scheduled RFC

Outputs

Successful or failed change
Problem record with associated incident

Roles and responsibilities

The Initiator has responsibility for ensuring the implementation follows the suggested plan, and that back out plans are implemented if required. They are also responsible for ensuring appropriate staffs are available to assist with implementation, when and if required.

Review

All changes which fall into the following categories are reviewed:

- Failed Changes
- Changes which exceeded the specified outage window
- Emergency or urgent changes
- Changes causing unexpected or unreasonable incident volumes

Changes falling into these categories will be passed to the Change Manager, who will ensure appropriate investigation take place, circulate a written report, and facilitate discussion to ensure any improvement to the process, or to the implementation can be identified and actions are taken to resolve.

All stakeholders and relevant Service Owners will be requested for information pertaining to the impact of RFC upon their operations, and will also receive a formal review report at the end of the process.

Inputs

Implemented Changes

Outputs

Review document to CAB m Stakeholders and Service Owners
Process Improvements

Roles and responsibility

The CAB members are responsible for appropriate review of changes and identification of improvements or additional safeguards to ensure future successful change implementation.

Closure

The formal process of RFC closure is the final step of the change Management process
The CAB members will close all RFCs formally at the normal CAB meeting, following any review or discussion required.

Inputs

Completed RFCs

Outputs

Closed RFCs

Roles and responsibilities

The Change Manager has the formal responsibility for RFC record closure.

Reporting

The PMU change management process incorporates several key communication opportunities.

Change Calendar

The Change Calendar will be published via the web as publicly available information. It is updated dynamically upon each visit. This allows all interested parties to see those changes which have been authorized, are still to be assessed etc.

Forward Schedule of Changes

The Forward Schedule of Changes is circulated to the ITD directors and IT Supervisory Committee where appropriate. This keeps those bodies informed of all upcoming changes.

Management Reporting

An essential element of the Change Management Process is the requirement to ensure Service Heads are well informed about all Changes relating to mission critical systems, especially those for which they have delegated accountability.

Change Process Metrics

Each step of the process should have associated metrics which allow the process quality to be monitored, and improvements to be identified.

Example metrics include:

- Time to assess
- % failed changes
- Number of assessments per RFC
- Impact as per incidents recorded

Policy 07: Data Center Operations

General Guidelines

- Staff and visitors alike may not tamper with, or in any manner adversely affect, security, infrastructure monitoring, and/or safety systems within the Data Center.
- Smoking, drinking, and eating are strictly prohibited within the Data Center raised floor space.
- Unless otherwise expressly permitted in writing, storage of combustible materials (e.g. wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids or solvents) are prohibited within the Data Center.
- Sharing Data Center Proprietary information (like architecture, design, facilities information and services) without the express written permission is strictly prohibited.
- All hand-carry containers, boxes, bags, laptops, purses, backpacks, or equipment carried into or out of the Data Center are subject to inspection by Data Center staff and/or Security.

Physical Security

- Data Center is a secured facility. Access to the data center and other areas of the facility are restricted to persons with authorization.
- Security controls include 24 x 7 security officer presence, sign-in procedures for all ingress and egress, managed key and access card plans, managed access permissions and access request methods.
- Ingress and egress to Data Center is monitored on Closed-circuit television (CCTV) cameras
- Tampering with, or in any manner adversely affecting, security and/or safety systems within the Data Center is strictly prohibited.
- Safety and Security Departments has the right to access any part of the Data Center at any time for safety and security reasons.
- All persons entering the Data Center must:
    - Possess either authorized staff ID or authorized visitor ID
    - Have Authorization to access the facility

Rack/Cabinet and Cabling

- All refuse materials (which include, but are not limited to boxes, crates, corrugated paper, plastic, foam packing materials, and any other materials which are non-essential to the operation of equipment) must be removed. Materials must be placed in designated disposal
- All spare equipment shall be stored in a cabinet or must be kept in approved plastic or metal containers. Containers must be sealed, stacked neatly and can not impede ingress/egress or cooling.
- The tops of the cabinets or racks may not be used for physical storage.
- Mounting or hanging anything on walls of Data Center or on housed cabinets is prohibited
- “Un-racked”, operating equipment outside of cabinets/racks is strictly prohibited.
- Unsecured cabling across aisles or on the floor is prohibited. All devices must be installed in racks or cabinets.
- Cable wrapping, wire management, zip ties and/or Velcro, must be used to organize cabling in a rack or cabinet
- Cabling must not obstruct airflow / ventilation /AC (perforated tiles) or access to power strips
- All Network connected equipment is labeled with host names.

Floor Tiles

- The sub-floor (access floor) area is restricted area, accessible by or in the presence of Data Center Management Staff. The perforated tiles are strategically placed for HVAC cooling patterns in-line with the cooling requirement of the equipments/racks/cabinets

Power Protection and Backup Policy

- Main Utility Power Supply to the Data Center need upgrade should the load reaches 80% of the installed capacity
- Emergency Power Generator facility with Automatic Transfer Switch (ATS) is available to support Data Center facility for 72 Hours in absence of

Utility Power Supply

- All the Distribution Communications rooms are equipped/supplied with Emergency Power in order to provide communications facility via UPS provision of power to all switches
- Power Supply to the equipment/racks/cabinets are drawn from two different panels to provide redundancy
- All the equipment housed in Data Center is properly grounded/bonded
- Sizing of the Power Protection & Power Backup device is 50% more than the projected load
- Power Backup time is greater than or equal to 90 minutes on full projected load. The system sends alert Emails/messages to the Data Center Management Staff.
- Equipment brought into the Data Center is powered in consultation with Data Center Management in order to help calculate and determine additional power draw for the new equipment being installed

Data Center Environment Policy

- Data Center temperatures are recorded/monitored and maintained in a range of 18-22 degrees Celsius
- Relative Humidity is recorded and observed in a range of 45-55%.
- Precision AC units work in rotation with at least one unit being standby at all times.
- Adequate fire detection/alarm and suppression systems are in place
- Leak detection system is in place to monitor and report on any seepages of liquids

Supplement on Disaster Recovery

Introduction

This functional policy covers PMU's Backup & Recovery Polices. The primary purpose for the backup system is to provide for disaster recovery of key network servers and services. The backup system is not an archival system for storing information off-line for indefinite periods of time, and is not set up to recover individual email messages. It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement wherever required is supported by standards, procedures to achieve a complete security framework at PMU.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Backup & Recovery Functional Policies:

- Identify computerized systems that store information.
- Implement standard frequency of backup for each type of system or platform in use based on the significance of the information and its frequency of change.
- Implement procedures for transferring a recent copy of backup media to a physically and environmentally secure off-site storage location.
- Ensure that documented procedures exist for the recovery and restoration of information from backup media.
- Monitor backup and recovery procedures and practices to ensure compliance with this policy.
- Identify I.T. staff responsible for ensuring successful back-ups.
- Transport or provide for the transportation and storage of current backup media at an off-site storage Location.
- Ensure that a recent copy of backup media is stored off site at all times.
- Determine that the off-site storage location has sufficient physical and environmental controls to ensure the safety of backup media.

Backup & Recovery Functional Policies

Operations

- Backups are scheduled to run daily; files that were captured in weekly backup will be available for restore for a period of 3 months.

Accidental Deletion, Overwrite, Corruption

- A file that has been accidentally deleted can only be recovered from the backup system if that file existed on the network at the time of the last backup

Schedules

- Backups are to be performed, usually incremental backup daily refered as Incremental Backup.
- Schedules must be followed to perform Incremental Backup; full backup schedule should be developed to perform certain backup.
- Incremental backup will be performed request

Retention

- Depending on the type and location of the files, backup tapes are kept available for recoveries for a minimum period of 1 to 3 months before being recycled. After that, tapes should be recycled (information is overwritten) as necessary to keep the backup system running
- Off-site monthly backups to be retained for 1 year.

Notification

- System Owners/Application owners to be notified of the status of daily backups
- Weekly status of the backup system to be notified to the office of CIO.

Recoveries

- Any file stored on a network server should be "recoverable" from tape after it has entered the backup cycle, and as long as the tape has not exceeded its retention period.
- A request for a recovery must be made to support personnel (helpdesk).
- It is not possible for individuals to recover their own files for security reasons.
- When a recovery is requested, the most recent version of a file that can be successfully recovered should be restored to the network server.
- The backup system cannot recover modifications to a file made between the last successful backup and the point of failure
- The files stored on Network Drive can be requested to be restored.

Users Responsibilities

- Users must provide support personnel with three pieces of information in order for any file to be recovered.
    - When the file was lost, deleted, overwritten, or corrupted.
    - The name (spelled correctly) of the file to be recovered
    - The full directory path to where the file was located should be passed by the user.
- Users are responsible for backing up any data not stored on Authorized Servers.

Operators Responsibilities

- Backing up systems on a daily basis /weekly basis
- Backing up all necessary data files and programs to recreate the operating environment
- Storing backup copies at an off-site location sufficiently distant from the data centre to ensure their protection if the original system is destroyed
- Backing up the printed documentation and pre-printed forms necessary for recovery
- Ensuring that backup is not continually performed on the same set of tapes
- Testing the backup to determine if data files and programs can be recovered

- Ensure that the following are stored at an off-site storage location:
    - Source and object code for production programs
    - Master files and transaction files necessary to recreate the current master files
    - System and program documentation
    - Operating systems, utilities, and other environmental software

Procedures Supporting Policy

Policy 08: Security

Introduction

It is each user's responsibility and obligation to ensure that all resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption. This FP Intends to Clarify to all users on PMU infrastructure, what their responsibilities are; Define what the potential risks and dangers are for PMU in the event of misappropriation and abuse of Infrastructure users; and regulate the professional and effective use of Infrastructure within PMU as well as between PMU and external entities.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets
- All software assets
- All physical assets, such as computer and network equipment
- All supporting services, such as power and network link
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy Statements govern the General Security Guidelines:

- Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined;
- A management authorisation process for new information processing facilities must be established;
- Advice on information security provided by in-house or specialist advisors must be sought and communicated throughout the organisation;
- Arrangements involving access to organisational information processing facilities by an organisation handling the outsourcing must be based on a formal contract containing all necessary security requirements;
- An inventory of all-important assets must be drawn up and maintained;
- Owners must be identified for all major assets and the responsibility for the maintenance of appropriate controls must be assigned.
- A regular inventory of assets must be performed.it's a necessary security requirements;
- Classifications and associated protective controls for information must be suited to business needs for sharing or restricting information and the business impacts associated with such needs;
- A set of operational and security procedures must be defined for information labelling and handling in accordance with the classification scheme adopted by the PMU
- An information classification scheme must be implemented
- Aspects related to information security must be addressed in an employee's terms and conditions of employment and for third parties, with a formal contract with PMU;
- Any security related incidents must be reported immediately through the established channels after the incident is discovered;
- Users of information services must be required to note and report any observed or suspected security weaknesses in or threats to systems or services;
- Mechanisms must be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored;
- The violation of organisational security policies, functional policies and procedures by employees must be dealt with through a formal disciplinary process;

- Physical security perimeters must exist for all areas housing relevant information processing facilities;
- Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access;
- Secure areas must be created in order to protect offices, rooms and facilities having special security requirements;
- Additional controls and guidelines for working in secure areas must be used to enhance the security provided by the physical controls protecting the secure areas;
- Delivery and loading areas must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access;
- Access to the machine rooms must be restricted to only those people who are permitted to use the machines;
- Access to the machine rooms must be monitored for illegal access attempts;
  Any information processing equipment, used for information processing on PMU's systems, but situated outside PMU's secure perimeters, must be secured in a way equivalent to PMU's on-site equipment;
- Information must be erased from equipment prior to disposal or re-use;
- No employee must be allowed to remove property from the PMU premises unless they have obtained authority to do so from an approving manager;
- PMU must have and implement a clear desk and a clear screen policy in order to reduce the risks of unauthorized access, loss of, and damage to information;
- Removal of any equipment, information or information facilities that belong to PMU, from the premises must be strictly monitored and controlled;
- Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to security incidents;
- Duties and areas of responsibility must be segregated in order to reduce opportunities for unauthorised modification or misuse of information or services;
- Detection and preventive controls to protect information and information processing facilities against malicious software and appropriate user awareness procedures must be implemented;
- Back-up copies of essential business information and software must be taken regularly;
- Systems and applications backup documentation must include the following information:
  - Ownership;
  - Procedures;
  - System dependencies;
  - Data validation results; and
  - Source code.
- Operational staff must maintain a log of their systems operation activities;
- Faults must be reported immediately and corrective action taken;
- Regular inventory of backup media must be performed;

- The management of removable computer media, such as tapes, disks, cassettes and printed reports must be protected and controlled according to its classification;
- Media must be disposed of securely and safely when no longer required;
- Procedures for the handling and storage of information must be established in order to protect such information from unauthorized disclosure or misuse;
- Controls to prevent unauthorised access to system documentation must be developed;
- Content scanning must only be enforced in checking for malicious software, viruses or violations;
- The allocation of passwords must be controlled through a formal management process;
- A formal process must be conducted at regular intervals to review users' access rights;
- Operating systems and applications must include as a minimum, adequate user access controls, password controls and monitoring controls;
- PMU must enforce all users to follow good security practices in the selection and use of passwords;
- Users must be required to ensure that unattended equipment has appropriate protection;
- Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly;
- Users must not install modems in office PC's and dial in to those PC's;
- Functional policies and procedures on the use of cryptographic controls for the protection of information must be developed and followed;
- Encryption must be applied to protect the confidentiality of sensitive or critical information;
- Digital signatures must be applied to protect the authenticity and integrity of critical electronic information, where necessary;
- Non-repudiation services must be used to resolve disputes about occurrence or non-occurrence of an event or action;
- Modifications to software packages must be discouraged and essential changes strictly controlled;
- The purchase, use and modification of software must be controlled and checked to protect against possible covert channels and Trojan code;
- Controls must be applied to secure outsourced software development.

General Security Functional

Desktop Confidentiality

- To promote desktop confidentiality the following must be adhered to:
- In an open plan office users must be aware of unauthorized users reading

information displayed on their screen.

- Users must switch off their computer when it will be left unattended for an extended period of time,
- No obvious links or shortcuts to sensitive documentation must be created, e.g. shortcut for “Marketing Information.doc” on the Windows desktop.
- All Windows desktop backgrounds must be in accordance with PMU Policy
- No proprietary information must be posted on the computer screen, i.e. with post-it stickers.
- Clear Screen
- The controls pertaining to a clear screen include:

Screen Savers

A password protected screen saver will obscure the content of your computer screen after a period of no activity. Use of screen savers must be used in accordance with the following:

- User must enable screen savers on their computers, which will require input of a password if inactive for more than 15 minutes.
- Users must use screen savers, which promotes PMU business and does not offend, intimidate or disparage others.
- Users must change their screen saver password regularly,.
- Users are not allowed to disclose their screen saver password to any personnel without authorization from their direct manager at PMU.
- When entering passwords users must prevent unauthorized observation by any third party, e.g. shoulder surfing.

Computer lockout

Computer lockout must be in accordance with the following:

- Users must lock out of their workstation(s) and any active applications or log out when leaving their computers unattended.
- Users must not disclose their passwords to any personnel who want to unlock their workstation without authorization.
- A user must ensure they have logged out of all systems, including the network, after hours.

Passwords

- **Creating Passwords**: Creation of passwords must be in accordance with the following:

- Passwords must be a minimum of six (6) characters in length for regular users, eight (8) characters in length for managers and other privileged users, and must comprise of letters, numbers, and special characters to the extent possible.
- Passwords must not be easily associated with PMU or the user (i.e. identification number, employee number, address, numerical equivalent of name, family names, birthdate, spouse name, pet names etc.).
- Passwords must not contain:
- Words from a dictionary, movie or geographical location;and
- Common character sequences such as “123456”.
- Passwords should not be based upon month/year combinations such as "jan01" or "april2001". ‘Hackers’ use these types of words in attempts to guess passwords.
- Users will not use cyclical passwords. For example, users cannot add a numeric at the end of the password in sequence.
- Passwords must not consist of identical all numeric or all alphabetic characters, for example 1111111 or aaaaaaa.

- **Safeguarding Passwords:** For effective safeguarding of password, users must adhere to the following:

  - A password must be known only to the user who creates it. Passwords must not be shared with others.
  - A password must not be shared except in a temporary emergency situation. If a situation requires a password to be revealed to a second person, the owner of the password must change the password as soon as possible after the emergency situation has passed.
  - Passwords must not be stored in readable form (i.e. writing down passwords).
  - Passwords should be changed:
  - Every 45 days or less for supervisors and other privileged users and every 90 days or less for regular users; or
  - Whenever there is any indication that the user’s password has been compromised, passwords must be changed immediately.
  - As an exception, password for application user ID may be set to “never expires”, provided the password is encrypted.
  - Temporary passwords assigned to users must be changed at first log-on.

- **Handling of Privileged Passwords:** Privileged passwords, such as root or super user, are powerful passwords. As such, the custodians of these passwords must properly handle them by adhering to the following:

  - A privileged password must be known only to the Administrator responsible for the system. The backup administrator should have

no knowledge of it.

- In case of emergency and in the absence of the Administrator, the backup Administrator should be given access to the password with the proper approval from his Dept. Manager. The Emergency Password form should be filled up by the requester and signed by the Dept. Manager.
- The custodian of the privileged password must use his own account to log into the system. He should then switch from his own account to the privileged account.
- After using the password, the backup Administrator should change the password,
- When the Administrator returns, he should get the new password from the backup Administrator & change it.

Virus and Malicious Software Protection

- Virus Detection Programs
  - ITD should ensure that the latest version is installed on all computers.
  - Users are not allowed to remove or de-activate virus detection programs installed on their computers, without approval from ITD.
- Preventing Viruses
  - Externally supplied floppy disks, CD-ROMs, and other removable storage media must not be used unless they have first been checked for viruses.
  - Externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) must be unzipped prior to being subjected to an approved virus checking process.
  - If the files have been encrypted, they must be decrypted before running a virus detection program. Many virus detection programs cannot detect viruses in a zipped or encrypted file.
- Eradicating Viruses
  - Because viruses can be complex and sophisticated, users must not attempt to eradicate them without expert assistance.
  - If users suspect infection by a virus, they must immediately stop using the involved computer, disconnect from all networks, and call the Helpdesk.
  - If the suspected virus appears to be damaging information or software, users must turn the computer off immediately.

- Playing with Viruses

  Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any PMU computer system. Such software may be called a virus, bacteria, worm, Trojan horse, etc.

- Related Functional policies

  Users must adhere to the Protection against Malicious Software and Viruses Functional Policy in particular the following:

  - Users must not open e-mail attachments from unknown sources. All e-mail attachments received from known sources must be scanned for viruses.
  - Executable attachments (i.e. .exe) must not be launched and should be deleted immediately.
  - All software and/or freeware downloaded from the Internet or attachments from mail programs used on the Internet must be scanned for viruses.

Intellectual Property Rights Protection

General

- All personal computing device software must be obtained from approved sources, as defined by PMU.
- Software not supplied by PMU or at PMU direction must not be loaded or used on PMU personal computing devices.
- Obtaining or downloading of public domain and/or evaluation copies of software from other than PMU sources is permitted only under the following conditions:
- The software must be required for a legitimate business purpose and approved by management;
- Use of the software must comply with all applicable copyright and license agreements;
- At a minimum the person obtaining the software must perform an evaluation, as to the safety and reliability of the vendor or provider of the software; and
- The software should be checked for viruses and other malicious code. This evaluation should be done on a single system before deploying the

software to others.

Copyright Protection: PMU strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Users must therefore strictly adhere to the following conditions:

- Making unauthorized copies of licensed and copyrighted software, even if only for "evaluation" purposes, is strictly forbidden.
- Reproduction of copyrighted materials may only be allowed with the permission of the author/owner or a court of competent jurisdiction.
- If users have any questions about the relevance of copyright laws, they should contact PMU IT Department.
- Unless they receive information to the contrary, users should assume that software and other materials are copyrighted.
- It is the responsibility of each employee to protect PMU interests as they perform their duties. This includes responsibility for assuring that commercial software, acquired by PMU, is used only in accordance with licensing agreements.

Back-up Protection of Information

Periodic Back-up

- All proprietary and/or valuable information resident on PMU computer systems must be periodically backed-up.
- Unless automatic back-up systems are known to be operational, all end-users are responsible for making back-up copies of sensitive, critical, or valuable files. These separate back-up copies should be made each time that a significant number of changes are saved.
- Users must ensure the back-up process was successful by restoring selected files from back-ups made.
- Access to back-up copies should be properly restricted; e.g. storage media such as disks, etc. should be locked-up and access to back-up drives should be set up with user profile access control links.

Destruction of Information

Deletion of Information

- Users are required to delete information from their computers if it is clearly no longer needed or potentially useful.
- Use of an “erase” feature (e.g. putting a document in a trash can icon) is not sufficient for proprietary information because the information may still be recoverable.
- All disks and CDs must be formatted before given to any third party or employee of PMU not authorized to see content. Users should contact the Helpdesk for assistance on formatting disk and CDs after authorization has been obtained from the owner of the information.

Destruction of Information

- Electronic Media: Prior to disposal, defective or damaged disks containing proprietary information must be destroyed using scissors or other methods approved

Asset Accountability

Information Assets

- Users must not leave proprietary information unattended e.g. at a printer or on photocopy machines.
- All users must protect information in any format (hard copy, disk, tape, etc) at the level commensurate with its classification.

Software Assets

- Users must protect personal computing device software from theft, unauthorized use, and/or unauthorized copying.
- Users are not allowed to install or remove any software from any of PMU computing equipment.

Hardware Assets

- Computing Equipment: Users’ accountability for computing equipment must be in accordance with the following:
    - Users must not leave laptops unattended in an unsecured environment (on site or off-site).
    - Users must not leave laptops exposed in cars or hotel rooms.
    - User must never check-in a laptop as luggage when traveling. Always carry it on as hand luggage, in a briefcase

or a laptop carry case. Airport X-ray machines do not damage data on a laptop or diskette.

- Users must return any items issued to them (laptop computers, keys, ID cards, software, data, documentation, policys etc.) to their manager or the Human Resources (HR) Department upon resignation or termination.
- Users are accountable for any damage to computers and related equipment in their work area.
- Equipment and media taken off the premises should not be left unattended in public places.
- Equipment must not be exposed to extreme heat or cold.
- Avoid storing any devices (i.e. hard disks, etc) and equipment (i.e. laptops, desktops, etc) in automobiles.
- Automobiles and hotel rooms are potential theft areas. Store devices out of the view of others.

Use of Networking Facilities

Use of Modems

- Modems for office computers are not permitted. Mobile and telecommuting computers are an exception to this rule. The use of modems must be approved as per the policy.
- Do not provide IP addresses or dial-up access phone numbers to vendors and/or unauthorized parties.
- Any individual who requires an individual analog line for dial-in/dial-out must obtain approval from the IT Department.
- Remote access software such as PC Anywhere or Carbon Copy is strictly prohibited from use on PMU computing resources without the expressed permission of the IT Department.
- Persons using remote, e.g., in-dial, ISDN, wireless or Internet, access to an PMU information resource must be individually identified and authenticated by an independent dedicated device such as Firewall.

Unauthorized Browsing

- Users must not browse through PMU computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited.
- Steps taken to legitimately locate information needed to perform one's job is not considered browsing.

Identification of Security Incidents

Methods by which suspicious activity can be identified by a user include, but is not limited to:

- Unexpected account lockout;
- Unusual last login time; and/or
- Unknown files in their file areas.

Reporting Security Incidents

- All PMU users must watch for any potential security incidents including:
    - Breaches of confidentiality;
    - Denial of service;
    - Errors resulting from incomplete or inaccurate business data; and
    - Information system failures and loss of service
- Any such incidents must be promptly reported to the Helpdesk and/or their Information Security Officers thru phone call or e-mail.
- Reporting of Weaknesses
    - Users are required to note and report any suspected security weaknesses in, or threats to, systems or services.
    - Users must not attempt to prove a suspected weakness as testing weaknesses might be interpreted as a potential misuse of the system.
- Reporting of Software Malfunctions
    - Prior to reporting software malfunctions, the following should be considered by the user:
        - The symptoms of the problem should be noted;
        - Any messages appearing on the screen should be noted;
        - Use of the computer should be suspended and the computer isolated;
        - The computer should be disconnected from PMU network; and
        - Disks, which were used on the affected computer, should not be transferred to any other computer.
- Users must not attempt to remove the suspected software, unless authorized by IT.
- Disciplinary Action
    - Users must know and understand that in the event of an incident caused by user negligence, they will face disciplinary action.

- All users who commit security breaches will be subjected to a formal disciplinary process.

Controlling Configuration Changes on Computers

Changes to Software

PMU has a standard list of permissible software packages that users can run on their computers. Software package conditions that user must adhere to include:

- Users must not install other software packages on their computers without obtaining advance permission from IT
- Users must not permit automatic software installation routines to be run on PMU computers unless IT has first approved these routines.
- Auto discovery license management software may be used to remotely determine which software packages are resident on users' hard disks; unapproved software may be removed without giving user advance notice.
- Users are not allowed to download and install software, games and/ or freeware from the Internet.

Changes to Operating System Configurations

- Users must not change their computer operating system configurations, including:
  - Upgrade existing operating systems; and/or
  - Installing new operating systems.
  - If such changes are required and authorized, they will be performed by IT

Changes to Hardware

Computer equipment supplied by PMU must not be altered or added to in any way (e.g. upgraded processor, expanded memory, or extra circuit boards) without the prior knowledge of and authorization from IT.

Prohibited Use of Information Resources

- Any activity intended to degrade the performance of an PMU information

resource, circumvent security controls, or misuse the resource in any way is prohibited.

- Users are prohibited from attempting to access other user accounts and/or files to which access has not been expressly authorized.
- All information resources, including all owned, leased and contracted services involving word processing, minicomputers, mainframes, public telephone network elements and service bureaus, must be used only as authorized by PMU
- Unauthorized use of any PMU information resource may subject the user to disciplinary action, up to and including termination of employment, termination of a supplier, contractor or agency agreement,

Protection against Social Engineering

Social engineering is the practice of impersonating someone else to gain information or services in a fraudulent manner. Employees must take steps to avoid being the victims of social engineering. Required steps include:

- Know with whom you are communicating.
- If you do not know the caller personally or suspect the caller may not be valid, insist on a callback number and before returning the call, verify that the caller is legitimate.
- You can be “spoofed” via E-mail. The name and address you receive or send to via E-mail may not be the real name and address of the person. Do not send PMU or customer proprietary information or reply with PMU or customer proprietary information to E-mail addresses you do not know or cannot verify as correct.
- Make sure that the caller has a business need to know the information they are requesting. Never furnish proprietary information until the caller's need to know has been established.
- Users who become the victim of social engineering, or social engineering attempts must report the incident to IT immediately.

PMU Internal Network Security

- When connected to and using PMU internal networks, including Local Area Networks (LANs):
    - Do not misrepresent yourself (i.e., masquerade) as someone else on the network.
    - Unauthorized individuals should not monitor network traffic (i.e., use a "sniffer" or similar device) without first obtaining explicit management approval and informing IT.

    - Do not add any network device which creates an external connection (e.g. a bridge, router, gateway, hub, modem) to your workstation without first obtaining permission from your Provider of Service.
    - Do not install file sharing or peer-to-peer software (e.g. "Napster") unless PMU provides it.
- Sharing files on your own hard drive (via network connections) can pose the following threats:
    - Unauthorized access to data files
    - Damage to data/program files - either accidental or malicious
    - Damage caused by virus attacks
- If you must allow other users to access or store files on your network connected workstation:
    - You must select either User ID access control or password access control when defining the share options for the workstation disk drives and files.
    - You must not allow ANONYMOUS FTP, TFTP, or other unauthenticated access to program or data files on your workstation.

Physical and Environmental Security

Introduction

This functional policy covers PMU's Physical and Environmental Security. All information, systems and assets within PMU will enforce proper and strict physical access control. Physical security measures will be implemented to ensure the physical security and integrity of building facilities and computer centers. Protection measures will be appropriate to the classification level of the assets and information processed, stored, and handled within.

Objective

The objective of this Information Security Policies is to secure PMU Information Assets and staff. Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.
.

Governing Policy Statements

The following Executive Policy Statements govern the Physical and Environmental Security Functional Policies listed in this document:

- Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators must be maintained;
- The risks associated with access to organisational information processing facilities by third parties must be assessed and appropriate security controls;
- All risks resulting from third party access must be reassessed on a periodic basis, or whenever such risks change;
- Arrangements involving third party access to organizational information *processing* facilities must be based on a formal contract that must contain all necessary security requirements accompanied with appropriate responsibility and confidentiality undertaking. Any violations thereto must be dealt with accordingly;
- Arrangements involving access to organisational information processing facilities by an organisation handling the outsourcing must be based on a formal contract containing all necessary security requirements.

- Physical security perimeters must exist for all areas housing relevant information processing facilities;
- ITD must ensure that secure access areas be protected by appropriate entry controls to ensure that only authorised personnel are allowed access;
- Secure areas must be created in order to protect offices, rooms and facilities having special security requirements;
- Additional controls and guidelines for working in secure areas must be used to enhance the security provided by the physical controls protecting the secure areas;
- Delivery and loading areas must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.
- Access to the machine rooms must be restricted to only those people who are permitted to use the machines;
- Access to the machine rooms must be monitored for illegal access attempts.
- Equipment must be sited and protected to reduce risks from environmental hazards and opportunities for unauthorised access;
- Equipment must be protected from power failures and electrical anomalies;
- Power and telecommunications cabling carrying data or information services must be protected from interception or damage;
- Any information processing equipment, used for information processing on PMU's systems, but situated outside PMU's secure perimeters, must be secured in a way equivalent to PMU's on-site equipment;
- All access requirements must be based on a need to know, need to do basis;
- Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly.

Physical and Environmental Security Functional Policies

Access to PMU Premises

Physical Security Perimeter

- Based on a risk assessment, all PMU buildings must be classified and separated into secure areas. Based on the classification of secure areas

physical security measures must be implemented to provide adequate protection.

- For all PMU facilities, a security perimeter must be established. The strength of the security perimeter will be determined by an assessment of the risks and threats to the physical environment. The security perimeter includes, but is not limited to:
    - Clearly defining the facility and security perimeter boundaries;
    - Ensuring all physical perimeter components (walls, doors, windows, etc.) are physically sound;
    - Effective access control 24 hours a day, seven days a week;
    - Implementing a manned reception area to control access to the main entry of the facility and appropriate controls to secondary entrances;
    - Implement alarmed fire control doors as per local safety requirements; and comply with all applicable safety regulations.
- Any subdivision of the PMUfacilities requiring enhanced physical security must have its own physical security perimeters. These areas are referred to as “secure areas”. These areas would include, but are not limited to:
    - Computer data centres;
    - Security control centres;
    - Any vault or valuable storage facility;
    - Production or processing control centres.

Physical Entry Controls

- All PMU employees and visitors must be authorized by a PMU Head of Department/Business Unit and Security Department for physical entry into PMU facilities.
- Access rights to all areas must be reviewed on an annual basis.
- Access to areas deemed ”secure areas” (e.g. computer data centers, security control centers, valuable storage facilities or production processing centers), must be reviewed on a quarterly basis.
- Physical access to all computer rooms must be tightly controlled. Doors must be locked at all times with only authorized personnel having access.
- Authorized personnel must not allow unknown or unauthorized individuals into restricted areas without escort. Any unrecognized and unescorted personnel within a computer room must be immediately challenged to determine the reason for their presence.
- Personnel without a valid reason for being in the computer room must be escorted out of the computer room immediately and the Security Department must be contacted through the department head or his representatives.
- It is the responsibility of each employee, vendor or visitor that has been issued an access card to immediately report lost or stolen badges.

Securing Offices, Rooms and Facilities

All Areas

All areas within PMU which need to be secured, due to the nature of the information or assets they contain, must adhere to the following controls:

- All critical computer rooms and data centres will be monitored 24 hours a day. This monitoring can be by cameras, alarmed doors and windows, people manning the centres, or a combination of the above. This monitoring ensures that unauthorised physical access to critical resources and information does not occur.
- Buildings that house the Bank's computers or communications systems must be protected with physical security measures that prevent unauthorised persons from gaining access.
- Computer room access must be limited to only those people with a valid business reason for access. Access must be reviewed quarterly and revoked immediately once it is no longer needed.
- PMU computer and data centres are restricted areas. Programmers and users are not permitted unsupervised access to the computer centres.
- Directories and internal books identifying locations of PMU information processing facilities or any other sensitive or secure area must not be readily available or accessible to the public.
- Any hazardous or combustible materials must be stored at a safe distance from any secure area per local safety regulations and manufacturer specifications.
- All doors and windows must be locked when unattended and comply with any local safety regulations.
- Rooms containing wiring or communications equipment (wiring closets, PBX rooms, etc.) must be locked at all times with access restricted to authorised personnel only. Signs are not to be posted on wiring closets, telephone rooms and other equipment components that would attract the attention of unauthorised individuals.
- Computer facility rooms must be equipped with doors that automatically close immediately after they have been opened, and which set off an audible alarm when they have been kept open beyond a certain period of time.
- To avoid unnecessary access and damages, computer facility rooms must not be used for printing, faxing, storage of computers, parts of computers or stationary.

- Computer facility rooms must not be shared with third parties.
- There must be no signs indicating the location of computer or communications centres.
- Backup and recovery media and facilities must be located at a safe distance from main facilities. The backup facilities must be at a distance that would protect it from damage from any incident at the main site.

Secure Areas

- Any person working or having access to a “secure area” must be informed of the enhanced security requirements of the “secure area”, this includes:
    - The details of the security perimeter of that area; and
    - The associated responsibilities for the area.
- Recording equipment, like photo, video, audio is not allowed unless specifically authorised by an appropriate Department/Business Unit.
- Any third party access granted to a “secure area” must be strictly controlled and monitored. All parties with access to the area must be authorised and logged. This includes support services such as cleaning or waste removal.
- Any area deemed a “secure area” must be locked when vacant and physically checked periodically. The period of checks will be determined during the designation of the security requirements for that “secure area”' and creation of the security perimeter.

Equipment Security

Cabling Security

- Ethernet ports or network cabling must not be left unprotected. Exposed Ethernet ports or cabling can be used as an entry point to the PMU network by unauthorised users.
- All power and telecommunications equipment and cabling must be protected against deliberate or accidental interruption of service. This includes protecting control boxes, cables, wiring hubs and other equipment from fire, vandalism, interception of communications or disruption of service.
- All PMU network connections must be removed and/or deactivated when a site is being vacated. Unauthorised users can use Ethernet ports or cabling that are not removed or deactivated as an entry point to the PMU network.

Equipment Maintenance

- All equipment shall be under support and/or maintenance contracts. The level of maintenance taken out is to be appropriate for the importance of the item of equipment.
- All equipment must be maintained, monitored and inspected in accordance with the suppliers' recommended service intervals and specifications to provide availability and protect the integrity and confidentiality of information.
- Only authorised maintenance personnel are allowed to perform repairs and all repairs or service work must be recorded to identify potential failure patterns.
- If equipment must be sent offsite for repairs, the confidentiality and integrity of any information must be ensured.

Equipment Staging and Protection

- The level of protection that must be provided for any information resource within PMU must be assigned and will be dependent on:
    - The criticality of the service/operation being provided by the resource. For example, Is the service provided to a single user or multiple users? Is the service critical to PMU;
    - Effect of loss on supported services/operations;
    - The monetary value of the information resource;
    - Risk of theft; and
    - Value of the resource.
- A physical location must be determined for each information resource in accordance with its specified level of protection.
- Equipment must only be sited in a physical location after due consideration of the following potential threats:
    - Theft of equipment or vandalism;
    - Vibration;
    - Impact of disasters happening in nearby premises;
    - Electrical supply interference;
    - Electromagnetic radiation; and
    - Environmental factors, such mentioned in section 3.4.
- Computer equipment must be housed in an environment equipped with fire and water detection and prevention measures.

- Rooms adjacent to the computer facility room must not be used for purposes that may involve high risks (i.e. storage space, electricity room).
- Any equipment located in publicly accessible areas, or rooms that cannot be locked, is to be fastened down by some physical means such as a cable lock system or enclosed in a lockable computer equipment unit or case.
- Clear identification of ownership should be clearly marked on all computer equipment, including the asset number.

Power Supplies

- To avoid power failures, a suitable electrical power supply must be provided in such way that Single Points of Failure can be avoided.
- Based on business criticality, the use of a back-up generator must be considered.
- Recovery procedures must be documented to ensure proper fallback or fail over processes. These procedures should be part of the disaster recovery plan.
- Uninterruptible Power Supplies (UPS) must be used for equipment supporting critical business operations to orderly close down or allow systems to continue running.
- UPS and generator equipment will be checked on a quarterly basis to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.

Secure Disposal or Re-use of Equipment

- Any PMU information processing equipment that is to be disposed of, or reused, must undergo a cleansing process before release. The cleansing process must consist of:
    - Destruction of the information residing on equipment;
    - Validation of the process; and
    - Testing of the process to ensure no data is left on the equipment.
- If the equipment stored information classified as “confidential” or “critical” the equipment must be physically destroyed beyond repair or restoration before being disposed of.

Environmental Control

- Adequate environmental safeguards must be implemented to protect IT

system resources as deemed appropriate for the sensitivity or criticality of the resource. At least the following environmental safeguards are to be assessed:

    - Fire prevention, detection, suppression and protection;
    - Water hazard prevention, detection and correction;
    - Electric power supply protection (an international guide on maximum reasonable expenditure on power protection suggests 4 percent of the value of the equipment being protected unless the mission critical nature of a particular system necessitates additional protection.);
        - Temperature control;
        - Humidity control;
        - Natural disaster protection (from lightning, etc.);
        - Magnetism protection; and
        - Good housekeeping procedures for protection against dust and dirt.
- Environmental conditions should be periodically reviewed and monitored for conditions, which could affect PMU information processing facilities.
- Fire walls surrounding computer facilities must be non-combustible and resistant to fire for at least one hour. All openings to these walls (doors, ventilation ducts, etc.) should be self-closing and likewise rated at least one hour.
- To minimise theft and water damage, multi-user computers and communications facilities must be located above the first floor in buildings.
- All computer equipment must operate in a climate-controlled atmosphere at all times. Backup ventilation plans must be provided in the event that air conditioning systems in computer rooms fail.
- Facilities management must monitor and test fire suppression system test equipment at least every 6 months and document the test results.
- All computer room personnel must be trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers, and in the proper response to smoke and fire alarms.
- Use of mobile phones must be restricted inside the computer rooms.
- Fire drill for Computer Operations staff should be conducted quarterly.

Removal of Property

- Equipment, information or software should not be taken off-site without written authorization. A copy of the authorization should be kept by the user and the manager. Written authorization should include, but is not limited to the following detail:
    - The date the removal is authorized for;
    - The name of the person that granted the authorization as well as

his signature;

- The name of the person the authorization is granted to as well as his ID and signature; and
- The serial number(s) where applicable.

- Where necessary and appropriate, equipment should be logged out and logged back in when returned (serial number(s) used, where possible).
- Spot checks should be undertaken to detect unauthorized removal of property. Individuals should be made aware that spot checks will take place.
- Computer media in transit must be protected from loss or misuse during transportation. Reliable transport or couriers should be used. Appropriate heat- resistant and water-resistant packaging should be used to protect the contents from heat, water and any physical damage likely to arise during transit, in accordance with manufacturers' specifications.

Securing Communications Networks

- Physical access to communications equipment and facilities must be restricted to authorized personnel.
- Suppliers or service engineers must be supervised when they have access to communications equipment.
- Critical areas, such as network operation centers, including those at remote sites, must be protected from power failure, such as by the use of uninterruptible power supplies (UPS).
- Communications cables should be protected by use of the following:
    - Concealed installation;
    - Armored Conduit;
    - Locked inspection/termination points;
    - Alternative feeds or routing; and
    - Avoidance of routes through public areas.
- Fiber optic cables should be used to reduce the risk of data in transit being intercepted.

Supplement on Virus Prevention, Detection, and Removal

Introduction

This functional policy covers PMU's Protection against Malicious Software and Viruses. Communications and operational management of information resources and systems are essential to maintaining a high level of service.

Security requirements will be developed and implemented to maintain control over communications and operations
It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU 's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU.

Purpose and Scope

This policy applies to ITD, Owners, their delegates and/or Custodians. In the PMU context the term "Owner" covers any of the following: an information, application, installation, network, business and/or development owner:

- All Information Assets
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All business activities supported by PMU.
- All of the above are either owned or leased by PMU and under PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Protection Against Malicious Software and Viruses Functional Policies listed in this document.

- Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined;
- The risks associated with access to organizational information processing facilities by third parties must be assessed and appropriate security controls implemented;
- Any security related incidents must be reported immediately through the established channels after the incident is discovered;
- Detection and preventive controls to protect information and information processing facilities against malicious software and appropriate user awareness procedures must be implemented;
- The management of removable computer media, such as tapes, disks, cassettes and printed reports must be protected and controlled according to its classification;
- Back-up copies of essential business information and software must be taken regularly;
- Content scanning must only be enforced in checking for malicious software, viruses or violations;
- Media being transported must be protected from unauthorized access, misuse or corruption;
- The purchase, use and modification of software must be controlled and checked to protect against possible covert channels and Trojan code.

Protection Against Malicious Software and Viruses

Malicious Software Delivery Mechanisms

Users should also be aware that malicious software is commonly delivered by one of the following methods:

- Physical Transfer of Storage Data.
- Computer systems may become infected by exposure to a contaminated source. Malicious software can infect any form of storage media, including hard drives, diskettes, CDs, magnetic tapes and cartridges, or optical media.
- Some of the most frequent sources of contamination are:
    - Copying data from an infected diskette; and
    - Booting from an infected disk or CD.

- Infected media may be received from another user within PMU, a vendor or even in commercial shrink-wrapped software.

Electronic Mail

- Malicious code is often spread when documents and files are sent over e-mail.
- Basic e-mail is pure text and cannot contain viruses or other malicious code.
- However, most e-mail applications today allow file attachments. These attachments may contain executable macros or scripts. When the message is received, the attached macro or script may be activated by the user, giving the malicious software an opportunity to attack and spread.

Downloaded Software

- Software downloaded from the Internet or an electronic bulletin board system may include malicious software and computer viruses.
- Files exchanged in chat sessions are becoming a frequent method of propagating malicious software.

Mobile Code

- Mobile code is software that will run on multiple platforms.
- Mobile code is contained in small applications called applets, which are often used on Web pages to provide news tickers; front-end graphical user interfaces (GUIs) and video games.
- Some examples of programming languages used in developing mobile code include Java, JavaScript, ActiveX, and Postscript.
- Malicious code can be hidden within Java applets, ActiveX controls and plug-ins to steal information from a computer file or disable a system.

Preventing Malicious Software and Viruses

To protect PMU resources against the risk of physically transferred malicious code, the following protection measures must be adhered to:

Physical Transfer

- Users should avoid booting or copying files from removable media such as USB drives or CD-ROM’s unless they have been obtained from a trusted source.
- Users should avoid leaving removable media such as diskettes and CD-ROM’s in boot-able drives.
- All storage media obtained from sources external to PMU must be scanned by an approved anti-virus software product with current signature files prior to use.
- Prior to providing storage media to customers, vendors, or others outside PMU, the media must be scanned by an approved anti-virus software product with current signature files.

Electronic Mail

- Users should be suspicious of all e-mail messages from people that they don't know.
- All e-mail messages that include attachments should be viewed with suspicion. Users should know the purpose of attachments before opening them.
- Suspicious e-mail messages with executable attachments (e.g. com or exe) should not be opened, even if they appear to be from people known to the user (s).
- Macro programs contained in Word or Excel files received by e-mail should not be executed until it has been determined that they are from a trusted source.

Downloaded Software

- Software should not be downloaded from an unknown or un-trusted source.
- Obtaining or downloading of public domain, shareware, or evaluation copies of software from other than PMU sources is permitted only under certain conditions.
- Software downloaded from sources external to PMU must be scanned by an approved anti-virus software product with current signature files prior to

being installed on an PMU information resource.

Mobile Code

- In an interactive environment, a server is accessed across a network and an application (applet) is downloaded onto the computer that is then executed. The Users web browsers should be configured to prevent downloading of applets.
- Java and ActiveX should only be enabled when they are needed to access a trusted Web site.

Application Software

- Many software applications such as Internet Explorer, Mozilla Firefox and Google Chrome and the Microsoft Office Suite, contain features designed to alert the user before opening or activating files that could contain potentially dangerous software.
- Users should carefully consider the source of files that are flagged in this manner.
- Users should not configure the application software to disable these warnings.

Anti-Virus Software

Anti-Virus software is the main line of defense against computer viruses.

ITD responsibilities include:

- Ensuring that current, University approved, anti-virus software is installed and activated on all computers issued to users.
- Configuration of the software to scan all file types, not just executables.

User responsibilities include:

- Software must not be written; generated, copied, propagated or executed that will damage or hinder the performance of any PMU information resource.
- Users of any PMU PC must ensure that current; University approved, anti-virus software is activated on their PC. This software must be actively enabled at all times.

Detecting Malicious Software and Viruses

Identification of Malicious Software

- Malicious software can be identified through observation, technical knowledge, or virus alerts.
- Several factors can indicate that malicious code has infected a system. Below are some indicators to help confirm the presence of a virus:
- File size increase;
- Change in update timestamp;
- Sudden decrease of free space;
- Numerous unexpected disk accesses; and
- Strange macros attached to files.

Further Guidelines

- The anti-virus software should be used to perform a periodic scan of all files on the system. PMU ITD maintains a local signature server that contains the most recent updates. All University laptops and Desktops are configured to get their updates from this central server.
- Any machine suspected to be infected by a virus is immediately disconnected from all networks. The machine must not be reconnected to the network until IT staff can verify that the virus has been removed.

Reporting Malicious Software and Viruses

- Malicious software can spread quickly and needs to be eradicated as soon as possible to limit damage to PMU information resources.
- Reporting actual attacks by viruses or other malicious software is important because it allows PMU to collect information regarding the magnitude and severity of the attack and to take appropriate steps to halt

further contamination.

- For assistance in removing a virus or other malicious software, if needed, or for help repairing any damage that resulted, users should contact the Help desk.
- Any significant malicious software attacks must be reported to the Help desk for further investigation and assessment. An attack should be considered "significant" if one or more of the following apply:
    - The infection has caused the loss or damage of PMU data;
    - The infection has impacted more than one computer or system; and/or
    - The infection is the result of a virus that has previously been assessed by PMU as a high risk.
- Correcting Malicious Software and Viruses
- Backup
    - The ability to recover from a malicious attack depends upon maintaining frequent backups.
- Recovery
    - If it is not practical or feasible to obtain a new copy of the file without the virus, when attempting recovery, anti-virus software may be used to remove the virus.
- Virus Hoaxes
    - A virus hoax is the fraudulent report of a virus for the purpose of generating large amounts of network traffic about the non-existent virus.
    - While PMU will sometimes make use of established employee communications channels to distribute information regarding viruses, users must ignore and not forward e-mail or other messages originating from other sources regarding supposed viruses.
    - Passing on messages about hoaxes only serves to further propagate them and unnecessarily increase the utilization of PMU resources.
    - PMU security personnel regularly receive information from the major anti-virus software vendors and other sources. It is not necessary to pass information to them regarding possible viruses

Supplement on SPAM, Intrusion Prevention and Detection

Introduction

It is each user's responsibility and obligation to ensure that all resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption. This FP Intends to Clarify to all users on PMU infrastructure, what their responsibilities are; Define what the potential risks and dangers are for PMU in the event of misappropriation and abuse of Infrastructure users; and regulate the professional and effective use of Infrastructure within PMU as well as between PMU and external entities.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff. Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Combating Cyber Crime Functional

Policies listed in this document:

- Intrusion detection software which records attempted and successful access to your systems.
- Access control lists and facilities, which record certain activities for specific files, such as: read, write, execute, and delete
- Network usage analysis, which identifies application access and reports on user authorization levels
- Network packet sniffing software to detect attack origins
- Disable specific applications, for example, an e-mail system subjected to a SPAM attack
- Ensure that all system and access events are logged
- Gather evidence to prove malicious intent, especially if the suspects are organization staff
- Access Controls should limit access to only those persons so authorized. Use a combination of policies and guidelines to promote both awareness and compliance
- Implement strong authentication and appropriate access control measures.
- Always perform rigorous System Testing before releasing into live 'production'
- Restrict and control all software and utilities which could be used inappropriately
- All software downloads must be virus-scanned
- Deploy software scanning tools to detect the 'footprint' of malicious code, introduced via e-mail, Internet download or by other means, e.g. diskette or CD-ROM
- Foster a sense of constant vigilance throughout the organization
- Nominate a technically oriented member of staff as 'virus control officer' to be the first point of contact for all virus alert issues and who co-ordinates follow up actions
- Advise staff of virus reports identified as hoaxes, in order to minimize disruption to business
- Considering designating a specific telephone extension as the virus 'hotline', reserved for virus and other malicious code reports / warnings.
- The Information Security Officer, the System Administrator, and the nominated virus control officer should collaborate to prepare a **Virus Incident**

Response Plan

- Ensure that **all** PCs are protected, and that regular anti-virus updates are

distributed

- After a virus attack, consider regularly reviewing software and files used for critical business processes to identify and investigate unauthorized and / or suspicious changes
- Promote awareness of the risks and encourage best practice regarding the receipt of e-mail attachments
- Consider the optimum deployment: servers only, or servers and workstations. The latter is recommended
- Ensuring that the license agreement includes updates of the anti-virus software and of the vaccine files
- Choosing e a vendor who offers 'hotline' support to deal with newly released virus strains

Functional Policy

Combating Cyber Crime

Cyber Crime remains a major area of Information Security risk. The sophistication of these threats is consistently increasing and the methods employed to combat these threats must match this level of sophistication. As a result, it is necessary for all systems users to be especially vigilant at all times

Defending Against Premeditated Third Party Cyber Crime Attacks.

Criminals may target organization's information systems, resulting in serious financial loss and embarrassment.

- Security on the network is to be maintained at the highest level. Those responsible for the network and external communications are to receive proper training in risk assessment and how to build secure systems which minimize the threats from cyber crime.

Minimize the Impact of Cyber Attacks.

Even the most Information Security conscious organizations can be attacked; this may be to 'prove a point' or for other malicious reasons

- Plans are to be prepared, maintained and regularly tested to ensure that damage done by possible external cyber crime attacks can be minimized and that restoration takes place as quickly as possible

Collecting Evidence for Cyber Crime Prosecution

In order to prosecute Cyber Crime successfully you need proof. This can be difficult to provide, unless your organization's information systems have adequate

controls and audit capabilities.

- Perpetrators of cyber crime will be prosecuted by PMU . Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence

Defending Against Premeditated Internal Attacks

Access to confidential data may be legitimized in employees' job descriptions. The act of copying sensitive data may not necessarily leave a 'footprint' on the system, and such copies can then be exported from your organization by e-mail or by removable media without leaving a trace. The effects of outright malicious data destruction are obvious, but the computer entry process of so doing may have seemed routine.

- To reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times

.

Defending Against Opportunistic Cyber Crime Attacks

Opportunistic criminal attacks usually arise from chance discovery of a loophole in the system, which permits access to unauthorized information

- It is a priority to minimize the opportunities for cyber crime attacks on PMU systems and information through a combination of technical access controls and robust procedures

Safeguarding against Malicious Denial of Service Attack.

Denial of Service (DoS) attacks have gained notoriety as being an effective way to disable Web based services. See DoS for an explanation of the techniques used and their consequences.

- Contingency plans for a denial of service attack are to be maintained and periodically tested to ensure adequacy

Defending Against Hackers

Unlike other forms of Cyber Crime, these attacks take a 'scatter gun' approach, in that they do not target a specific organization. If you happen to be 'in the firing line', and your Information Security safeguards are poor, you are likely to be hit.

- Threats to PMU-IT systems and information are to be minimized by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices

Handling Hoax Virus Warnings

Threats from viruses are well known throughout the IT community. Hoax threats - the spreading of rumors of fictitious viruses or other malicious code - can waste time, as staff attempt to locate a virus which does not exist

Vigilance and good virus intelligence warnings are the key to minimizing the impact of hoaxes.

Defending Against Virus Attacks

Virus infection can be minimized by deploying proven anti-virus software and regularly updating the associated vaccine files. Many anti-virus companies supply such updates from their Web sites.

- Without exception, Anti Virus software is to be deployed across all PCs with regular virus definition updates and scanning across both servers, PCs and laptop computers

Responding to Virus Incidents

Despite general awareness and technical safeguards, some viruses nevertheless enter and infect the organization's systems. Dealing with a virus in a professional and planned way reduces both its impact and its spread throughout the organization and beyond.

- The threat posed by the infiltration of a virus is high, as is the risk to PMU -IT systems and data files, Formal procedures for responding to a virus incident are to be developed, tested and implemented.
- *Virus incident response must be regularly reviewed and tested*

Virus Scanning Software

The development of anti-virus software is a highly technical and specialized area. Consequently, selection of the product should be with utmost care.

- Anti Virus software must be chosen from a proven leading supplier

Supplement on Authentication and Passwords

Introduction

This functional policy covers Authentication at PMU. It governs logical access to all information, systems and equipment. This will be enforced by a set of access rights or profiles to ensure that users can only gain access on a 'need-to-know' and 'need-to-do' basis to those resources on the system to which he has been properly authorised.
It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy Statements govern the Functional Policies on Log

on and Authentication listed in this document:

- Business requirements for access control must be defined and documented, and access must be restricted to what is defined in the access control policy.
- All access requirements must be based on a need to know, need to do basis.
- The allocation of passwords must be controlled through a formal management process.
- Operating systems and applications must include as a minimum, adequate user access controls, password controls and monitoring controls.
- Each System Owner at PMU must enforce all users to follow good security practices in the selection and use of passwords.
- Access by remote users must be subject to authentication.
- Connections to remote computer systems must be authenticated.
- The procedure for logging onto computer systems must be designed to minimize the opportunity for unauthorized access.
- User identification and authentication must be strictly enforced.
- Access to information services must use a secure log-on process.
- All users must have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual.
- A password management system must be in place to provide an effective, interactive facility that ensures quality passwords.
- Use of system utility programs must be restricted and tightly controlled.
- Inactive terminals in high risk locations or serving high risk systems must shut down after a defined period of inactivity to prevent access by unauthorized persons.
- Restrictions on connection times must be used to provide additional security for high-risk applications.
- Audit logs recording exceptions and other security-relevant events must be produced and kept for an agreed period to assist in future investigations and access control monitoring.
- Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly.
- Computer clocks must be synchronised for accurate recording.

Authentication Functional Policies

- Log on
    - Pre-Log on Banner: All computer systems within PMU must contain

a pre-log on warning banner to address the following:

- Before being given the opportunity to log onto a computer facility, intended users will be presented with a login banner, where applicable.
- This provides: Users with a chance to terminate the login before accessing a computer that they are not authorized to; Identification of PMU, the network, location, or host must not appear prior to a successful login.
- Systems must be configured to not give any information on an unsuccessful login. This includes identifying which portion of login sequence (user ID or password) was incorrect.

- Authentication

    - User Identification
        - All users must have their identity verified with a user ID and a secret password, or by other means that provide equal or greater security, prior to being permitted to use PMU information resources.
        - Unless prior permission from the ITD has been granted, all System Administrators must consistently observe the user-ID naming standards.
        - Each computer and communication system user-ID must be unique and forever connected solely with the user to whom it has been assigned.
        - After a worker leaves PMU, there should be no re-use of any user-IDs. Any exceptions should be authorized. This serves to minimize the risk of dormant access permissions being inherited by a new user.
        - Administrators with access to super user or privileged accounts must use their account to log into systems. They should then switch from their own accounts to the privileged account.

    All Guest Accounts must be disabled on servers, desktops,databases and applications.

Assigning Passwords

Administrator's responsibilities when assigning passwords include:

- The initial temporary password assigned to users must be a minimum of six (6) characters in length and comprised of alphanumeric, non-alphanumeric and special characters.
    - Passwords assigned must be unique for each user.
    - Passwords must only be supplied to users in a secure manner e.g. not via a third party.
    - Initial passwords must not be easily associated with PMU or the user (i.e. identification number, employee number, address, numerical equivalent of name, etc.)
    - On initial log on, new users will be forced by the system they are accessing to change their initial password to one that meets the relevant password functional policies.

Safeguarding Passwords

Administrators must adhere to the following regarding safeguarding of passwords:

- ITD must perform password testing on quarterly basis to ensure proper passwords are being used. This includes the use of password cracking tools.
- This process must be controlled in the strictest manner and subject to explicit supervision.
- Users whose password is cracked must be notified immediately, their account disabled, and a new password issued using the normal allocation methods.
- Users must be forced to change passwords every Academic semester. System administrators shall enforce this through technical means by deploying password aging on systems.
- Default passwords shipped with servers, operating systems software or applications must always be changed when the hardware or application is installed or implemented.
- Where technically feasible, systems must use password history techniques to maintain a password history of users. This will ensure that users do not reuse passwords when forced to change the password.
- All computers, databases or applications that store user account and password information must be secured in the strictest manner. Access to the user account base must be restricted to only authorize administrators.
- This access must be reviewed at least twice a year along with a technical review of the host/server/user store.

System Account Controls

General Account Controls

General account controls include the following:

- For high security environments it may be necessary to limit session initiation to specific terminals or locations. In this case, unique device identifiers must be associated with the approved connection points or direct connection to a server may be required.
- Users given command line access to systems must, where feasible, be limited to the access or service needed. This may include restricted shells, application menu restrictions, and the like.
- Unless authorized to the user, systems should not allow users to have multiple sessions on the same system.

Account Lockout

- Upon three consecutive authentication failures, users must be locked out of the resource in which they are attempting to gain access to and will have to have their account policy reset.
- In the event that an account requires a new password, Help desk/System Administrator personnel must be contacted.
- In the event that the account requires resetting without changing the password, the reset must only be executed after verification of the user's identity.

Disabling Inactive Accounts

User accounts that have not been accessed for 90 days must automatically be disabled.

Automatic time-outs

Automatic time-outs must be in accordance with the following:

- PC's/laptops and Servers, when applicable, must be configured with a password-protected screen saver. The screen saver must require the entry of a password after a PC/laptop or Server console has been left idle for five (15) minutes.
- Systems must force users off after 30 minutes of inactivity. The user should have to log back into the system.
- System sessions that are not active for two (2) hours will be automatically terminated. For those systems that cannot automatically terminate connections, password protected screen savers or terminal locks must be activated.

Use of System Utilities

A number of utilities are available to enable system administrators to perform low-level maintenance tasks on a system. If inappropriate access is gained to these utilities they may be used to circumvent logical security controls. All utilities must:

- Be stored off-line if not required on a daily basis;
- Have access restricted to a very limited group of authorized users; and
- Include logging facilities to record their use.

Application Access Controls

All users must only be provided with the minimum level of access required to perform their duties. This should be achieved using a combination of:

- Logical security within an application;
- Hiding the availability of unauthorized options;
- Limiting file permissions, e.g. read-only- Control of output distribution.

Monitoring System Access and Use

For applications that will be initiated and developed from the publication date of this document, the application program should pass the user logon ID to the Oracle database for proper monitoring.

Clock Synchronization

System clocks must be synchronised to an agreed standard to ensure the accuracy of audit logs. For example, Greenwich Mean Time or Local time.

System Monitoring

System Administrators must ensure that monitoring tools are installed in order to log user access activity and security violations against critical production data.

Security Event Logs

- Computer and communications systems handling sensitive, valuable, or critical PMU information must securely log all security relevant events.
- Logs containing computer or communications system security relevant events must be retained for a period prescribed. During this period, logs must be secured such that they cannot be modified, and such that they can be read only by authorized persons.
- ITD will review records reflecting security relevant events in conjunction with Computer Operations and Systems Administration staff. All potential security incidents must be reported immediately.
- Security Administrator must ensure that monitoring tools are installed in order to log user access activity and security violations against critical production data.

Supplement on Incident Handling and Reporting

Introduction

This functional policy covers PMU's Incident Handling and Reporting. In order to minimise the damage from security incidents and malfunctions within PMU, adequate security controls will be followed and security will be monitored to

detect security breaches, incidents or areas of non-compliance with security policies, Functional Policies and procedures.

It is each user's responsibility and obligation to ensure that all IT resources are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, appropriation, or corruption.

Objective

The objective of this Information Security Policies is to secure PMU's Information Assets and staff.

Each policy statement in this policy wherever required is supported by standards, procedures to achieve a complete security framework in the PMU

Purpose and Scope

- All Information Assets (Digital Media)
- All software assets
- All physical assets, such as computer and network equipment.
- All supporting services, such as power and network link
- All management information systems
- All business activities supported by PMU.
- All of the above are either owned or leased by the PMU and under the PMU possession, custody, or control.

General Responsibilities

It is the responsibility of the different departments/offices and each employee to take necessary steps for ensuring compliance with the guidelines in this policy, and any further Policies and Procedures that may be added in due course of time.

Governing Policy

The following Executive Policy statements govern the Incident Handling and Reporting Functional Policies listed in this document:

- Training and orientation are provided to newly hired employees through the induction process;
- Any security related incidents must be reported immediately through the established channels after the incident is discovered;
- Procedures must be established and followed for reporting software malfunctions;
- Users of information services are required to note and report any observed or suspected security weaknesses in or threats to systems or services;
- Mechanisms must be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored;
- The violation of organisational policies, functional policies and procedures by employees must be dealt with through a formal disciplinary process;
- Incident management responsibilities and procedures are established to ensure a quick, effective and orderly response to incidents;
- Faults must be reported immediately and corrective action taken;
- An intrusion detection system is in place to detect unauthorised use of PMU networks;
- Audit logs recording exceptions and other security-relevant events are produced and kept for 3 months to assist in future investigations and access control monitoring.

Incident Handling and Reporting

Incident Levels

All incidents must be reported based on the severity of the incident and can be classified as one of the following:

Critical Alert

A critical alert is an event that is, or could become a serious and immediate threat to any of the devices on PMU network and requires immediate attention and action.
Threatened devices may include routers, networks, servers, firewalls, network management hosts, attached LAN's, or user hosts.

Major Alert

A major alert is an event that is, or could become, a future threat, but which has not been

determined as serious enough as of that time. Hence, it may or may not require an immediate response depending on the incident.

Minor Alert

A minor alert is an event that is, or could become, a minor annoyance or threat; or which has been determined to be a non-threat resulting from either authorised, or unauthorised network activity.

Minor alerts are informational in nature.

Types of Incidents

The type of incidents which can be reported by users, include but is not limited to the following:

- Accidental and/or negligent incidents, including:
- Compromise of system integrity;
- Denial of system resources;
- Illegal access to a system (either a penetration or an intrusion);
- Malicious use of system resources,
- Any kind of damage to a system.
- Power Outages

Reporting Security Incidents

Reporting Violations

- All incidents will be reported to the IT Help Desk
- Help Desk will escalate the incident for investigation to appropriate senior personel.
- All incidents will be investigated by ITD to determine the severity of the incident.
- Investigative methods and procedures will be used based upon the Security Incident Level.
- In cases where the violation is clearly illegal with intent, notification to the Higher Management shall be immediate.
- In cases where the intent is not clear, the violator shall be advised to correct the violation. A repeat violation shall be reported immediately to management and the appropriate disciplinary action will be taken based on the severity of the incident.
- In cases where the violation is either a support or resource-sharing issue,

the violator will be informed of the violation and advised of possible corrective action. Records shall be kept of such violations.

- If support teams determine that repeated violations of policies and functional policies are causing support or resource-sharing problems, they may contact ITD who may defer support and/or report the violation to ITD management.
- No PMU employees are allowed to talk about any security incident in public or media.

Responding to Incidents

ITD Responsibilities

The ITD have the following responsibilities when responding to incidents:

- Confirming that an intrusion has occurred (or is occurring).
- Keeping records of work efforts.
- Activating additional event logs immediately.

Initial Analysis

- To be able to address incidents properly it might be necessary to collect evidence as soon as possible after the occurrence.
- Regardless of how the suspicious activity is identified, the administrator must quickly perform an initial analysis to determine if the possible intrusion is the result of:
    - Hardware or software problems;
    - User error; or
    - An actual security intrusion.
- The initial analysis must be performed immediately, so that innocent activities can be quickly eliminated, and intrusions can get prompt attention.

Taking Action

- If PMU information resources are in danger of being irreparably harmed, the administrator of the system must take immediate action to protect these resources.
- Examples of irreparable harm include, but are not limited to:
    - An intruder has entered a system and is in the process of destroying or damaging data that cannot be recovered;
    - An intruder is actively bringing systems down and impacting customer service; or
    - An intruder is actively engaged in other behaviour that will cause unrecoverable loss or damage to PMU or PMU information resources.

- Examples of protective actions to be taken could include, but are not limited to:
    - Disabling all system accounts and/or changing all system passwords and/or disabling access permissions;
    - Correcting the vulnerability that allowed the intruder to gain access in the first place;
    - Removing or shutting down the access method being used by the intruder;
    - Bringing the system down or disconnecting it from the network; and
    - Physically removing disk drives, tape files, or other system resources.
- Where feasible, any action taken should be performed in a manner to prevent the intruder from being made aware that his actions have been noticed.
- Security violations will be followed by corrective action by management and the users involved in the incident.

Learning from Incidents

- All security violations and other incidents investigated must provide sufficient information so that management can take steps to ensure that:
    - Such incidents cannot reasonably take place again; and
    - Effective security measures have been re-established.
- Information that should be collected by the investigating body during the investigation, include:
    - Time spent on incident;
    - The type of incident; and
    - Cost of incident or malfunction. Loss due to man-hours must be calculated for all incidents.
- Summary reports of all incidents should be maintained by ITD for historical documentation.

Disciplinary Action

- Users must know and understand that in the event of an incident caused by user negligence, they may face disciplinary action.
- Disciplinary actions must be co-ordinated by the ITD through the Human Resource (HR) Department.
- All users who commit security breaches may be subjected to a formal disciplinary process.

Section 7.4.3.

Technical support is available for teaching staff and students using information and communications technology.

STAR: 3

Strengths:

University Help Desk system used to track and trace support request to successful resolution.

Opportunities for improvement:

Aging reports are required to move service level from 3 to 4.

Action Plan:

Evaluate cost effective commercial package solution for service desk software. Point person is Abdulaziz. Mr. Abdulaziz to gather functional requirements, survey current market options to meet these requirements, select vendors for Request for Proposals (RFP), create and process RFP through ETA office. Recommendation to Eng. Yamani through CIO due by January 31, 2012.

Section 7.4.4.

Opportunities are available for teaching staff input into plans for acquisition and replacement of IT equipment for use in the program.

STAR : 2

Strengths:

Faculty orientation program completed to orient teaching staff to technology resources available at PMU and enable them to engage in informed discussions about the acquisition and replacement of IT equipment used in the program.

- Presentation on faculty orientation
- Using YouTube for Teaching Learning @PMU

Action Plan :

Part 2 conduct faculty survey. Part 3 is work with Learning Resource Center to establish faculty forum for education Director of LRC and College Deans not later than March 31, 2012. CIO and Team Lead of MIS to finalize faculty satisfaction survey not later than October 26, 2011.

- IT survey instrument

Introducing New (And Old) Faculty and Staff to IT Resources

Prince Mohammed bin Fahd University

IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long)

- 20 Minutes on the Basics
  - Who Do I Call When I Have A Problem?
    - One Stop Shop: X8888 Is Also the Number You Call for all Engineering and Technical Affairs (Which Includes IT and Facilities and Maintenance)
    - Demo of Outlook E-Mail, Web Site, Call! (2 Minutes)
  - Using My Computer From Work
    - Wired in Your Office (2 Minutes)
    - Wireless in Common Areas at Campus (2 Minutes)
    - Using a USB Flash Drive
    - Getting Access to the Local Network Server (2 Minutes)
    - Applications on My Computer - Faculty Laptops (2 Minutes)
    - Accessing the Required Documents Through the Intranet (5 Minutes)
  - Introduction to IPT (10 Minutes)

IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long) -- Continued

- **10 Minutes:** Using My Computer From the Compound
  - Getting Internet via STC or Mobily (5 Minutes)
  - Online Banking (5 Minutes)
- 5 Minutes: Getting and Setting Up My PMU E-Mail Account:
  - Outlook & Web Mail
- My Banner Faculty Self-Service Account: Getting and Setting Up **and Submitting Grades!**

IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long) -- Continued

- 20 Minutes: My Banner Faculty Self-Service Account
  - Introduction to Banner (2 Minutes)
  - Login In to Faculty Self-Service For the First Time (2 Minutes)
  - Introduction to Your Self-Service Banner Session and Main Menu (4 Minute)
  - Introduction to Your Faculty Schedule (6 Minutes)
    - Detailed Schedule
    - Week at a Glance
    - Master Class Schedule
  - Start With the End in Mind: How To Submit Student Grades at the End of Semester in Banner (6 Minutes)

ITD-Classroom Services 4 PMU Faculty (1 Time for 1 Hr Long)

- Two Groups - Male and Female (1 Hr Long)
- Traditional 20 Minutes
- Smart 20 Minutes
- Enhanced 20 Minutes

Traditional Classrooms: 20 Mins

- Instructor Work Station
- Projector
- Smart Board & Promethean Active Boards (Female)

Smart Classrooms: 20 Mins

- Instructor Podiums
- Projectors
- Review After the Walk Through:
  - YouTube Playlist: Smart Classroom Basics at PMU
  - Google Presentation: Overview of Smart Classrooms at PMU

Enhanced Classrooms: 20 Mins

- Instructor Podiums
- Projectors
- Video Conferencing

ITD-College Blackboard for Beginners (ITD Will Be Doing 3 Times for 1 Hr)

- **ITD Will Be Doing Three Level I Sessions:**
  - **Getting and Setting Up**
    - Accessing Url
    - Login
    - Changing password
  - **Introduction to Syllabus, Hours, Assignments, Presentations**
- Later Topics Will Include:
  - Level II: Tracking Assignments & Grade Book
  - Level III: Assessments & Tests
  - Level IV: Working With Instructional Multimedia

Using YouTube for Teaching & Learning @PMU

College of Business
Fall 2011

What is YouTube Good For?

@PMU?

Dr. Michael E. Dobe, Sr.
professordobe's Channel

All | Uploads | Favorites | Playlists

Uploads (134)

see all
arrange

HIST 1301 Review (I of 6)
342 views - 1 year ago

HIST 1301 Review (2 of 6)
288 views - 1 year ago

HIST 1301 Review (3 of 6)
171 views - 1 year ago

HIST 1301 Review (4 of 6)
142 views - 1 year ago

HIST 1301 Review (5 of 6)
83 views - 1 year ago

HIST 1301 Review (6 of 6)
200 views - 1 year ago

Favorites (81)

see all
arrange

David Blight on Frederick Douglass
gilderleh... - 614 views

Discovery Uncovering the real Gangs of New
Docmate - 35,969 views

Discovery Uncovering the real Gangs of New
Docmate - 36,463 views

Discovery Uncovering the real Gangs of New
Docmate - 45,980 views

Discovery - Uncovering the real Gangs of New
Docmate - 87,537 views

Playlists (81)

see all
arrange

Strategic Management
2 months ago
more info

Dr. Bruce's Aramco Health and Wellness
3 months ago
more info

New Student Orientation @PMU
4 months ago
more info

Smart Classroom Basics @PMU
1 month ago
more info

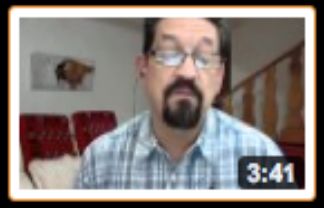
HIST 1301 Exam Review
3 months ago
more info

« Back to Playlists

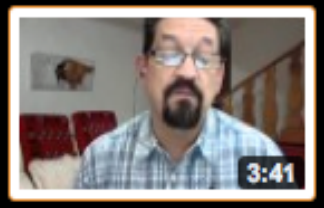
Edit My Playlist

Strategic Management

URL: http://www.youtube.com/user/professordobe#grid/user/DCCF62A0E9E5E5DB

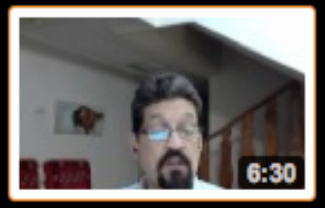


BUSI 4362 Strategic Management
cisnerosfgp1
123 views

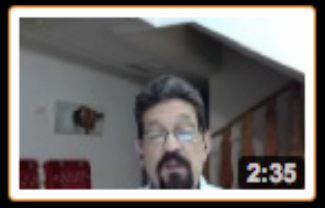


BUSI 4362 Strategic Management
cisnerosfgp1
123 views

BUSI 4362 Strategic Management Base
cisnerosfgp1
85 views



BUSI 4261 Entrepreneurship
cisnerosfgp1
7 views



BUSI 4261 Entrepreneurship
cisnerosfgp1
8 views

Class Notes Mission Statement Vision and
cisnerosfgp1
36 views

« Back to Playlists

Edit My Playlist

Dr. Bruce's Aramco Health and Wellness Workshop

Videos of the 6 June 2011 Health and Wellness Workshop conducted at the Aramco Abqaiq facilities by Dr. Bruce Wells (PMU).

URL: http://www.youtube.com/user/professordobe#grid/user/E8B08985862C8E0F

Health and Wellness Workshop at ARAMCO
professordobe
358 views

Health and Wellness Workshop at ARAMCO
professordobe
153 views

Health and Wellness Workshop at ARAMCO
professordobe
262 views

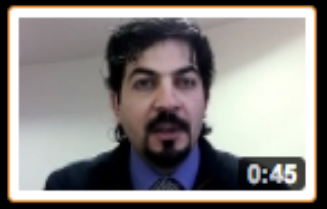
« Back to Playlists

Edit My Playlist

New Student Orientation @PMU

URL: http://www.youtube.com/user/professordobe#grid/user/E97C64A6A767A6E5

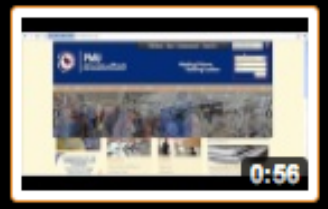
PMU IT Services - English
professordobe
70 views



PMU IT Services - Arabic
professordobe
71 views

PMU Laptop Configuration -
professordobe
63 views

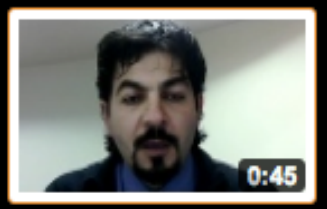
PMU Laptop Configuration - Arabic
professordobe
82 views



PMU EMail - English
professordobe
46 views

PMU EMail - Arabic
professordobe
46 views

PMU IT Help Desk - English
professordobe
87 views



PMU IT Help Desk - Arabic
professordobe
73 views

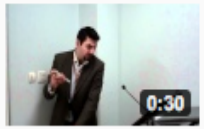
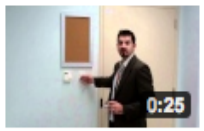
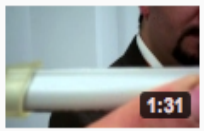
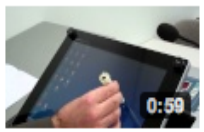
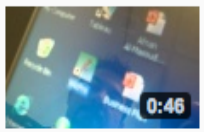
Smart Classroom Basics @PMU

by professordobe's channel

Play All Share

Edit Playlist

10 videos | 12:13 duration | 40 views

1	 0:30	Smart Step 01 - Logging Into Active Directory by professordobe	47 views
2	 0:40	Smart Step 02 - Turning on Power, Lights, Lowering S... by professordobe	35 views
3	 0:59	Smart Step 03 - Turning on the Overhead Projector by professordobe	24 views
4	 0:25	Smart Step 04 - Adjusting Lighting in Classroom by professordobe	21 views
5	 1:31	Smart Step 05 - Turning on Wireless Stylus (Pen) by professordobe	27 views
6	 0:59	Smart Step 06 - Using the Wizpro Software by professordobe	14 views
7	 0:46	Smart Step 07 - Double Take on the Wizpro Software by professordobe	17 views

About Playlist Creator

19,624 views
22 subscribers

http://www.youtube.com/playlist?list=PLA2BAA4FAD05509AC&feature=viewall

How to Become a YouTube Content Creator

@PMU?

What Do You Need?

- A Couple Hours of Your Time
- An Internet Connection (Home or Office)
- A Computer With a WebCam
- Video Recording Software ...
- For Example These Programs Come With Your Operating System:
  - Windows Movie Maker
  - Apple QuickTime
- Last But Not Least: A YouTube Account (Do I Mention it is Free?)

A Couple Hours of Your Time

- Well, we don't have that much time, so we'll have to rush ...

An Internet Connection

- The faster the better... STC DSL is probably your best bet at this point.
- Today we will be using the on campus connection.

A Compter With a Web Cam

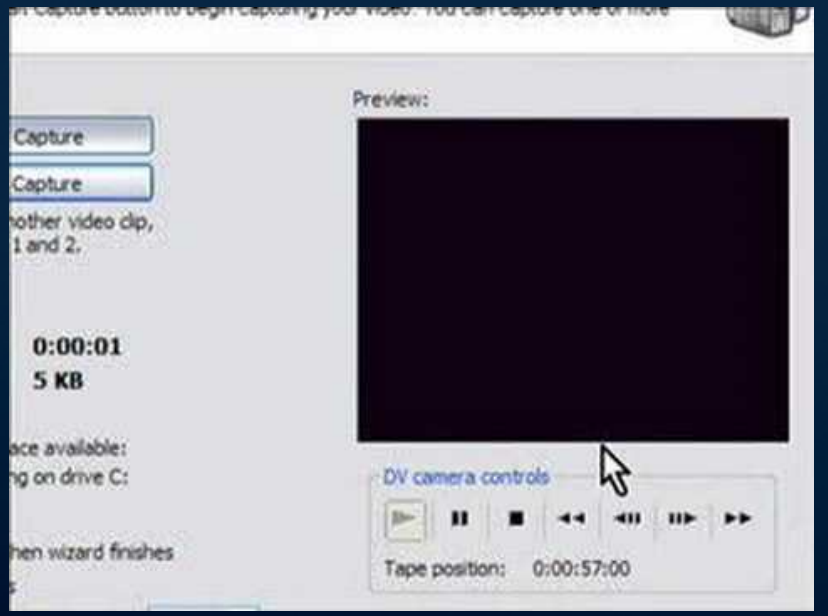
- Carrefour and Jarir Bookstore Carry Web Cams Ranging from 100 - 400 SAR
- You Get What You Pay For!
- On campus, you can use your office laptop or visit the Microstudio on the first floor of Wing B ...

PMU Microstudio

SEARCH YOUTUBE FOR >>>>

Windows Movie Maker YouTube Tutorial

How To Create A YouTube Account & Upload Your First Video



YouTube's Powerful Features

@PMU?

What Next Now That I Have an Account and am Uploading?

- Linking to Your Video in Blackboard
- Security Options: Public, Unlisted, Private
- Advanced Topics:
  - Embed Code
  - Closed Captioning

Section 7.4.5.

Security systems are in place to protect privacy of personal and sensitive personal and institutional information, and to protect against externally introduced viruses.

STAR: 5

Strengths:

Based upon 20 years in IT Services, current CIO believes the level of security at PMU is higher than any institution he has ever worked for and it suitable for financial institution such as Bank.

Opportunities for improvement:

N / A

Action Plan

N / A

Section 7.4.6

Compliance with a code of conduct relating to inappropriate use of material on the Internet is checked and instances of inappropriate behavior dealt with appropriately.

STAR: N/A

Strengths:

Opportunities for improvement:

N/A

Action Plan:
N/A

Section 7.4.7

Training programs are available for faculty and staff to ensure effective use of computing equipment and appropriate software for teaching, student assessment, and administration.

STAR: 4

Strengths:

IT supports Learning Resource Center by providing subject matter expert trainers who participate in professional development for all employees (faculty and staff). Also, IT supports the Student Affairs Division with student orientation and other training required to help students use systems and services.

- Student Orientation.
- Spring 2011 Introduction to IT Resources
- Using You Tube for Teaching Learning @ PMU

Opportunities for improvement:

ITD will continue to share knowledge and conduct on-going review of resources utilized at orientations.

Action Plan:
N/A

Overall Evaluation of Provision of Facilities and Equipment. This report should refer to evidence and relevant benchmarks, and include a summary of particular strengths, areas requiring improvement, and priorities for action

Student Orientation for Information Technology

تعريف الطالبات بتكنولوجيا المعلومات

Presented by Mrs. Ameera Al-Balushi

Fall 2011

What is to be discussed

الموضوعات التي ستناقش

Information Technology Services at Prince Mohammad University	خدمات تكنولوجيا المعلومات في جامعة الامير محمد
Laptop Configuration	إعدادات جهاز الكمبيوتر المحمول
When I Have a Problem With My Computer at Prince Mohammad University, What Do I Do?	عندما تواجه مشكله مع جهاز الكمبيوتر في جامعة الامير محمد, ماذا تفعل؟

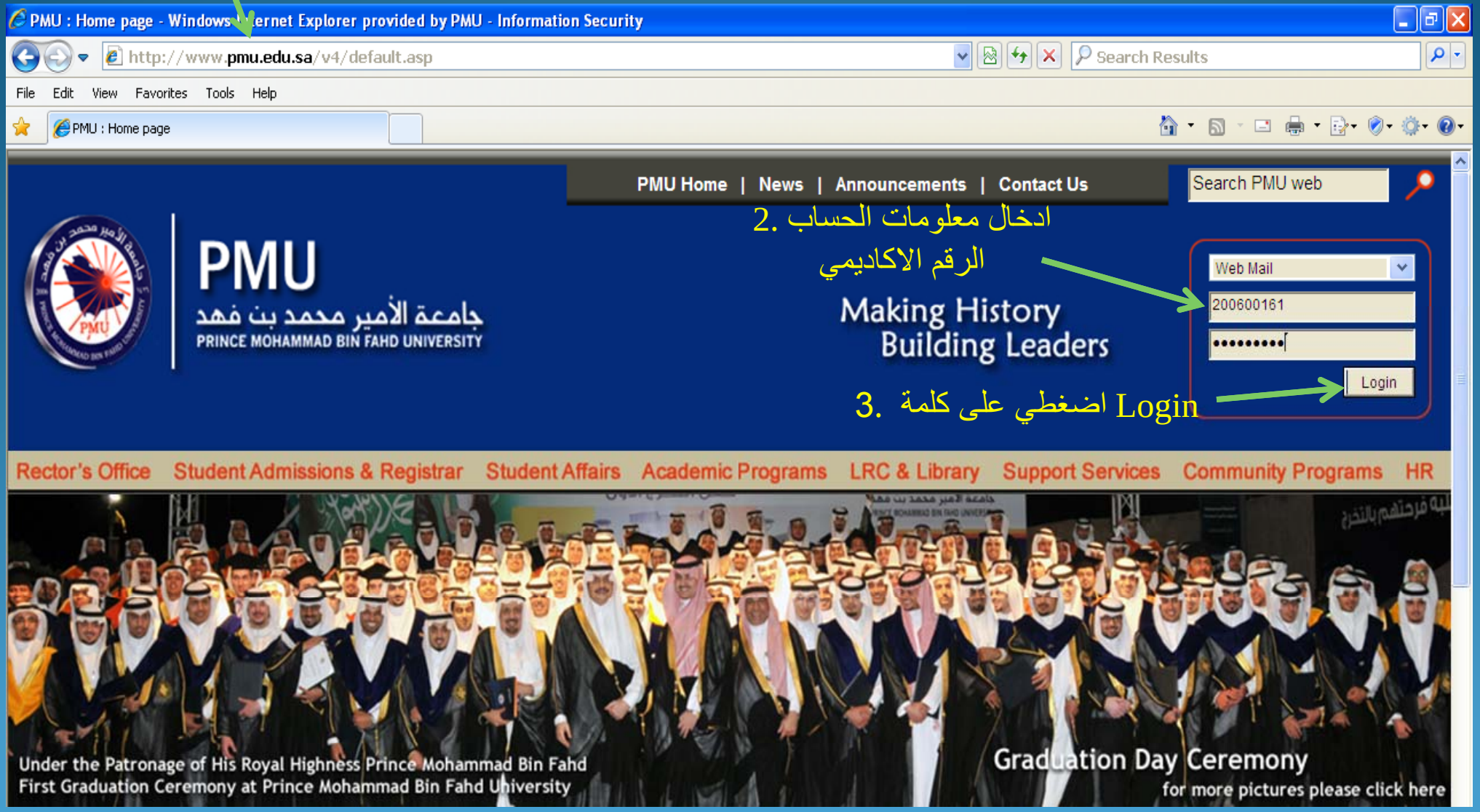
Information Technology Services at Prince Mohammad University

خدمات تكنولوجيا المعلومات في جامعة الامير محمد

Email	**البريد الالكتروني**
Black Board	**البلاك بورد**
Banner	**البانر**

البريد الالكتروني Email

1. الدخول الى موقع الجامعة
www.pmu.edu.sa



البريد الالكتروني Email

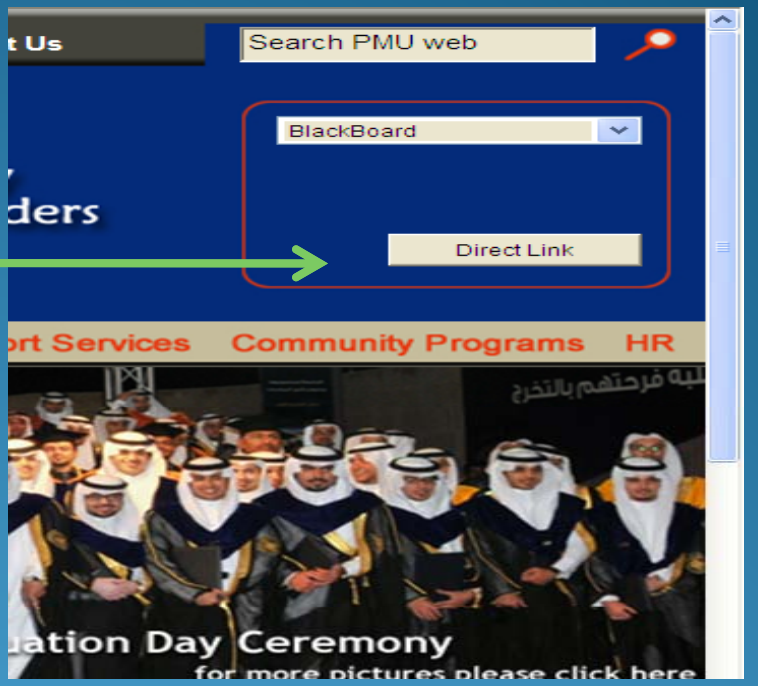
البريد الالكتروني Email

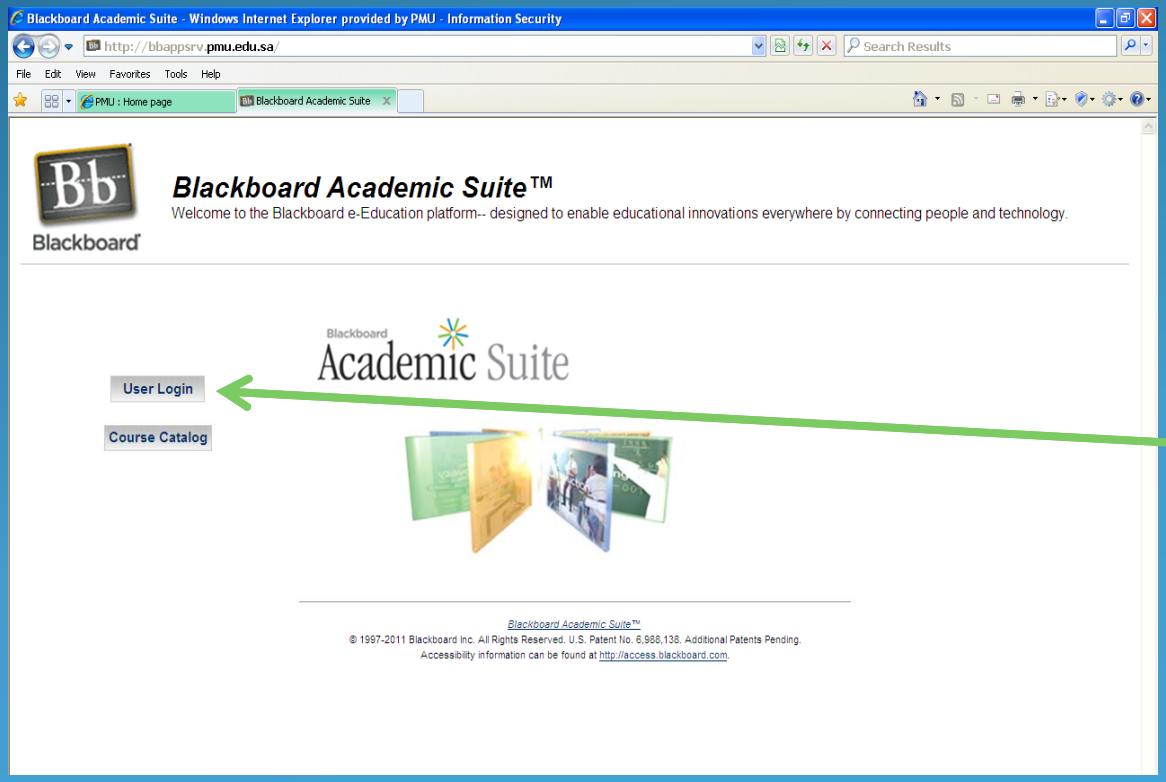
يمكنك تغيير كلمة السر بالضغط على هذا الخيار

You may change your password by clicking here

Black Board البلاك بورد

- ادخلي الى موقع الجامعة www.pmu.edu.sa
- اختاري Blcak Board
- ثم اضغطي على Direct Link

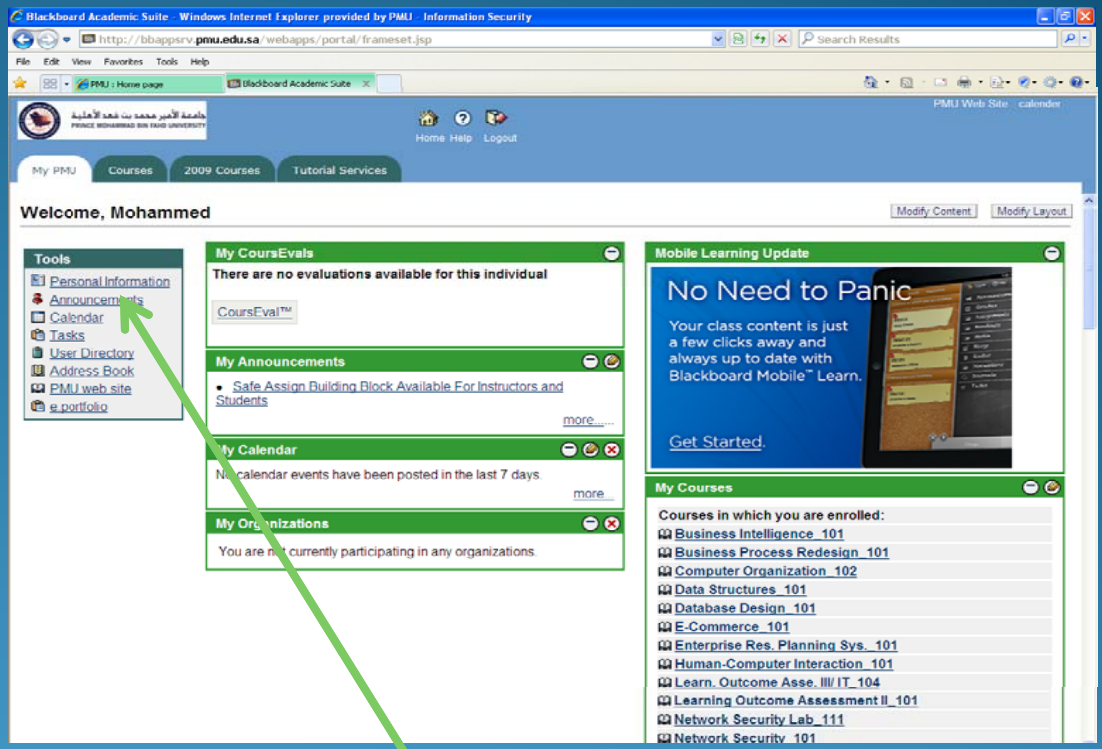


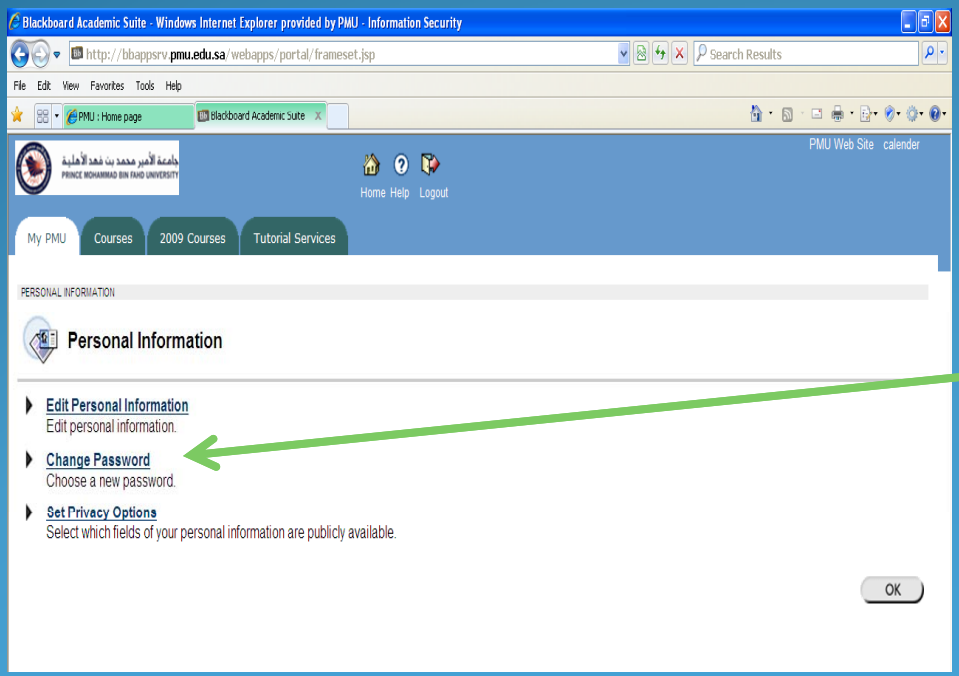


- اضغطي على ايقونة User Login
- استخدمي رقمك الاكاديمي للدخول للBlack Board
- كلمة السر هي ذاتها رقمك الاكاديمي

Black Board البلاك بورد

جميع المواد المسجلة لك ستجدينها مدرجة في صفحة ال Black Board



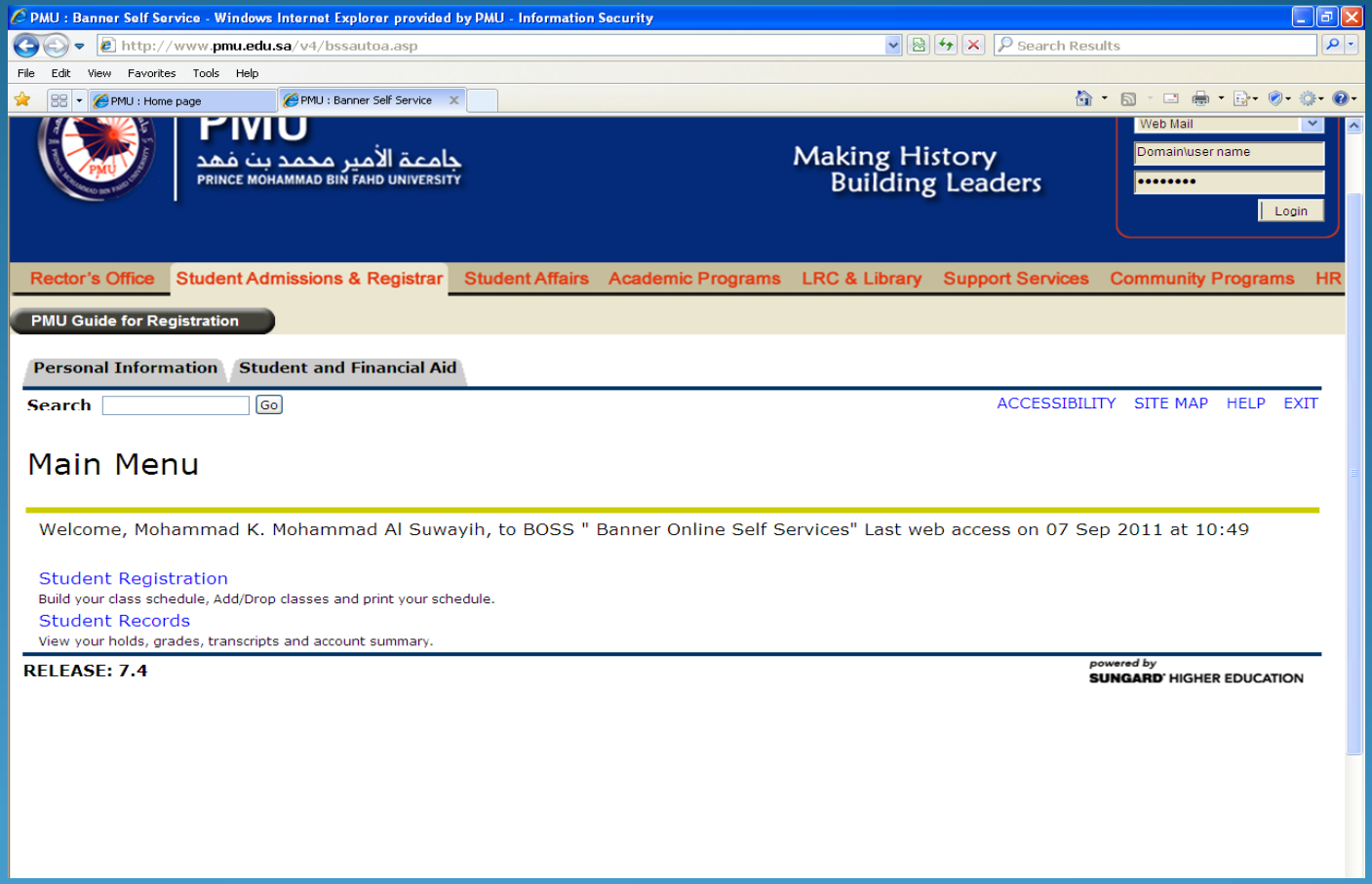


يمكنك تغيير كلمة السر بالدخول الى Personal Information

Banner الباتر

ماهو البانر ؟؟

- تسجيل المواد
- حذف / إضافة مادة
- متابعة الدرجات



الدخول لنظام البانر يكون باستخدام الرقم الاكاديمي والPIN

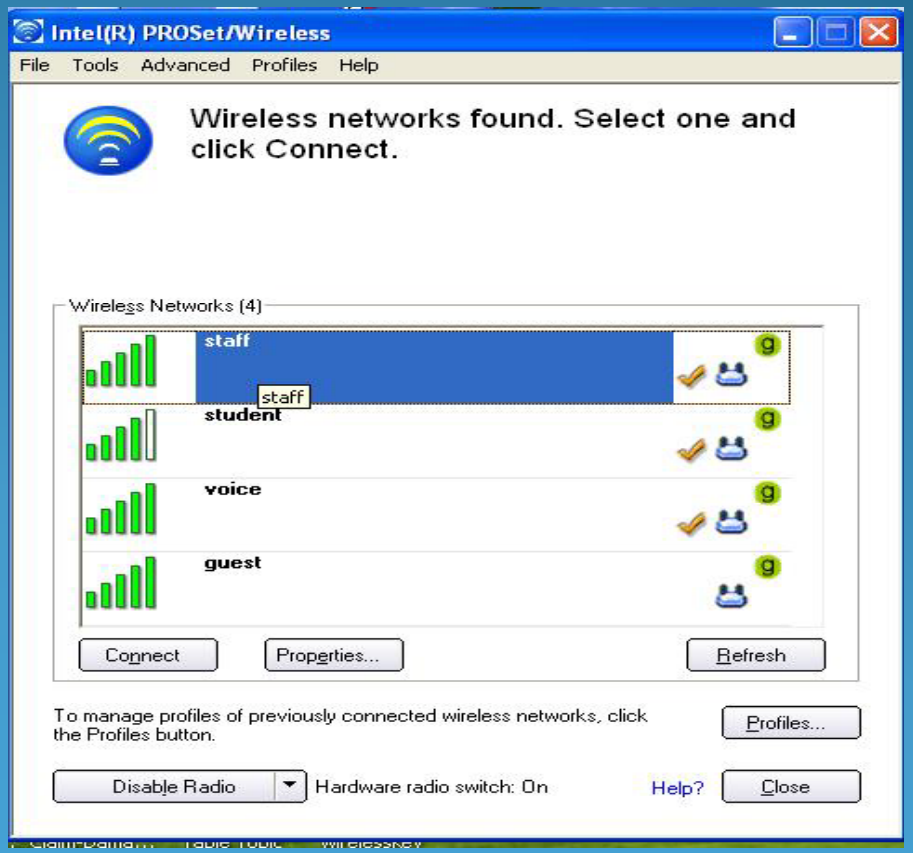
يمكنك الحصول على ال Pin من مكتب Ms. Bashira Chanane / G009

Laptop Configuration
إعدادات جهاز الكمبيوتر المحمول

What Do You Need to Connect to the Wireless Network at PMU?

ماذا تحتاج كي تتصل بالشبكه اللاسلكية في جامعة الامير محمد؟

Check that the wireless button is on/enabled on your laptop.



When I Have a Problem With My Computer at Prince Mohammad University, What Do I Do?

عندما تواجه مشكله مع جهاز الكمبيوتر في جامعة الامير محمد, ماذا تفعل؟

G056

Thank you for listening

شكرا

Introducing New (And Old) Faculty and Staff to IT Resources

Prince Mohammed bin Fahd University

IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long)

- 20 Minutes on the Basics
  - Who Do I Call When I Have A Problem?
    - One Stop Shop: X8888 Is Also the Number You Call for all Engineering and Technical Affairs (Which Includes IT and Facilities and Maintenance)
    - Demo of Outlook E-Mail, Web Site, Call! (2 Minutes)
  - Using My Computer From Work
    - Wired in Your Office (2 Minutes)
    - Wireless in Common Areas at Campus (2 Minutes)
    - Using a USB Flash Drive
    - Getting Access to the Local Network Server (2 Minutes)
    - Applications on My Computer - Faculty Laptops (2 Minutes)
    - Accessing the Required Documents Through the Intranet (5 Minutes)
  - Introduction to IPT (10 Minutes)

IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long) -- Continued

- **10 Minutes:** Using My Computer From the Compound
  - Getting Internet via STC or Mobily (5 Minutes)
  - Online Banking (5 Minutes)
- 5 Minutes: Getting and Setting Up My PMU E-Mail Account:
  - Outlook & Web Mail
- My Banner Faculty Self-Service Account: Getting and Setting Up **and Submitting Grades!**

IT Services for PMU Faculty and Staff (1 Time, 1 Hr Long) -- Continued

- 20 Minutes: My Banner Faculty Self-Service Account
  - Introduction to Banner (2 Minutes)
  - Login In to Faculty Self-Service For the First Time (2 Minutes)
  - Introduction to Your Self-Service Banner Session and Main Menu (4 Minute)
  - Introduction to Your Faculty Schedule (6 Minutes)
    - Detailed Schedule
    - Week at a Glance
    - Master Class Schedule
  - Start With the End in Mind: How To Submit Student Grades at the End of Semester in Banner (6 Minutes)

ITD-Classroom Services 4 PMU Faculty (1 Time for 1 Hr Long)

- Two Groups - Male and Female (1 Hr Long)
- Traditional 20 Minutes
- Smart 20 Minutes
- Enhanced 20 Minutes

Traditional Classrooms: 20 Mins

- Instructor Work Station
- Projector
- Smart Board & Promethean Active Boards (Female)

Smart Classrooms: 20 Mins

- Instructor Podiums
- Projectors
- Review After the Walk Through:
  - YouTube Playlist: Smart Classroom Basics at PMU
  - Google Presentation: Overview of Smart Classrooms at PMU

Enhanced Classrooms: 20 Mins

- Instructor Podiums
- Projectors
- Video Conferencing

ITD-College Blackboard for Beginners (ITD Will Be Doing 3 Times for 1 Hr)

- **ITD Will Be Doing Three Level I Sessions:**
  - **Getting and Setting Up**
    - Accessing Url
    - Login
    - Changing password
  - **Introduction to Syllabus, Hours, Assignments, Presentations**
- Later Topics Will Include:
  - Level II: Tracking Assignments & Grade Book
  - Level III: Assessments & Tests
  - Level IV: Working With Instructional Multimedia

Using YouTube for Teaching & Learning @PMU

College of Business
Fall 2011

What is YouTube Good For?

@PMU?

Dr. Michael E. Dobe, Sr.
professordobe's Channel

All | Uploads | Favorites | Playlists

Uploads (134)

see all
arrange

HIST 1301 Review (I of 6)
342 views - 1 year ago

HIST 1301 Review (2 of 6)
288 views - 1 year ago

HIST 1301 Review (3 of 6)
171 views - 1 year ago

HIST 1301 Review (4 of 6)
142 views - 1 year ago

HIST 1301 Review (5 of 6)
83 views - 1 year ago

HIST 1301 Review (6 of 6)
200 views - 1 year ago

Favorites (81)

see all
arrange

David Blight on Frederick Douglass
gilderleh... - 614 views

Discovery Uncovering the real Gangs of New
Docmate - 35,969 views

Discovery Uncovering the real Gangs of New
Docmate - 36,463 views

Discovery Uncovering the real Gangs of New
Docmate - 45,980 views

Discovery - Uncovering the real Gangs of New
Docmate - 87,537 views

Playlists (81)

see all
arrange

Strategic Management
2 months ago
more info

Dr. Bruce's Aramco Health and Wellness
3 months ago
more info

New Student Orientation @PMU
4 months ago
more info

Smart Classroom Basics @PMU
1 month ago
more info

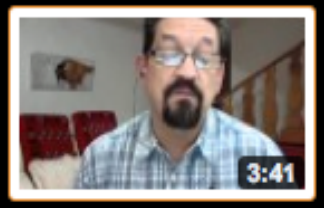
HIST 1301 Exam Review
3 months ago
more info

« Back to Playlists

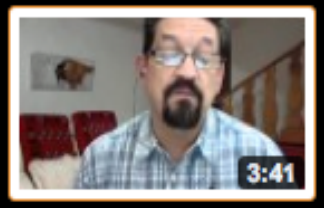
Edit My Playlist

Strategic Management

URL: http://www.youtube.com/user/professordobe#grid/user/DCCF62A0E9E5E5DB

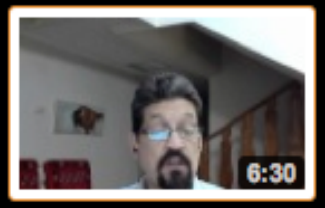


BUSI 4362 Strategic Management
cisnerosfgp1
123 views

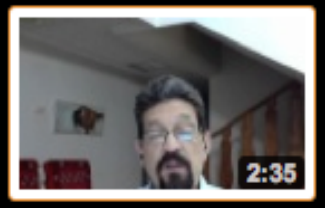


BUSI 4362 Strategic Management
cisnerosfgp1
123 views

BUSI 4362 Strategic Management Base
cisnerosfgp1
85 views



BUSI 4261 Entrepreneurship
cisnerosfgp1
7 views



BUSI 4261 Entrepreneurship
cisnerosfgp1
8 views

Class Notes Mission Statement Vision and
cisnerosfgp1
36 views

« Back to Playlists

Edit My Playlist

Dr. Bruce's Aramco Health and Wellness Workshop

Videos of the 6 June 2011 Health and Wellness Workshop conducted at the Aramco Abqaiq facilities by Dr. Bruce Wells (PMU).

URL: http://www.youtube.com/user/professordobe#grid/user/E8B08985862C8E0F

Health and Wellness Workshop at ARAMCO
professordobe
358 views

Health and Wellness Workshop at ARAMCO
professordobe
153 views

Health and Wellness Workshop at ARAMCO
professordobe
262 views

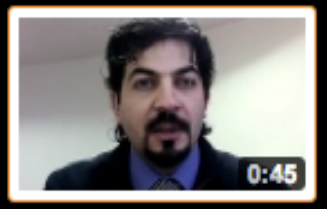
« Back to Playlists

Edit My Playlist

New Student Orientation @PMU

URL: http://www.youtube.com/user/professordobe#grid/user/E97C64A6A767A6E5

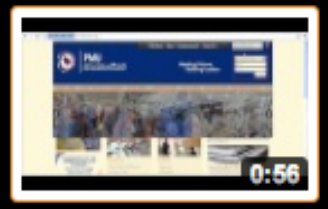
PMU IT Services - English
professordobe
70 views



PMU IT Services - Arabic
professordobe
71 views

PMU Laptop Configuration -
professordobe
63 views

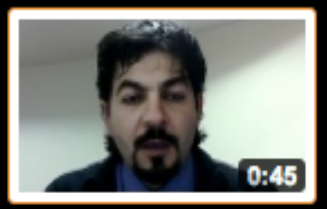
PMU Laptop Configuration - Arabic
professordobe
82 views



PMU EMail - English
professordobe
46 views

PMU EMail - Arabic
professordobe
46 views

PMU IT Help Desk - English
professordobe
87 views



PMU IT Help Desk - Arabic
professordobe
73 views

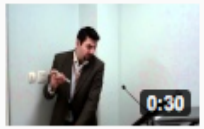
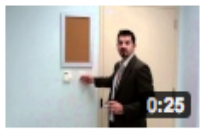
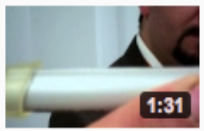
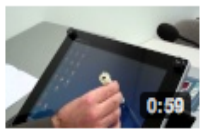
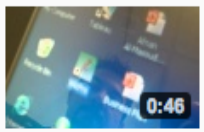
Smart Classroom Basics @PMU

by professordobe's channel

Play All Share

Edit Playlist

10 videos | 12:13 duration | 40 views

1	 0:30	Smart Step 01 - Logging Into Active Directory by professordobe	47 views
2	 0:40	Smart Step 02 - Turning on Power, Lights, Lowering S... by professordobe	35 views
3	 0:59	Smart Step 03 - Turning on the Overhead Projector by professordobe	24 views
4	 0:25	Smart Step 04 - Adjusting Lighting in Classroom by professordobe	21 views
5	 1:31	Smart Step 05 - Turning on Wireless Stylus (Pen) by professordobe	27 views
6	 0:59	Smart Step 06 - Using the Wizpro Software by professordobe	14 views
7	 0:46	Smart Step 07 - Double Take on the Wizpro Software by professordobe	17 views

About Playlist Creator

19,624 views
22 subscribers

http://www.youtube.com/playlist?list=PLA2BAA4FAD05509AC&feature=viewall

How to Become a YouTube Content Creator

@PMU?

What Do You Need?

- A Couple Hours of Your Time
- An Internet Connection (Home or Office)
- A Computer With a WebCam
- Video Recording Software ...
- For Example These Programs Come With Your Operating System:
  - Windows Movie Maker
  - Apple QuickTime
- Last But Not Least: A YouTube Account (Do I Mention it is Free?)

A Couple Hours of Your Time

- Well, we don't have that much time, so we'll have to rush ...

An Internet Connection

- The faster the better... STC DSL is probably your best bet at this point.
- Today we will be using the on campus connection.

A Compter With a Web Cam

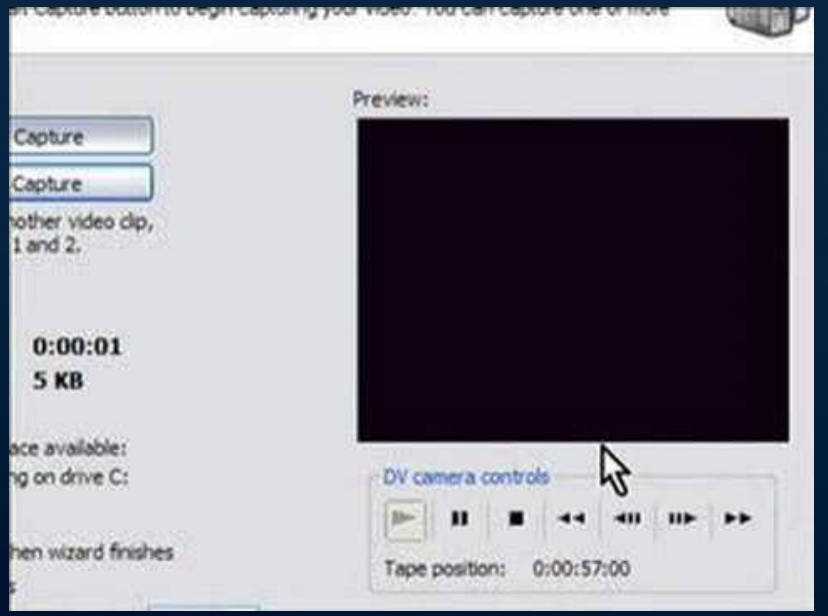
- Carrefour and Jarir Bookstore Carry Web Cams Ranging from 100 - 400 SAR
- You Get What You Pay For!
- On campus, you can use your office laptop or visit the Microstudio on the first floor of Wing B ...

PMU Microstudio

SEARCH YOUTUBE FOR >>>>

Windows Movie Maker YouTube Tutorial

How To Create A YouTube Account & Upload Your First Video



YouTube's Powerful Features

@PMU?

What Next Now That I Have an Account and am Uploading?

- Linking to Your Video in Blackboard
- Security Options: Public, Unlisted, Private
- Advanced Topics:
  - Embed Code
  - Closed Captioning

ENGINEERING AND TECHNICAL AFFAIRS DIVISION

ENGINEERING AND TECHNICAL AFFAIRES Division is the backbone of PMU to give to students, scholars and workers a safe and healthy environment for high quality education, monitoring all facilities to correct every kind of abnormalities and working hard pursuing excellence on serving the external constituencies of the University. Also it is the responsible for the proper maintenance of all P.M.U. facilities from University Campus to housing facilities and compounds at Al-Khobar.

Engineering and Technical Affaires Division is constituted by five Departments as follows:

1. **Engineering Affairs**
   - **1.1 Projects Section**
   - **1.2 Operation & Maintenance Section**
2. **Safety & Security Department**
3. **QA /QC Department**
4. **Support and Auxiliary Services**
5. **IT – Chief Information Office**

Regular meetings are held between E.T.A. Supervisor and managers of each Department discussing needs and situations to conceive solutions, planning activities for development not only regarding present and future projects as also operations and maintenance of existing facilities.

Overall Star Rating:

1. Engineering Affairs

This Department not only is the physical responsible for the existence of the before referred environment as it was one the first Departments of PMU and the one who made possible the existence of the University starting with the achievement of Mini-Campus by 2006 that allowed PMU to begin its teaching activities.

Engineering Affaires Department is composed by two sections, Projects section and Operation and Maintenance Section.

Overall Engineering Affaires Department Star Rating: 3.05

1.1. Projects Section

Coordination and control of all works at PMU from Civil to Mechanical and Electrical, of all Landscaping Works, all activities involving all Projects regarding PMU, both the existing ones as the new ones, including preparation and follow-up at their different stages like the new Housing Project for instance, and also follow-up and support in all technical aspects to all other PMU's Departments and Sections with special attention on the Operation and Maintenance one.

Main objectives to be achieved in the near future:

- Completion of PMU's Landscaping Project, including Green House.
- Construction of Reverse Osmosis Plant at PMU.
- Total completion of PMU's Project in every aspect.
- PMU's Housing Project execution.
- Construction of New offices at Administration Building's free area.
- Increment of Conference Hall's Sound System.
- Development of Prince Sultan College (for sight handicaps) Project.
- Improvement of Air conditioning at Chiller Plant Unit.
- Increase of Electrical Power Supply.

PROJECTS SECTION SELF EVALUATION RATE

1.1.1 – Policy and Planning

Star Rating: 3.5

1.1.2 – Quality and Adequacy of Facilities and Equipment

Star Rating: 3.0

1.1.3 – Management and Administration

Star Rating: 3.0

1.1.4 – Information Technology

Star Rating: Not Applicable to ETA Projects Section

1.1.5 – Students Residences

Star Rating: Not Applicable to ETA Projects Section

Projects Section Overall Star Rating: 3.17

1.2. Operation & Maintenance Section

This Section deals with Operations and Maintenance of all PMU's facilities and housing, by establishing an effective help desk services that receives and distributes maintenance requests through e-mails to proper concerned departments and personals.

It's quite remarkable its achievements within such a short period of time improving the operation of a full team equipped and trained to perform normal, emergency, and preventive maintenance activities at PMU Campus and Housing Effectively in order to provide proper educational environment.

To provide high quality services and well maintained educational environment and reach to the customer satisfaction, following initiative have been established:

- Improving help desk services to receive and distribute maintenance request e-mails to proper concern departments and personals with more advanced follow up system.
- Services provided should be scheduled and conducted in proper timing and without affecting the operation of the university.
- Proper maintenance plans should be prepared and updated frequently in order to meet the recent requirements.
- Perform preventive maintenance and check-up activities effectively scheduled.

To provide a full qualified maintenance team staff, the following is now being done or to be done in the nearest future:

- Recruitment of additional highly qualified trained technicians.
- Ongoing site job training for technicians.
- Site permanent technical supervision.
- Maintain workforce motivation properly.
- Reach adequate number of skilled manpower on Maintenance Team.
- Improvement of Material Controlling System.
- Improvement of adequate financial operation and maintenance budget.
- Operation and Maintenance vehicles proper maintenance to improve.

OPERATION AND MAINTENANCE SECTION SELF EVALUATION RATE

1.2.1 – Policy and Planning

Star Rating: 2.75

1.2.2 – Quality and Adequacy of Facilities and Equipment

Star Rating: 2.86

1.2.3 – Management and Administration

Star Rating: 3.16

1.2.4 – Information Technology

Star Rating: Not Applicable to ETA Op. & Mnt. Section

1.2.5 – Students Residences

Star Rating: Not Applicable to ETA Op. & Mnt. Section

Operations & Maintenance Section Overall Star Rating: 2.92

1.3. Safety & Security Section

As the name indicates this Department is composed by two distinct sections working along with each other.

Safety Section deals with all aspects regarding this matter in all PMU Campus.

This is a very small section, comparing to Security Section which has more than 15 workers, however has already achieved some important assets to PMU:

- Established a zero major incidents /accidents record due to the implemented safety rules and regulations.
- Provided fire protection equipments and regularly inspected and maintained by the contractor to avoid any failure.
- Conducted the Fire Extinguisher Training to produce fire volunteer's team.
- Submitted daily observation and monthly summary reports.

To keep this racket these are going to be done in the nearest future:

- Maintenance zero major incident / accident record.
- Fire drill and safety training to PMU's staff.
- Creation of a fire fighting & rescue team to answer any emergency.
- Provision of fire truck, additional fire fighting equipments and tools according to the future needs.
- Promotion of safety slogan /campaign contest.
- Provision of service vehicle for safety department .

SAFETY SECTION SELF EVALUATION RATE

1.1.1 – Policy and Planning

Star Rating: 3.0

1.1.2 – Quality and Adequacy of Facilities and Equipment

Star Rating: 2.7

1.1.3 – Management and Administration

Star Rating: 2.75

1.1.4 – Information Technology

Star Rating: Not Applicable to ETA Safety Section

1.1.5 – Students Residences

Star Rating: Not Applicable to ETA Safety Section

E.T.A. SAFETY Section Overall Star Rating: 2.82