ICT & Knowledge Management Directorate Handbook - V 2.0

Applied Science University

Bahrain | Higher Education

2014 – 2015

Volume 2.0

Contents

Forward

We will develop, maintain and make available an ICT infrastructure and knowledge management environment, which is "best in class" while remaining aligned with the University's requirements. This will provide a strong, technologically rich, yet focused environment that supports teaching, research, learning and administration. ICT & KM will support existing and anticipated business requirements, while also influencing and shaping future developments and innovation across all of the University's functions, supporting change and organizational transformation as appropriate.

CHAPTER 1: ICT & KM VISION AND OBJECTIVES

1.1 Vision

To provide a contemporary and integrated technological environment, which sustains and strengthens the University's ability to deliver its strategic objectives, facilitating collaboration, excellent teaching and research, and efficient business processes.
We aim to deliver an environment which will support students, researchers and academics by providing an empowering platform and knowledge creation and exchange.

1.2 Objective

The ICT & KM Directorate is committed to developing, deploying and supporting innovative, quality and sustainable ICT solutions and services that meet the changing learning, teaching, research and management needs of the University. In addition, to maximize student and staff productivity, enhance teaching, learning and improve quality of research through Information Communication Technology and Knowledge Management. Our services will be recognized as an innovative and influential function, playing a core role in the operation and ongoing development of the University.

CHAPTER 2: STRATEGY OVERVIEW

2.1 ICT & KM Strategy Overview

- Address user demand for sophisticated, high quality, ubiquitous and reliable ICT provision whilst recognizing economic constraints;
- Promote a culture of customer focus in all ICT structures;
- Identify a long term, sustainable and accessible solution that addresses increasing demands for storage and the integration and interoperability of our ICT systems;
- Enable capacity to meet increasing network bandwidth demands and reduce single points of failure that would threaten the availability of network connectivity;
- Create additional business efficiencies, whilst improving service quality through centralization of core ICT provision, reducing duplication and the complexity of multiple systems and services where these exist at local level;
- Improve information security provision i.e. the confidentiality, reliability and availability of ICT systems and the information processed by those systems – reducing the likelihood of data breaches and/or the loss of confidential or personal data;
- Significantly reduce the ICT carbon footprint in the face of rising energy costs.

Our strategic plan aims are:

2.1.1 Research

"Helping facilitate our position as a distinctive, internationally renowned, research intensive institution", by:

- Providing a flexible, expandable and secure infrastructure and an information governance framework to support and sustain an excellent research base at the University, so that institutional requirements and aspirations can be met.
- Supporting the research community by technical support and guidance, drawing upon governmental and research networks and funder requirements, and working with others to apply these throughout the research lifecycle.
- Engaging with the research community, alerting others to significant developments in ICT, information processing and governance that could support and enhance research activity.

2.1.2 Learning and teaching

”Providing the technology to facilitate all modes of learning and teaching”, by:

- Providing a flexible, expandable and secure infrastructure and an information governance framework to support and sustain excellence in learning and teaching at the University, so that institutional requirements and personal aspirations can be met.
- Ensuring as far as possible that the University ICT infrastructure is agile and capable of change so that future requirements of the University and those of individual learners can be met with minimal impact on the University.
- Facilitating seamless communication in support of learning and teaching.
- Identifying and bring to the University’s attention technological innovations that could enhance the learning experience.
- Working with academic staff and students to understand learner needs.

2.1.3 Support

- Providing the technology, infrastructure and expertise to enable University staff and those engaged by ICT Services to be effective in their jobs.
- Contributing to the effective operations of the University through the appropriate deployment of technologies to enable business change and drive efficiencies.
- Providing an ICT and information management infrastructure to fully support existing and future requirements.
- Providing an effective, trusted management information system infrastructure that allows business units to collect and process information in line with their strategic and operational requirements.
- Ensuring that the confidentiality, reliability and availability of information systems and the information held, processed by those systems are protected and maintained.

2.2 ICT & KM Strategy Plan

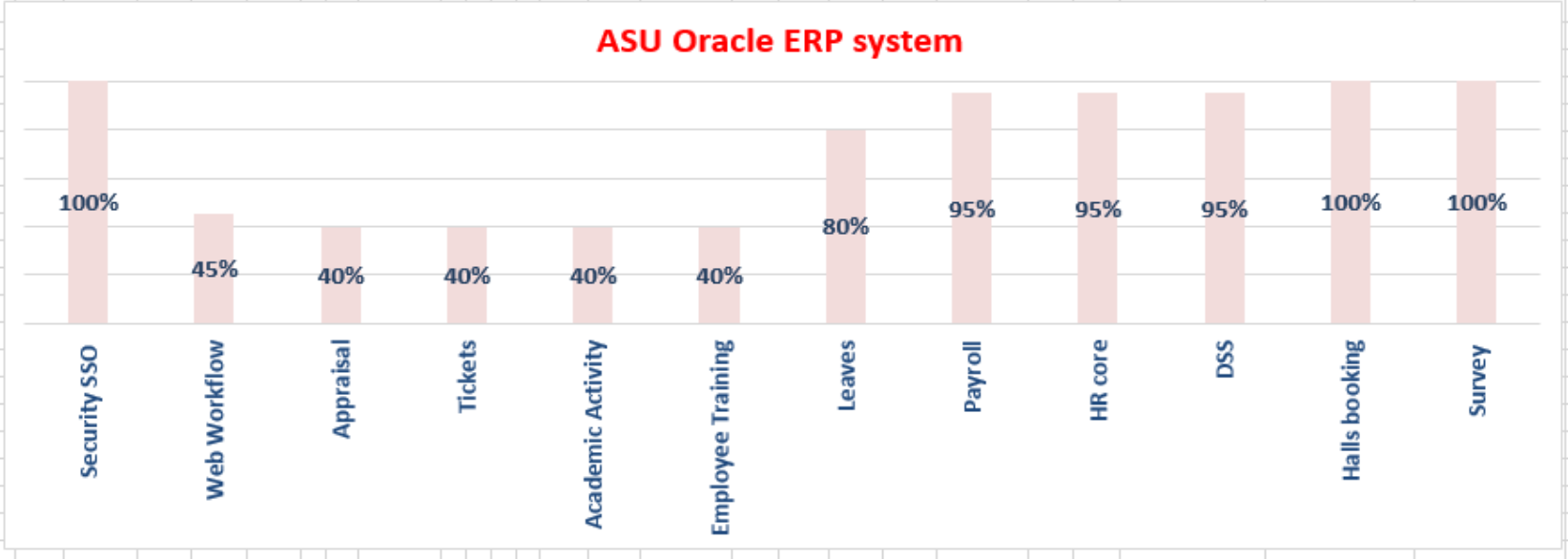
The ICT & KM Directorate was established in September 2013, and works to enhance its tasks (Strategic, Operational, and Day-to-day tasks) by both structure and department specialization. This section details the most important achievements during the last year.

Oracle ERP system

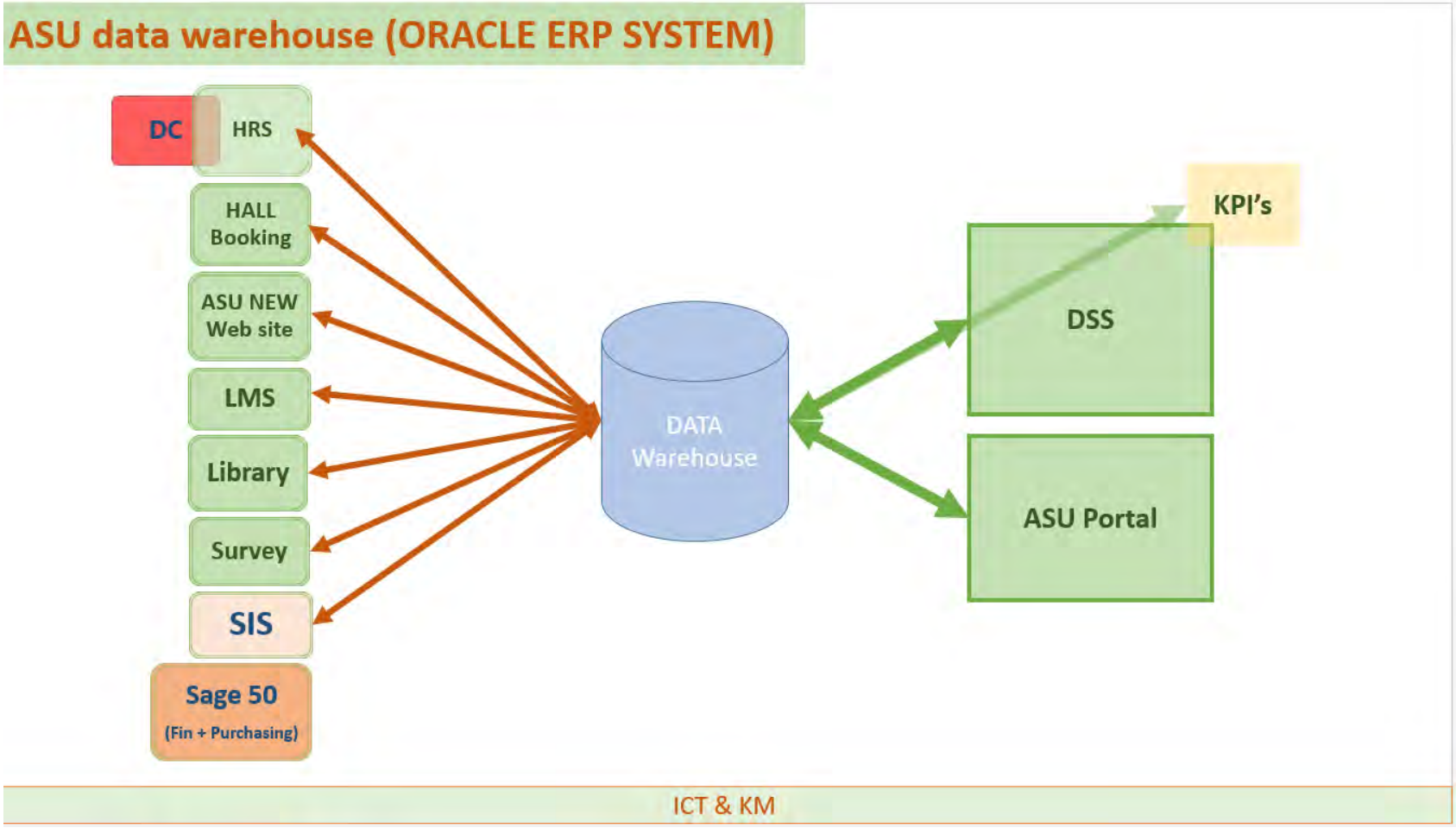
FROM 3/2014 TO 7/2015

SYSTEMS	Tasks Phases for each Month	Done %	Expected Date to complete with the current developers	Expected Date to complete with 2 developers
Security SSO		100%	–	–
Web Workflow		45%	Nov-15	Jul-15
Appraisal		40%	Apr-16	Oct-15
Tickets		40%	Dec-15	Aug-15
Academic Activity		40%	Jan-16	Sep-15
Employee Training		40%	Jul-16	Nov-15
Leaves		80%	Jun-15	May-15
Payroll		95%	–	–
HR core		95%	–	–
DSS		95%	–	–
Halls booking		100%	–	–
Survey		100%	–	–
	3/2014 4/2014 5/2014 6/2014 7/2014 8/2014 9/2014 10/2014 11/2014 12/2014 1/2015 2/2015 3/2015	73%	–	–

- Business Requirements Definition
- Existing Systems Examination
- Database Design and Build
- Application Development
- Data Conversion
- Integration
- Testing
- Training



2.3 ASU Data Warehouse (ORACLE ERP SYSTEM)



2.4 **ICT & KM Future Plan (ICT & KM Dream):**

Our vision is to have an ASU ERP, and the main targets that should be achieved after 3 years are;

ASU Portal
Training System
Student Complaint System-Tracking
Inventory System
Financial System + Fixed Assets+ Cost Centre
QA System
Research portal system
New SIS
ASU KPI's Dashboard
Archive System

CHAPTER 3: ICT & KM POLICY

3.1 ICT & KM Policy Statement

The Applied Science University (ASU) Information Communication Technology & Knowledge Management (ICT & KM) policy is the document governing the use of the University's ICT resources and internet access. The policy lays down the rules & regulations to guide the employees of the university, and is not intended to be an exact or implied contract.
It is clearly not possible to anticipate every situation in advance that may arise in the working environment or to give information that responds to every possible question. Therefore, the employees are expected to use their sound management, good judgment or common sense while acting in relation to the matters covered herein.

3.2 ICT & KM hardware acquisition and installation

The policy is intended to streamline the process of acquisition and installation of ICT hardware, from the point of identification for a need to purchase hardware, initiation of request to purchase hardware up to the point of purchase and installation of the hardware.

3.3 Hardware Selection Process

Prior to raising a request for purchase of any computer hardware or accessory, the faculty or staff member should consult with the following:

I. The ICT director to determine what items may or may not be compatible with the system and what items may be available in bulk purchase through the University.
II. Approach their respective Dean / Director of the College / Departmental for approval who shall determine whether multiple purchases of such hardware items may be warranted for department members.

3.4 Hardware Procurement Process

I. The Director of ICT shall initiate the purchase of hardware by eliciting quotes from a minimum of 3 vendors.
II. The quotes shall be compared on the basis of cost and features of the equipment. Additional benefits, if any, provided by any vendor, such as after sales support, maintenance support etc. shall be taken into account while short listing the final vendor.

III. The ICT & KM Directorate shall endeavour to ensure delivery of new hardware items in a timely manner after the receipt of approval from the respective Dean / Director of the College / Department.

3.5 Hardware Installation

I. Configuration, troubleshooting and adjustment of the hardware item by the ICT & KM Directorate to meet system compatibility requirements – the user should keep a log of any difficulties encountered with the new hardware during the initial month, and ensure a replacement if there is any persistent problem.
II. The ICT & KM Directorate shall be responsible for the installation of the hardware and ensuring that any initial issues / problems with the hardware, if any, are effectively resolved.

3.6 Hardware and Software maintenance

I. The ICT & KM Directorate will perform regular maintenance and upgrade on University Hardware and Software
II. The ICT & KM Directorate will ensure that subscriptions and licenses are periodically renewed for uninterrupted and smooth operations across the University systems
III. The ICT & KM Directorate will develop annual maintenance schedule for ICT equipment and Hardware and Software such as Servers, Routers, and Projectors etc.
    a. This schedule will contain the expiry dates of software agreements and the renewal schedule
    b. Schedule for Routine disk cleaning or formatting of Hard Drives as well as physical cleaning of the equipment.
IV. The ICT & KM Directorate will ensure that all university computers have anti-virus applications, appropriate firewalls, and anti-hacking software in place.

3.7 Internet Acceptable Use Policy

3.7.1 Purpose

The objective of this policy is to define the acceptable and unacceptable use of University's Internet resources, including the World Wide Web, e-gate, e-library, and FTP (file transfer protocol).

3.7.2 User Account information

The access to the internet resources at the University is controlled through individual domain user accounts and passwords. It is mandatory for each user of the University's internet resources to read this policy and sign an agreement on internet use before receiving the access details and password to the university network.
The ICT & KM Directorate is designated to assign authority / privileges for accessing the internet. The department directors/deans are authorized parties to approve requests for critical additional privileges for any staff in their department. A written request must be made to the ICT & KM Directorate.

3.7.3 Appropriate Use

The internet is available to staff of the University to facilitate achievement of University's aims and objectives. The following activities are considered appropriate for use of internet:

I. Collaborating with fellow staff, international researchers, students, academicians at other universities in the country etc. within the background of an individual's assigned duties.
II. Conducting any academic research.
III. Sharing or acquiring information required or related to the performance record of an individual's assigned duties.
IV. Taking part in professional or educational development activities.

3.7.4 Inappropriate Use

The excessive personal use of internet for carrying out leisure activities will be considered inappropriate. Internet use at the University must be in compliance with national laws, University policies and all the University contracts. This policy includes, but is not limited to, the following:

I. The Internet shouldn't be used for unlawful or illegal purposes, including copyright infringement, libel, obscenity, slander, defamation, fraud, plagiarism, intimidation, harassment, forgery, illegal gambling, impersonation, asking for illegal schemes, & computer tampering (e.g. distribution of PC viruses).
II. The Internet facility should not be used in a manner that harms the University's rules, policies, or administrative guidelines. Use of the Internet in a way that is not appropriate with the mission of the University, misrepresents the University, or violates any of the University policy is prohibited.
III. All employees must limit their private/ personal use of the Internet. The University allows restricted personal use for communication with friends and family, free learning and public service. The University forbids use for bulk unsolicited mailings, allowing for non-

employees to use the University's internet resources, or commercial activity unless prior approval is obtained from the ICT & KM.

IV. The individuals are prohibited to copy, alter or destroy the data, documentation, software, or data communications internal to the University or another third person without official permission.

V. With the concern of maintaining better network performance, users should avoid the sending of large e-mail attachments.

3.8 **Security**

Since the domain user account is the gateway to the internet, for security purposes, users shouldn't share their unique account information with another person. All individual accounts are unique and are to be used only by the given user of the account for approved purposes.
Users are required to reset or obtain a new password if they feel that any unauthorized user has learned/ memorized their password. Strong passwords are crucial for preventing unauthorized access to electronic devices and accounts. Passwords should not include guessable names or easily obtainable information about the user and must not consist of all numbers or all alphabets or less than 8 characters in length. Passwords should contain mixed-case alphabetic and non-alphabetic characters and must be easy to remember.

Users are advised to take all required precautions to avoid unauthorized access to the internet facility, as they shall be liable for any inappropriate use of internet done through their account.

3.9 Failure to Comply

Abuses of this policy will be taken as other allegations of unlawful activity at the University. Claims of misconduct will be judged according to the established procedures. Actions for inappropriate use of the Internet facility may result in, but are not limited to, one or more of the following actions:

I. Temporary or permanent cancellation of access to some or all resources of internet & facilities.

II. Disciplinary action according to University policies.

III. Steps towards legal action as per the applicable laws and signed agreements.

3.10 **Monitoring and Filtering**

The ICT & KM Directorate may monitor any Internet activity occurring on University equipment or accounts. If the University finds activities that have conflict with applicable law or University policy, records/ archives retrieved may be used to document the unlawful content in accordance with established procedures.

3.11 Maintaining reliable internet and intranet infrastructure

ICT&KM strive to provide stable connection to the internet and intranet to ASU all faculty members, staff and students. Through a high quality connection which contains two communication technologies, microwave to maintain internet and data transmission with speed up to 10 Mbps and leased line to maintain voice and telephony services with 4 Mbps speed and the two technologies are pre-configured as failover to recover any failure in each other.

Disclaimer

The University accepts no liability for any indirect or direct harm arising from the staff's connection to the Internet. The University is not answerable for the accuracy of any information taken from the Internet and it only facilitates the accessing platform and distribution of data through its systems. The internet should be used sensibly by the employees. Users are responsible for any material that they access and publish through the Internet.

3.12 Intranet Acceptable Use Policy

3.12.1 Purpose

The employees are expected to comply with the legal and ethical use guidelines of the University Intranet Systems. Any information and materials provided on the University Intranet portal is owned by the University. This information can only be used for the purpose of the university and any personal use of this information is not permissible.

This policy assures that the University will not be held liable for any unauthorized use of information through the Intranet. The University hopes to have a rich Intranet System and will keep updating the content at regular intervals.

3.12.2 Scope

This applies to all the users of the University Intranet portal starting with its full time employees, temporary employees, University students, contractors, consultants and any other employees who work at the University. Any modules or materials available on the University Intranet Portal system falls under this policy.

3.12.3 Acceptable Use

I. Only domain users who already have a Username and Password shall be granted access to the portal. Users with access to the portal should adhere to the policy and use the content appropriately.
II. Any information added to the University portal by the users is owned by the University. However, the University's ICT & KM Directorate will not be held responsible for guaranteeing the confidentiality and the accuracy of any data uploaded by authorized user through the University Intranet Portal.
III. All the pages contained within the Intranet portal are the property of the University; therefore, these pages should not be used for personal use and the employees should use their reasonable judgment to be judicious about what is added to the intranet.
IV. Users should make sure not to keep any information suspected to be confidential on the Intranet portal without getting approval from their line managers.
V. In order to maintain security, the ICT & KM Directorate is eligible to monitor network traffic and data uploaded at any time.
VI. The University has the absolute right to audit content, systems and network traffic on a periodic basis.

3.12.4 Security and Proprietary Information

I. In case confidential information is uploaded to the University Intranet Portal; it should be marked as confidential and this information should only be accessible to authorized users.
II. Authorized users should not expose their usernames and passwords as they will be held liable for any abuse that happens through their accounts.
III. If a user finds that there is certain confidential information accessible by them or others inadvertently (due to a technical glitch), then they must contact their line manager

3.12.5 Unacceptable Use

A list of prohibited actions has been provided below. However, there may be instances in which it is deemed necessary for an employee to be excused from one or more of these constraints. The employees using ASU's Intranet Systems will not be allowed to violate the rules as laid out under any circumstances under local, national or even international law. The points listed below represent a framework for unacceptable use of the system. The following actions are highly forbidden without exception:

I. Abusing the rights of a copyright protected property such as: patents, trading secrets, intellectual property, and distribution of published information or any pirated application that is not licensed for use by the University.
II. Unauthorized publishing, distributing or digitizing any copyrighted material, whether it includes photos, music, magazines but not limited to the mentioned above.
III. Using malicious programs in the system or any of the servers.
IV. Exposing one's password and allowing other to get access through their account.
V. Breaching security or affecting the network communication purposely in any way.
VI. Exposing information about any of the University's students, employees to parties from outside the University without proper authorization.

3.12.6 Enforcement

Employees or students caught violating the policy rules, will face a claim for damages and disciplinary action as per Universities guidelines.

Processes shall be run periodically to ensure that the policy is being applied in its entirety. If an employee violates or is found to have been involved in any illegal action or activity, then the ICT

& KM Directorate will inform their Dean/ Director and will specify what actions are be taken against him/ her.

In case an employee fails to satisfy the general guidelines, then he / she will be contacted by the ICT & KM Directorate to remove the content. However, if the content is affecting the performance of the system; it may also be removed immediately before contacting the concerned person.

3.13 E-Mail Acceptable Use Policy

3.13.1 Purpose

E-mail is a major mechanism for business communications or collaboration at the University. The use of the University's e-mail system and services is a privilege; thus, it must be used judiciously. The purpose of this policy is to lay down the appropriate and inappropriate use of University's e-mail systems and services, in order to reduce disruptions of activities and to comply with applicable policies and regulations.

3.13.2 Scope

This policy is applicable to all e-mail, exchange systems and services owned by the University, all e-mail account users/holders at the University.

3.13.3 Account Activation/Termination

E-mail access at the University is controlled through individual accounts and passwords. Each user of the University's e-mail & exchange system is obliged to read & sign a copy of the Electronic mail Acceptable Use Policy before receiving an e-mail account and password. It is the duty of the staff to safeguard the confidentiality of their account & password information.

All staff of the University are eligible to have an e-mail account. The accounts will be approved to the third party non-employees on a case-by-case basis, and shall be specifically approved by ICT & KM. The following outsiders (non-employees) may be eligible to access Universities e-mail account:

I. Contractors/ Consultants,
II. Maintenance & service providers, and
III. Audit & Quality assurance teams.

Requests for these accounts must be given in writing to the ICT & KM Directorate. All terms, conditions and limitations governing e-mail use should be communicated and agreed upon using a written and signed agreement.

The mail facility will be discontinued when the staff or third party stops their association with the University, unless any other preparations are made. The University is under no responsibility to forward or store the contents of an individual's e-mail account after the term of their service has ceased.

3.13.4 Expectations from End Users

The main official communications frequently delivered through e-mail. Therefore, the University staff and students with e-mail accounts are required to check their e-mail in a regular & timely manner.
It is the duty of the E-mail user to manage her/his mailbox including cleaning and organizing mails. If a user joins a mailing list, they must be aware of how to exit the list, or re-join the list in the event that their existing e-mail address changes. Mail users are also required to abide by. Normal standards of personal and professional courtesy and conduct in using the email communication.

3.13.5 Appropriate Use

All the employees at the University should use their official accounts for formal communication and for official purposes; and should avoid its usage for exchanging personal mail. The following activities are considered acceptable for use of Universities e-mail resources:

I. Communicating with staff, students, researchers, academicians at other partner Universities, etc.
II. Acquiring or providing information essential or related to the performance of an individual's assigned duties.
III. Taking part in professional or educational, development activities.

3.13.6 Inappropriate Use

The University's e-mail systems should not be used for activities that could cause excessive load on the system. Further, the e-mail use at the University should comply with all applicable laws, the University policies and agreements.
The following actions shall be considered inappropriate use of the University systems:

I. The use of university e-mail for criminal or unlawful purposes, including copyright infringement, offensiveness, slander, libel, defamation, plagiarism, fraud, harassment, forgery, intimidation, soliciting for illegal pyramid schemes, impersonation, and computer damaging activities (e.g. the spreading of computer viruses).
II. The use of e-mail in any way that violate the University's policies, rules, or administrative regulations.
III. Viewing or copying or altering, or deleting the e-mail or files belonging to another individual without proper permission.
IV. Sending of excessively large e-mail attachments. The total size of an individual's e-mail message sent (including attachment) must be 2 MB or less from an internal account & 20 MB from an External account.
V. Opening attachments of e-mails from strange or unknown sources. Attachments are the major source of PC viruses and those should be treated with maximum attention.
VI. E-mail accounts are unique and only to be used by registered users; therefore, sharing or exchanging e-mail account passwords with someone else, or trying to obtain another individual's e-mail account password is considered inappropriate.
VII. The University permits limited personal use of the mail resources for communication with friends and family, free learning and public services. The University forbids personal use of its e-mail resources and services for uninvited bulk mailings, political campaigning, non-university commercial activities, and dissemination of chain letters.

3.13.7 Monitoring and Confidentiality

The University may at its own discretion screen any / all e-mail circulation passing over its e-mail system. While the university doesn't read/view the end user e-mail; however, e-mail messages may be read by ICT staff during the usual audit and process of managing the system.
Additionally, backup copies of e-mail messages may exist, regardless of end-user deletion, in compliance with the University's information policy. The objective of archiving is to avoid the loss of business data.
If the University finds out or has a proper reason to suspect any activities that are in conflict with applicable laws of the university or this policy, then the e-mail records may be saved and used to document the activity as evidence. All possible efforts will be taken to inform an employee, if their e-mail archives are to be reviewed. Notification may not be possible if the staff member cannot be contacted due to unreachable absence.
The employees must pay extra attention when sending confidential or sensitive data via e-mail as all the e-mail messages sent outside of the University will be a property of the receiver. As a

rule of thumb, it is better not to communicate any information that one would not feel as comfortable being made public.

Extra care must be shown before using the command of "Reply" or "forward" during the e-mail communication.

3.13.8 Reporting Misuse

Any claims of misuse must be properly reported to the ICT & KM directorate.

3.13.9 Failure to Comply

Abuse of this policy will be taken as an act of misconduct at the University. The allegations of misbehaviour will be treated as per the established procedures. The following action may be taken for inappropriate use of the University's e-mail systems & services:

1. Temporary or permanent cancellation of e-mail access.
2. Disciplinary action according to the applicable University policies.
3. Legal action as per the applicable laws and the signed contractual agreements.

Disclaimer

The University accepts no legal responsibility for indirect and/or direct damages arising from the employee's use of the University's e-mail services. The employees are completely responsible for the content they distribute. The University is not accountable for any third-party demand, claim, or harm arising out of use the University's e-mail exchange systems or services.

3.14 Applications Development

The ICT & KM's Applications Development Department is responsible for all ASU information systems, the in-house developing and outsource systems, which are used to manage and enhance the faculty, staff and students records and services. The main objective of this department is to enhance any system in-house to get ASU ERP system under the ASU umbrella.

3.15 Information Classification Policy

3.15.1 Purpose

The information contained in this policy includes University information on all the mediums – paper, electronic, and visual (such as video and telephone conferencing) or verbal.

All the key staff members should be aware of the categorization of information and the guidance for handling that will be outlined in this policy. It must be noticed that the sensitive level definitions were created as policies and to emphasize the common logical steps that can be taken to safeguard the University's confidential data (e.g. minutes of meetings shouldn't be left unattended in the meeting room).

3.15.2 Terms and Definitions

I. **Configuration of the University- connections to-other businesses:** Connections will be set up in a way that only specific information is visible to other businesses. This may include setting up applications and network configurations to allow a restricted access to the specific data.
II. **Approved Electronic File Transmission Methods:** Supported FTP clients & Web browsers
III. **Approved Electronic Mail:** All e-mail systems supported by the ICT Support Team
IV. **University Information System Resources:** The University data system resources contain, but are not restricted to, all computers, their programs and data, as well as all paper information & any data at the Internal Use Only rank and above.
V. **Expunge:** To erase reliably or data expunge on a PC, contact the ICT & KM Directorate. It is a must to use a special program to overwrite data as the PC's usual erasure routine keeps the data in recoverable format until overwritten.
VI. **Individual Access Controls:** Individual Access Controls are ways of electronically guarding files from being accessed by third parties other than those specially designated by the proprietor. On personal computers, this includes using the passwords on screensavers and/or Disk lock.
VII. **Insecure Internet Links:** Non-secure Internet Links are all network links that initiate from a local communicate over lines that are not fully under the control of the University.
VIII. **Encryption:** Secure the University Sensitive data as encrypted as per the policy.
IX. **Physical Security:** Physical security denotes having control over the computer or other hardware at all times. This could be achieved by locking and password protecting the devices when not in use. To ensure the physical security of portable devices (notebooks /

laptops), they should always be connected to a lock down cable. It should be ensured that notebook/laptop or other handy computer, are not left unattended alone in a meeting room, hotels or on a flight seat, etc. Make sure the devices are locked or stored properly. While leaving the campus for the day, protect the laptop & any other sensitive material in a locked cabinet or drawer.

3.15.3 Scope

The confidentiality requirement for the University's information will be classified in the following terms:

I. **Public** – this information can be freely shared with individuals on or off campus without any further authorization by the appropriate Information Guardian/ Dean / Departmental head
II. **Internal** – this information can be freely shared with members of the University community. Sharing such information with individuals outside of the University community requires authorization by the appropriate information guardian/ Dean / Departmental head.
III. **Departmental –** this Information can be freely shared with members of the owning department. Sharing such information with individuals outside of the owning department requires authorization by the appropriate information guardian/ Departmental head.
IV. **Confidential** – this information can only be shared on a "need to know" basis with individuals who have been authorized by the appropriate Information Guardian/ Dean / Departmental head, either by job function or by name.
V. **Highly confidential** – this information can only be shared on a "need to know" basis with a limited number of individuals who have been identified by the appropriate Information Guardian/ / Dean / Departmental head.

The University employees are expected to use common sense and sound judgment in safeguarding the University's private information to the suitable extent. If an employee is unclear of the sensitivity of a specific piece of information, they should seek clarity from relevant directors / deans.

3.15.4 Guidelines to manage information sensitivity

The guidelines mentioned below provide information on how to safeguard University data based on the level of sensitivity involved. These guidelines should only be used as a reference, as the security requirements will differ depending on the nature of confidential data in question.

3.15.5 Low Sensitivity

Consists of: General business information; some personnel and technical data.
Storage guidelines: For data in electronic form or hard copy, proper marking should be devised to ensure proper handling of the data.
Access: The University staffs and Students, contractors, individuals with a business need and pre-defined level of authorization.
Distribution within the University: Standard inter-office e-mail, accepted electronic mail & electronic file transfer methods.
Distribution outside of the University, External mail:
From employee@asu.edu.bh mail & other private or public carriers, accepted electronic mail & electronic file transferring ways.
Electronic distribution: No limitations except it should be sent to the only approved receivers.
Disposal/Destruction: Drop outdated papers of information in specially marked disposal bins on the University buildings; electronic records should be purged/ cleared. Reliably wipe out the data or destroy the media physically.
Penalty for intentional or unintentional disclosure: In certain cases of intended disclosure, appropriate disciplinary action will be taken including written warnings up to termination, civil or criminal action to the full extent of the applicable law.

3.15.6 Medium Sensitivity

Consists of: Technical, Business, financial, and most personnel information
Storage guidelines: For data in electronic form or hard copy, proper marking should be devised to ensure proper handling of the data.
Access: To authorized University staff and non-staff with a duly executed non-disclosure agreement.
Distribution within the University: Standard inter-office e-mail, accepted electronic mail & electronic file transfer methods.
Distribution outside of the University External mail: Sent via the University's official id or through permitted private carriers.
Electronic distribution: No restrictions on officially accepted receivers within the University, but it should be sent via a private link or encrypted to the approved recipients outside of the University premises.
Storage: Single and unique access controls are highly recommended for electronic data.
Disposal/Destruction: Drop outdated papers of information in specially marked disposal bins on the University buildings; electronic records should be purged/ cleared. Reliably wipe out the data or destroy the media physically.

Penalty for direct or indirect disclosure: In cases of intended disclosure or negligence shown in the handling of sensitive information appropriate disciplinary action will be taken including written warnings up to termination, civil or criminal action to the full extent of the applicable law.

3.15.7 High Sensitivity

Consists of: internal meeting minutes, business secrets, financial information, personnel data, source code and technical data essential to the success of the University.
Storage guidelines: For data in electronic form or hard copy, proper marking should be devised to ensure proper handling of the data.
Access: Only the individuals assigned with official access and signed non-disclosure contracts.
Distribution within the University: Sent direct – signature needed, envelopes must be stamped confidential, or accepted electronic file transferring methods.
Distribution outside of the University External mail: Handover direct, required a signature, or private approved carriers.
Electronic distribution: No limitation to accepted receivers within the University, but it is highly recommended that all data be strongly encrypted.
Storage: Individual and unique access controls should be used for accessing the electronic data. Physical security must be used and the data should be kept in a physically secured PC.
Disposal / Destruction: The physical copies should be disposed of using specifically marked disposal bins on the University premises; and the electronic data should be wiped out properly from the electronic medium.
Penalty for direct or indirect disclosure: In cases of intended disclosure or negligence shown in the handling of sensitive information, appropriate disciplinary action will be taken including written warnings up to termination, civil or criminal action to the full extent of the applicable law.

3.16 Information Security and Back-up Policy

3.16.1 Scope

This policy contains guidelines for classification of information to make appropriate provisions for the security and back-up of information on the basis of this classification.

3.16.2 Purpose

To minimize information security and business continuity risks associated with data loss by defining a sound back up regime for all the centralized ICT data services.

3.16.3 Definitions and acronyms

Archive – move data to another medium (the backup media) for long term storage. Archive is intended for the storage of data that is not required to be immediately accessible, but which may possibly be required at some point in the future.

Backup – copy data to another medium on a regular basis to protect from active data loss, and to ensure that the data is recoverable in a recent form, if not in completely current version. Backup is primarily required for disaster recovery.

Data custodian – A nominated trustee of ASU's data; a data custodian holds responsibility for protecting the data and for ensuring data integrity. A data custodian may be nominated by their role with the ASU, or by their role in relation to an ICT service. A data custodian will typically have responsibility for the management of a location of shared information, a database, or an application referencing a database distinct from the role of a systems administrator.

Data custodians may include, but are not limited to:

I. Applications manager
II. Data managers
III. Business systems owners

The ASU staff authorized by the ICT & KM to maintain and/or administer ICT services, facilities infrastructure, user level account and passwords.

3.16.4 Classification of information for defining the level of security and back-up

The security and back-up requirements for the information shall be expressed as follows:

I. **Non-critical** – Information is classified as non-critical if its unauthorized modification, loss or destruction would cause little more than temporary inconvenience to the user community and support staff, and incur limited recovery costs. Reasonable measures to protect information deemed "non-critical" include making regular backup copies for the electronic information and using standard access control mechanisms to prevent unauthorized individuals from updating computer-based information
II. **Critical** – Information is classified as critical if its unauthorized modification, loss, or destruction through malicious activity, accident or irresponsible management could potentially cause the University to:
    a. Suffer significant financial loss or damage to its reputation,
    b. Be out of compliance with legal/regulatory or contractual requirements,
    c. Adversely impact its stakeholders.

Therefore, additional safeguards are required to be implemented for securing "**Critical**" information:

I. "Critical" information must be verified either visually or against other sources on a regular basis, and
II. A business continuity plan to recover "critical" information that has been lost or damaged must be developed, documented, deployed and tested annually
III. Proper online security / anti-virus software should be deployed to safeguard the integrity and reliability of this information
IV. Regular back up of this information needs to be maintained at an external location as well

3.16.5 Responsibility

It is the responsibility of the creator of information to classify it as 'critical' or 'non-critical'. This classification should be approved by the departmental head or the dean of the college. It will be the responsibility of the ICT & KM directorate to take relevant steps for ensuring proper back up and safety of this information.

3.17 ICT information system auditing process

ICT & KM is responsible to monitor the information in all ASU systems to ensure of any an authorized changes for the students marking and finance records. This done by an internal information system audit.

3.17.1 Scope

This policy contains guidelines for audit of all ASU information systems to make appropriate provisions for the information security, process, and risk management on the basis of this ICT governance.

3.17.2 Purpose

To minimize risk and business continuity risks associated with information changes by defining an audit process regime for all the centralized ICT information systems.

3.17.3 Responsibility

It is the responsibility of the Dean of Admission and Registration with a reason and evidence. It will be the responsibility of the ICT & KM directorate to take relevant steps for ensuring proper change of this information.

3.18 ICT Service and Help Desk

This policy contains guidelines for providing any service; hardware, software, internet, application, or any troubleshooting, how to receive the service request, record it, and then provide the solution.

3.18.1 Purpose

To minimize number of fails and provide solutions to have business continuity by defining a guidelines process regime for all the staff and students.

3.18.2 Responsibility

It is the responsibility of the ICT & KM directorate to take relevant steps for ensuring solving any ICT problem based on three level to solve any incident.

CHAPTER 4: ICT & KM PROCEDURES

3.19 Set up and maintain an internal University email system

I. ICT& KM have an agreement with Microsoft Office 365 for Educational use which provide ASU with multiple e-mail account hosting that is maintained by Microsoft and controlled by ICT&KM, as shown in Table 3 below.

II. ICT& KM is responsible for configuring the E-mail account for ASU faculty members and staff including Outlook in their office PCs and laptops and web access is guaranteed to them through smart devices and external computers.

III. ICT & KM is responsible for preparing the user guide and training the users about these services.

IV. ICT & KM create the e-mail ID to all the ASU members after a request from the HR department about the new member, and the e-mails ID is:
firstname.lastname@asu.edu.bh

V. ICT & KM create the e-mail ID to all new students in each semester after the registration date is completed, the students and the alumni e-mail ID is:
student ID@student.asu.edu.bh

VI. ASU e-mail protection: ASU will identify the best software to Protect email from spam and malware, and help keep your data confidential. These include:

VII. ASU e-mail flow: ASU email will allow the users to manage mail flow, and track delivery of messages sent by or received from your users through:
   - Anti-malware
   - Anti-spam connection filter
   - Anti-spam content filter
   - Outbound spam
   - DLP policies

VIII. ASU e-mail Auditing: ICT and KM will generate periodical Audit reports to track changes made to mailboxes and organization-wide settings.
   - Custom mail rules
   - Delivery reports

Table 1: ASU e-mails subscription

SUBSCRIPTION	QUANTITY	TERM END DATE
Office 365 Education A2 for Faculty	10000 user licenses	Auto-renews November 25, 2016
Office 365 Education A2 for Students	100000 user licenses	Auto-renews November 25, 2016
Exchange Online (Plan 1) for Alumni	1000000 user licenses	Auto-renews November 25, 2016

3.20 Back-up Procedure

Backup is an automated process, which performed by the backup software, daily. The ICT & KM director will then verify that the process was successful and will save a copy on a labelled tape and DVD and store them in a safe (vault) in the ICT & KM directorate, in the technical support office existing at the basement using safe case against the fire and the fireproof safe located within the University.

The ICT officer will copy all archived backup on the first of each month to send the backup outside the University and will be stored in a fireproof safe, which is **AL AMIN Company** in Mina Salman Industrial Area, (the distance is around **16 Km** from our University).

AL AMIN Company: Manama, Kingdom of Bahrain, Mina Salman Industrial Area – Block 343, Road 42, Flat 3, Building 108. P. O. Box. 707, FAX: +973 17 728 227, Tel No: +973 17 727 559, email: info@alkhajagroup.com.

ICT & KM directorate has four types of backup as follows:

3.20.1 ASU systems data backup:

Systems data backup is an automated process, which is performed by the backup software daily at 3:00 am (Bahrain Standard Time).
The backup done for all ASU management information systems:

- Students Information System (SIS).
- Digital Campus (DC).
- Peachtree accounting system.

- Learning Management System (LMS).

3.20.2 ASU Servers and Network configuration backup:

ASU server backup is an automated process which is performed by the backup software monthly every 4th Friday of the month at 1:00 am (Bahrain Standard Time).

3.20.3 ASU Network configuration backup:

The network configuration backup is manual backup for the ASU Network routers and switches performed by the ASU network administrator monthly and also in case configuration change or devices software update. ASU administrator will then verify that the process was successful and will save a copy on a labelled tape and DVD and store them in a safe (vault) in the ICT & KM directorate.

3.21 ASU DR and Fail-over Server:

ASU has a high specification server located on Amwaj Island (the distance is around 25 Km), in an agreement with the Nue-Tel Communication Company. This server is the disaster recovery, fail-over server and contains a full copy of the ASU database and is configured to take the load in case of any failure of the main database server and is integral in the disaster recovery plan to ensure ASU contiguity.

3.22 Physical access

The University had restricted access to sensitive areas that contain confidential information or student records and access is monitored through CCTV cameras and a fingerprint monitoring system with unique identification codes for all users.

a. Access to all administrative and staff areas is controlled by a fingerprint device and only authorised people can gain access to that area by saving their fingerprint in the fingerprint device.
b. ICT cover inside and outside ASU Campus with Video Monitoring through CCTV system 24/7.

The University has installed CCTV cameras across the University to monitor daily activities. The university system ensures round the clock coverage for areas that contain sensitive or confidential information.

3.23 Access to ASU systems and the internet

The access to ASU systems and the internet resources at the University is controlled through individual domain user accounts and passwords. It is mandatory for each user of the University's internet resources to read this policy and sign an agreement on internet use before receiving the access details & password to the university network.
ICT&KM is designated to assign authority / privileges for accessing the internet. The department director is the authorized party to approve requests for critical additional privileges for any staff in their department. A written request must be made to ICT&KM.

I. Access to ASU systems and the internet resources at the University is controlled through individual domain user accounts and passwords. It is mandatory for each user of the University's internet resources to read this policy and sign an agreement on internet use before receiving the access details & password to the university network.
II. ICT & KM is designated to assign authority / privileges for accessing the internet. The department director is the authorized party to approve requests for critical additional privileges for any staff in their department. A written request must be made to ICT & KM.

3.24 ASU Network

ASU have a v-center that controls the entire network using visualization and vlan switching, vlans provide enhanced network security, a vlan network environment, with multiple broadcast domains, and the ASU network administrator has control over each port and user. A malicious user can no longer just plug their workstation into any switch port and sniff the network traffic using a packet sniffer.

3.25 ASU Firewall

ICT & KM use a Fortigate 110c firewall device to protect the ASU Network to protect our systems from threats can enter ASU network from common applications like email and web browsers as well as the latest social networking tools.

I. Provide the visibility needed to detect hidden threats within legitimate content, even from trusted sources and authorized applications.
II. Provide web content filtering and URL filtering.
III. Provide network transmission monitoring and control.

3.26 Antivirus

ICT&KM has an agreement with ESET to use ESET Nod32 antivirus with the following features:

I. Proactive Protection
II. Secure and Control Removable Media
III. High Performance Scanning.
IV. Encrypted Communication Scanning
V. Free Technical Support
VI. Advanced Remote Management Tools
VII. Light on Your System

3.27 ICT information Auditing process

ICT & KM is responsible for monitoring the information in all ASU systems to ensure only authorized changes fare made to student marks and finance records. This process is done through:

3.27.1 Procedure 1

This is developed by taking a full backup of all information on SIS (Marks and Fees) for whole years at once, then creating another backup after the publication of marks for each semester. The information monitoring is done by comparing the full information in the different backups and cross matching them to identify any mismatching information.

3.27.2 Procedure 2

A full backup is taken after the lecturer confirms the marks and transfers them to the college dean. And another full backup is taken after the Admission and Registration Deanship has published the marks, a comparison is done between the two backups to check the marks that have been entered by the lecturer matches the published ones or not.

In case of mismatched and/or matched information a report is created and submitted directly to the Vice-President of Administration, Finance and Community Engagement, to be forwarded to the Vice-President of Academic Affairs and Development then the Admission and Registration Deanship to determine the reasons for any discrepancies or why changes were made.

3.28 ICT Service and Help Desk

3.28.1 Type of Services

ICT & KM Help Desk services constitute one of the largest services provided to University staff and students. Services provided could relate to a range of items including user accounts, email, network, or PC support etc. These services are divided into:

I. Assistance Services: routine ongoing support. This type of service is characterized by known requirements, solutions, costs, and risks.

II. Enhancement Services: modification and/or addition to an existing service (i.e. new report or even new application).

3.28.2 Incident solving

The ICT & KM procedure to handle incidents involves following one or more of the three levels of resolution. As shown in figure 4.1.

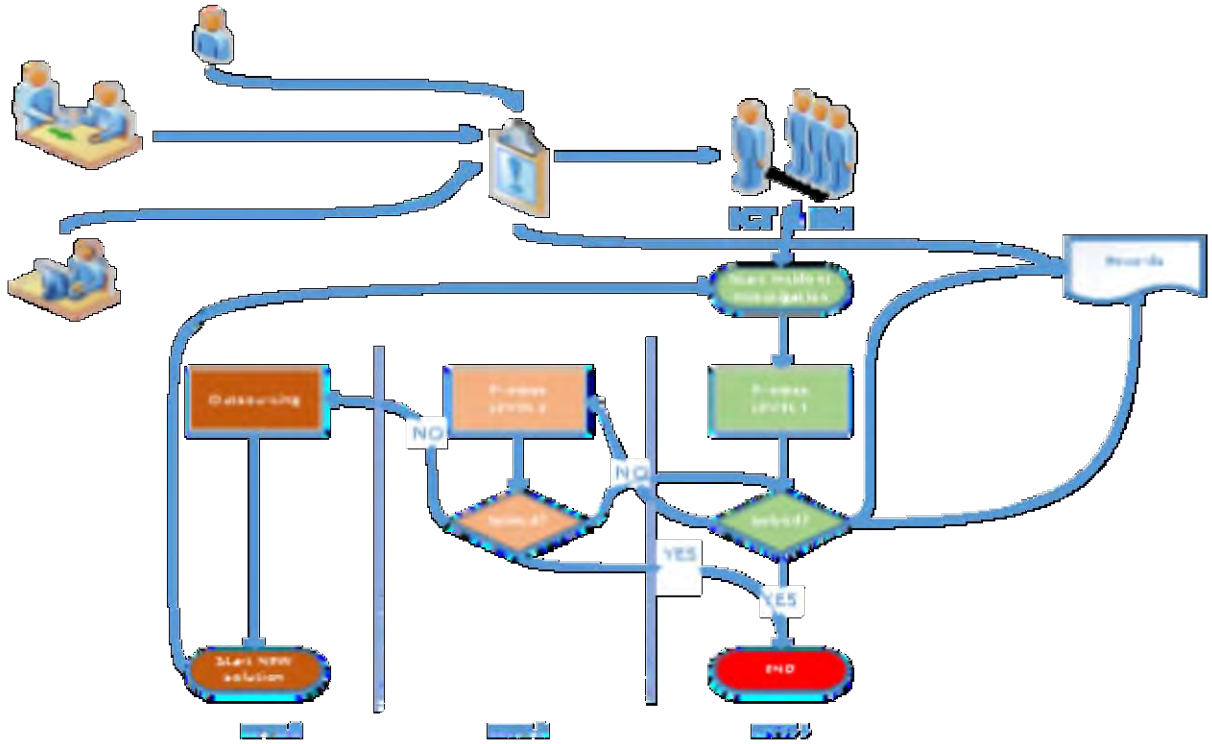


Figure 4. 1 Incident Management

4.10.2.1 1st Level Support

- The responsibility of 1st Level Support is to register and classify received Incidents and to undertake measures to restore a failed ICT service as quickly as possible.
- If no ad-hoc solution can be achieved, 1st Level Support will transfer the Incident to expert technical support groups (2nd Level Support).
- 1st Level Support also processes Service Requests and keeps users informed about their Incidents' status at agreed intervals.

4.10.2.2 2nd Level Support

- 2nd Level Support takes over Incidents which cannot be resolved immediately with the means of 1st Level Support.
- If necessary, it will request external support, e.g. from software or hardware manufacturers.
- The aim is to restore a failed ICT Service as quickly as possible.
- If no solution can be found, the 2nd Level Support passes on the Incident to Problem Management.

4.10.2.3 3rd Level Support

- 3rd Level Support is typically handled hardware or software manufacturers (third-party suppliers).
- Its services are requested by 2nd Level Support if required for solving an Incident.
- The aim is to restore a failed ICT Service as quickly as possible.

3.28.3 Service Procedure

The ICT service desk at the University handles all requests to ensure that standards of services are met. All service requests shall be either sent by email or by completing and submitting a form to the ICT service desk. The ICT service desk shall:

I. Record the requests.
II. Identify the type of service requested (Priority) in order to take appropriate action.
III. Maintain reports of services requested and the status of delivering the services.
IV. Validate solution/service with the one who requested the service to make certain their needs have been met. Based on the feedback, either close the request or take further action.

3.29 Providing ICT help and support to faculty members, students, and staff

ICT will provide help and support to ASU faculty members and staff in four different ways:

I. Normal Request: Either an online request on the Issue Tracker system (MS SharePoint) or email to IT which is responded to on the same day, if possible, but make take up to 3 working days.
II. Urgent Request: A telephone request for urgent matters and is acted upon immediately.
III. Scheduled technical visit: There is monthly technical visit to all ASU staff to check and maintain hardware and software if needed.
IV. Online support using the MS Lync application to remotely access and control the ASU user PC under his/her permission to solve the technical problems remotely.

3.30 Applications Development

The ICT & KM's Applications Development Department is responsible about all ASU information systems; the in-house developing and outsource systems. ICT & KM start to analyze the needs of any new system after receiving a request or suggestion from any department, then decide the priority of the required system to schedule the project tasks.

I. Implementing ASU applications, which are used to manage and enhance the faculty, staff and students records and services.
II. Find the solution to any new request of software or application and provide the University with the suitable solution by either purchasing it or implementing it internally.

ICT & KM follow an eight-step process to develop any new system, the SLDC, as shown in Figure 4.2. The eight-step process contains a procedural checklist and the systematic progression required to evolve an ICT system from conception to disposition.

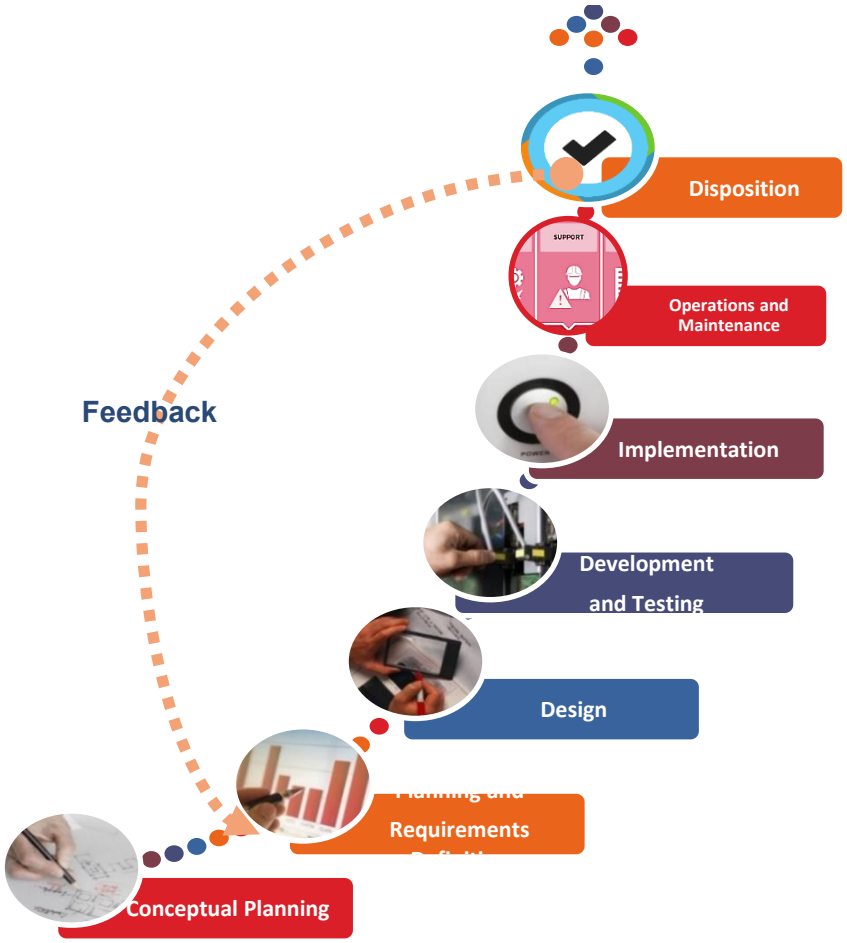


Figure 4. 2 Systems Development Life Cycle (SDLC)

The following descriptions briefly explain each of the eight steps of the SDLC:

1- **Conceptual Planning**:

This step is the first step of any system's life cycle. It is during this phase that a need to acquire or significantly enhance a system is identified, its feasibility and costs are assessed, and the risks and various project-planning approaches are defined. Roles and responsibilities for the Asset Manager, Sponsor's Representative, and other parties in SDLC policy are designated during this stage and updated throughout the system's life cycle.

2- **Planning and Requirements Definition**.

This step begins after the project has been defined and appropriate resources have been committed. The first portion of this phase involves collecting, defining and validating functional, support and training requirements. The second part is developing initial life cycle management

plans, including project planning, project management, support, operations, and training management.

3- **Design.**

During this step, functional, support and training requirements are translated into preliminary and detailed designs. Decisions are made to address how the system will meet functional requirements. A preliminary system design, emphasizing the functional features of the system, is produced as a high-level guide. Then a final (detailed) system design is produced that expands the design by specifying all the technical detail needed to develop the system.

4- **Development and Testing**:

During this step, systems are developed or acquired based on detailed design specifications. The system is validated through a sequence of unit, integration, performance, system, and acceptance testing. The objective is to ensure that the system functions as expected and that sponsor's requirements are satisfied. All system components, communications, applications, procedures, and associated documentation are developed/acquired, tested, and integrated. This phase requires strong end user participation in order to verify thorough testing of all requirements and to meet all business needs.

5- **Implementation:**

During this step, the new or enhanced system is installed in the production environment, users are trained, data is converted (as needed), the system is turned over to the sponsor, and business processes are evaluated. This phase includes efforts required to implement, resolve system problems identified during the implementation process, and plan for sustainment.

6- **Operations and Maintenance**:

The system becomes operational during this step. The emphasis during this step is to ensure that sponsor needs continue to be met and that the system continues to perform according to specifications. Routine hardware and software maintenance and upgrades are performed to ensure effective system operations. User training continues during this phase, as needed, to acquaint new users to the system or to introduce new features to current users. Additional user support is provided, as an ongoing activity, to help resolve reported problems.

7- **Disposition**:

This step represents the end of the system's life cycle. It provides for the systematic termination of a system to ensure that vital information is preserved for potential future access and/or reactivation. The system, when placed in the Disposition Phase, has been declared surplus and/or obsolete and has been scheduled for shutdown. The emphasis of this step is to ensure that the system (e.g., equipment, parts, software, data, procedures, and documentation) is packaged and disposed of in accordance with appropriate regulations and requirements.

8- Feedback:

Any new system required the end user feedback. Therefore, ICT & KM are always available to have the feedback and maintain the system. This feedback is used in an organized manner to improve the systems.

The duration to develop any new system is depended on the complexity. So, each step in the above SDLC is charged regarding the business requirements.

3.31 Help and support for ASU Students

I. ICT & KM handle all hardware and software support to ASU students who can get help and support directly from the technical support office.
II. ICT help and support scope cover only licensed educational software and applications and some general purpose utilities.
III. ICT & KM provide the Computer Science (CS) and Management information System (MIS) students with the latest programs and applications to use while studying practical courses. All the programs and applications are included in the MS IT Academic agreement (ASU Dream spark standard account). Each CS and MIS student has an MS account to download his needs of MS programs free.

3.32 Provide computing facilities to support specialist research and teaching.

ICT provides a variety of facilities for research and teaching that help instructors and students as well.

I. Each faculty member has credentials to access the learning management system (Moodle) which is an E-learning resource for ASU faculty members. Moodle is used to upload and download courses, teaching materials, communication, discussion and online exams.
II. The ICT team will handle the training for ASU faculty members to use Moodle.
III. Each faculty member and student has credentials to access the E-Lib System which guarantees him the access to the latest references and textbooks and journals and research in Arab and international libraries.
IV. Each faculty member has a blog on MS Office 365 (Faculty Profile) which can be used to upload all his/her information (i.e. publications, research, papers, books …etc.).
V. Each ASU member has a membership and access with MS YAMMER social network for knowledge management and sharing.

3.33 Provision for IT related training

I. Training conducted by ICT to ASU Faculty members and staff as per need in different areas of IT, especially the software and application that facilitate education and learning and improve staff skills.
II. ICT provide training do ASU staff to interact with ASU systems efficiently.
III. ICT prepare user guides for the systems and applications used by ASU staff.
IV. ICT distribute how to use guides and tips for ASU Faculty members and staff to help them to use new software applications by E-mail System.

3.34 Technology enabled Teaching

I. ICT keep ASU up to date with the latest technologies to enhance educational methods and learning as follow:
II. In each classroom, there is one PC in the instructor table connected to the internet and connected to one of the most dedicated interactive projector, which enable interaction with the board.
III. Each Faculty Member has projector remote control and inteli-pen.
IV. Each Faculty Member has PC and laptop and printer in his office.
V. Each Faculty Member has account in Microsoft portal, which provides him access to latest educational services i.e. Office 365, Exchange, Lync, SharePoint and sky drive for documents and file access, sharing and tracking.
VI. Online support by using the Lync application.

3.35 Purchasing (procurement) of ICT equipment.

The process of acquiring hardware shall be as follows:

3.35.1 Hardware Selection Process

Prior to raising a request for purchase of any computer hardware or accessory, the faculty or staff member should consult with the following:

I. The ICT & KM director to determine what items may or may not be compatible with the system and what items may be available in bulk purchase through the University.
II. Approach their respective Dean / Director of the College / Departmental for an approval, who shall determine whether multiple purchases of such hardware items may be warranted for department members.

3.35.2 Hardware Procurement Process

I. The ICT & KM shall initiate the purchase of hardware by submitting a request to the Purchasing department, which must elicit quotes from a minimum of 3 vendors.
II. The quotes shall be compared on the basis of cost and features of the equipment. Additional benefits, if any, provided by any vendor, such as after sales support, maintenance support etc. shall be taken into account while short listing the final vendor. The final decision to purchase is done by both ICT & KM and the Purchasing department.

3.36 Maintain, monitor and continuously update the ICT labs across the University

I. The ICT Technical Support Office has scheduled maintenance and software update for ICT labs across the university monthly and schedule checks and reviews of ICT labs before midterm exams and final exams to ensure the practical exams will be held with no errors or difficulties.
II. Each ASU lab is connected to the domain (active directory), which helps the ICT & KM to monitor the lab's PCs and preparing the required reports to the university about the lab. And library PC's usage (i.e. number of students usage, number of total hours of usage, and login file).

3.37 Reporting

The ICT & KM provide the Vice President for Admin, Finance & Community Engagement With:

I. All the official letters that are send from the ICT & KM to in/out the university.
II. Monthly report consist of all ICT & KM activities that are done that month.
III. Each ICT & KM meeting minutes.
IV. The yearly strategic plan of the ICT & KM.

3.38 Survey and Questionnaires

ICT & KM is responsible for:

Collection of data and information from all ASU systems (i.e. students faculty and staff surveys), and other information provided by ASU systems to present and analyse this information then provide it to the particular departments (i.e. VP of admin. and VP of academic) as reports and presented information.

The Application management department in the directorate developed a new survey system to handle all the ASU surveys and manage survey handling with an integrated system.

CHAPTER 5: ICT & KM STRUCTURE

ICT & KM consist of the two departments and one office, integrated and coordinated with each other in order to achieve the objectives of the directorate and each functions and services ASU provide, as it is described as follows:

5.1 Knowledge Management Department

This department is responsible for the development of knowledge management and the effective transfer of knowledge in order to facilitate the process of knowledge production, generation and improve the decision-making power, thus contributing to raising the efficiency of operations, and improving productivity by providing optimal solutions to problems, and the integration of human resource capacities creative with knowledge on one side and information technology requirements of the other. The main tasks and services of the KM team are to:

- Collect, organize and analyse information that is obtained from internal and external sources for the benefit of the parties concerned and improve the decision making, and strengthen academic services.
- Provide accurate information, accurately and timely assist one another in the decision making, achieve the objective evaluation, effective management and strategic planning in the educational system.
- Develop policies and procedures for the collection, analysis, demonstration and exchange of data and analysis in educational systems.
- Interact positively with requests for information and questionnaires foreign university administration believes it is a valuable and useful for the educational system.
- Provide advice and analytical services that help transform data into practical information that can be implemented and valuable.
- Prepare an annual report to include the activities and achievements of the centre. Develop a plan for research and development.
- Identify the training needs of individuals.
- Support TQM methods.
- Establish a culture of knowledge management in order to facilitate the process of knowledge production, generation and improve the decision-making power, and strengthen academic services, and unleash the intellectual and mental abilities of

individuals at all levels, thus contributing to raising the efficiency of operations, and improve productivity by providing optimal solutions to problems

- Support strategic planning processes, which achieve high capacity of the institution to monitor the knowledge from different sources, processing and analysis, they are a range of activities, processes and practices that aim to produce knowledge, and invest the balance of intellectual and knowledge through scientific research.
- Building a high human expertise in the fields of information technology and knowledge management of the sons of the university who are unable to achieve the above objectives.
- Update and modify the content of the university's website periodically with the different versions and university news.
- Allocate e-learning, provide training sessions, development of all the beneficiaries and technical support.
- Provide the e-mail service to academic and university staff and the issuance of special accounts such service.

5.2 Application Management Department

This Department is responsible for the design, construction, development, maintenance and protection of the database and computer information systems by the University; the most important of those are the Deanship of Admission and Registration, the Department of Human Recourse and the Department of Finance and Accounting and Procurement Service, and the tasks and key services provided by:

- Design and development of applications for various university departments as well as to enable them to manage the content of any of these applications through deletions, and additions and modification.
- Analysis of the computer-based information systems used and make the necessary adjustments in accordance to the changing needs of users in different Departments in the university and the educational system.
- Provide security and protection to the database and computer information systems at the university.
- Grant or withhold permission to users of computer information systems at the university commensurate with the nature of their work and their powers.
- Staff training on the use of information systems that have been developed.
- Issuance of special accounts using information systems for each beneficiary (academics, staff and students).

- Develop plans for the development of computer systems and keep pace with technological development in line with the strategy of the university.

5.3 Technical Support Office

This Office is responsible for providing substantive and technical support and maintenance of computer hardware and accessories used in the university and make all the necessary work to sustain their work and use. This Office also is responsible for the design, maintenance and protection of information and communication network linking the University computers which facilitates and makes it easier to connect with each other in order to share files and information. The main tasks and services provided by this Office:

- Identify technical specifications for computers and accessories to be purchased for use in colleges, departments and various university departments.
- Preview of computers and accessories used in the university on a regular basis to determine the suitability for use and work.
- Repair or replace devices according to the requirement and user needs.
- Preparation of technical reports on a regular basis.
- Installation of processing and preparation of computers and accessories that are newly purchased and configured to work, both in terms of the use of the software or protection and so on for all the employees of the university.
- Provide technical support needs and any events held inside or outside the campus and participate in colleges, deanships and various university departments.
- Provide Internet, telecommunications and Wi-Fi services for staff and students of the university and monitor sustainability of these service and not misused.
- Provide security and protection of electronic information network, servers, and communications at the university of viruses and intrusion attempts or vandalism.
- Manage network switches, devices and servers in the data centre and provide the required maintenance.
- Provide full support to achieve the ASU mission and the academic functions to enhance the educational process and scientific research at the university to provide high quality services and provide flexible and innovative solutions to information technology.
- Provide advices and studies to credibility and professionalism in the field of information technology to all actors in the university.
- Develop and implement special controls and policies using information Technology University in a professional and ethical and seek to educate all members of the educational system to reach the conscious user environment for information technology in terms of the availability of services, solutions, and technologies.

- Construct and apply of leading practices in information technology, to ensure the safety and security of information, reliability, availability, and quality.
- Try to automate the education and administrative in the educational system.
- Building an effective administrative entity for information technology, regulates the structure, operations and services, by adopting the best frameworks.
- Develop effective plans and budgets for information technology, for cost estimation and support decision making.
- Prepare reports about the indicators for Information Technology performance in addition to an annual report lists the activities and achievements of the department.

The ICT & KM Directorate of independent scientific follow the Vice President for Administrative Affairs and of Finance, as shown in Figure 1.

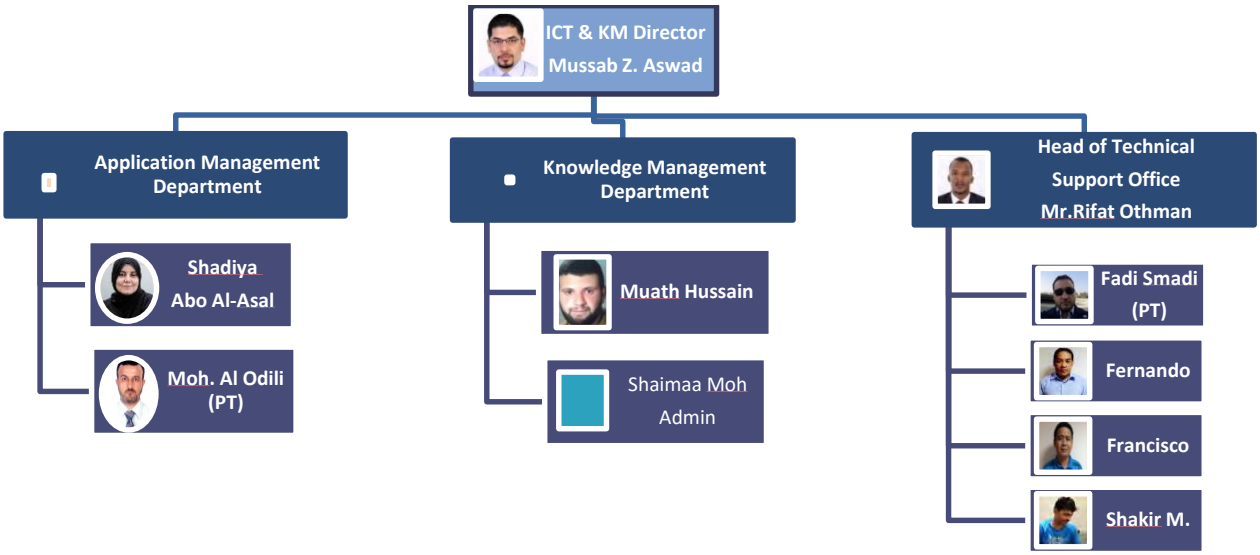


Figure 1: The ICT & KM Directorate Structure

5.4 ICT & KM team job title and description

Each member in the ICT & KM should know his role and job, below is a job description for each one in ICT & KM.

5.4.1 Knowledge Management Department

Muath Hussain: Web Developer (Full Time)

- Office 365 administrator / Exchange Admin.
- Web designer PHP/XML/HTML/ASP.NET.
- Moodle system Management (integration must know).
- Web & Application Server Maintenance, Knowledge WordPress themes/ Plugins & customization.
- Apache 5.4 onwards
- Domain/Subdomain Creation & redirection to particular IP address & CNAME/MX/A records entry & updates, Web Host Manager, FTP to any data server (file transfer from local to server using FTP).
- Database Maintenance & Migration (Digital campus system with HRS).

Shaima Dauod: Admin (Part Time)

- Support for our ICT & KM Senior programmers and web developers (Documentation, Data entry, used guide design).
- Follow-up with all ASU colleges and directorates to collect the needed information.
- Responsibilities: meeting mints, In/Out reference papers, user guides and communication.
- Help in end user training and support.

5.4.2 Application Management Department

Shadia Abu Al-Asal: Senior Programmer (Full Time)

- Systems analysis: Using Oracle Designer 10g (Entity Relationship Diagram, function hierarchy Diagram ,Head start 6.5 Utility
- Systems Development: using Oracle Designer 10g (server model, module application), Form Builder 10g, Report Builder 10g, Oracle Apex 4.2,PL/SQL

- Database Administration: Maintain Oracle 11g database server, Maintain application server, Maintain Web server for Apex applications.

Mohammed Ali Alodili: Senior Programmer (Part Time)

- Systems analysis: Using Oracle Designer 10g (Entity Relationship diagram, function hierarchy Diagram, Head start 6.5 Utility.
- Systems Development: using Oracle Designer 10g.
- Database Administration: Maintain Oracle 11g database server, Maintain application server, Maintain Web server for Apex applications.

More for Advanced Solutions Company: Outsource Programmer

- Systems Development: Using Oracle Designer 10g (server model) Apex 4.2, PL/SQL

5.4.3 Technical Support Office

Rifat Hasan: Network Administrator (Full Time)

- Responsible for designing, organizing, modifying, installing, and supporting a company's computer systems. Designs and installs LANs, WANs, Internet and intranet systems, and network segments.
- Install and support LANs, WANs, network segments, Internet, and intranet systems.
- Install and maintain network hardware and software.
- Analyze and isolate issues.
- Monitor networks to ensure security and availability to specific users.
- Evaluate and modify system's performance.
- Identify user needs.
- Determine network and system requirements.
- Maintain integrity of the network, server deployment, and security.
- Ensure network connectivity throughout a company's LAN/WAN infrastructure is on par with technical considerations.
- Design and deploy networks.
- Perform network address assignment.

- Assign routing protocols and routing table configuration.
- Assign configuration of authentication and authorization of directory services.
- Maintain network facilities in individual machines, such as drivers and settings of personal computers as well as printers.
- Maintain network servers such as file servers, VPNgateways, intrusion detection systems.
- Administer servers, desktop computers, printers, routers, switches, firewalls, phones, personal digital assistants, smartphones, software deployment, security updates and patches.
- Take the backup for all servers, systems data and network devices configuration.

Fadi Smadi: Network Administrator (Part Time)

- Install and support LANs, WANs, network segments, Internet, and intranet systems.
- Install and maintain network hardware and software.
- Ensure network connectivity throughout the University's LAN/WAN infrastructure is on par with technical considerations.
- Design and deploy networks.
- Perform network address assignment.
- ICT help and support, desktop computers, printers, phones, personal digital assistants, smartphones, software deployment, security updates and patches.

Fernando: ICT Technician

- ICT help and support, desktop computers, printers, phones, personal digital assistants, smartphones, software deployment, security updates and patches.
- Computer Laboratory, library, staff maintenance, system upgrading, software insulation.
- Monthly visit for maintenance.
- ICT companies contact for maintenance and services.
- ICT & KM inventory system administration.

Frances: ICT Technician

- ICT help and support, desktop computers, printers, phones, personal digital assistants, smartphones, software deployment, security updates and patches.
- Computer laboratory, library, staff maintenance, system upgrading, software insulation.

- Monthly visit for maintenance.

Shakir: ICT Technician:

- Install and support LANs, WANs, network segments, Internet, and intranet systems.
- Install and maintain network hardware routers, switches, firewalls, phones, personal digital assistants, and smartphones.
- CCTV installation and maintenance.
- Projector (data show) installing and maintenance.