جامعة الشرقية
A'SHARQIYAH UNIVERSITY

Information Technology Services Manual

2022/23

AD0002

Approvals

This document has been approved by

Name	Signature	Date reviewed
1. University Academic Board		22/May/2022
2. Academic Committee		8/June/2022
3. Board of Trustees		23/June/2022
4. Board of Directors		18/June/2023

Implementation and Responsibility

Document owner	Contact person	Date of Implementation
IT Services Department	Director of IT services	**18/June/2023**

General provisions

- Any form of non-compliance with this policy/procedure makes those responsible open to University disciplinary measures.

- Any exception from this policy/procedure upon application shall have no effect against the University or others unless it has been approved by the Vice Chancellor or the Board of Directors and/or the Board of Trustees as the case may be.

Revision history

Version	Author/ Reviewer	Revision(s) made	Date
1.0	Director of IT services	The IT policy was approved in 2017. In the past 5 years lot of changes happened in implemented Technology itself and as ASU is growing, it is important to review this Policy to align with ASU vision.	**4 /April /2022**
2.0	Director of IT services	The following are the ones which has been added in IT manual compared to old ones: b) Separate policy for email has been created. Previously this was distributed under different policy points. c) IT Asset policy d) IT Asset replacement policy e) Helpdesk Support Policy. f) BYOD (Bring Your Own Device) Policy	**4 /April /2022**

3.0	Director of IT services	The following has been removed from IT Manual compared to old ones: a) Roles and responsibilities b) IT Planning and Organization c) Change Management d) Laptop Policy	**4 /April /2022**

Contents

Contents

1 Introduction

1.1 Purpose

The purpose of the Information Technology policy and procedure Manual is to:

- Document the Information Technology policies and procedures of A'Sharqiyah University ('ASU'/'the University');
- Ensure that IT policies and procedures are applied consistently; and
- Maintain procedure consistency in the face of employee changes.

The manual is fulfilling all Commitments of ASU in the Strategic Plan that's related to IT Services Dept.

1.2 Scope

Significant areas in which policies and procedures have been developed include:

- Acceptable use of Information Technology Resources
- Network Policy
- Internet Policy
- Access Control Policy.
- Email Account Policy
- Physical and Environmental Security
- Backup and Restoration
- Incident Management;
- Educate and train users;
- IT Acquisition and Implementation Management.
- Business Continuity Management
- Bulk SMS
- IT Systems / Application Ownership; and
- IT Asset Policy
- IT Asset (Hardware/ Software) Replacement Policy
- Helpdesk support Policy
- BYOD (Bring Your Own Device) Policy

1.3 Structure of the manual

1 This manual consists of various policies and procedures that provide comprehensive information on the various activities that are required to be carried out by the IT department. The policy is divided into chapters which are further subdivided into sections wherever applicable.

2 Relevant forms to be used are provided at the end of the manual.

1.4 Distribution

The controller of this manual will be the Director of Information Technology Services. The Director of Information Technology Services should be contacted with any questions or requests for changes to the manual's contents.

The manual's contents are private and intended for internal University use only. The Manual Distribution Control Record regulates the distribution of the manual (Form 1.1).

Except in the event of auditors and government authorities, this manual should always be maintained in safe custody and should not be copied or exposed to third parties (those who are not employed by the University) without the express written approval of the manual's controller. Copies of this manual, in whole or in part, shall be distributed to all staff.

1.5 Revision

1. Revision of this manual shall be the responsibility of the Information Technology Services department.

- Revision of this manual is the principal way of implementing and communicating changes in the Information Technology policies and procedures that may arise in response to the changing needs and requirements of the University. Such revisions allow for greater flexibility in ensuring that the manual remains current at all times.

- Requests for revisions to this manual may come from a variety of department heads. If any other staff members wish to make changes to this manual, the request must be routed through the respective department heads. Manual Revision Proposal includes a request for manual revision (Form No 1.2).

- The proposed changes to this manual must be reviewed by the controller. If the revision proposal is not approved, notification will be sent along with the reason.

- If the revision proposal is approved, the controller must ensure that the relevant pages of the manual are revised. The controller will then distribute the revised pages to all manual custodians, identifying the attachments and the effective date for the revision's implementation. This manual includes a Manual Revision Control Sheet (Form1.3).

- Revision shall be conducted every three years.

1.6 Forms

Description	Form No.
Manual Distribution Control Record	1.1
Manual Revision Proposal	1.2
Manual Revision Control Sheet	1.3

1.7 Glossary of terms & abbreviations

Term / Abbreviation	Definition
ASU / the University	A'Sharqiyah University
VC	Vice Chancellor
DVC's	DVCRIS / DVCAAR
DVCRIS	Deputy of Vice Chancellor for resource and Institutional Support
DVCAAR	Deputy of Vice Chancellor for Academic Affairs and Research
DOD	Director of Department
IT Dept	Information Technology Services Department
Users	Staffs, faculties (Full time, part time, visitors) , students, Trainees, guest (Contractors, third party vendors or anyone who was given permission to access University resources (Research council or Library access)
IT Resources	Desktop, Laptop, Printers, Projectors, Switches, Email, Internet, Network, Photocopiers, Access Points, CCTV system, PA system, Telephone system, SMS system, Call centers, Software's and applications, Mobiles, Tabs, Digital Signage, Access Door etc

2 Acceptable Use of Information Technology Resources

2.1 Purpose:

All information resources are considered as assets and their security and integrity is essential to ASU. It is ASU's responsibility to manage its Information Technology resources and to support its activities. While ASU's employees are free to use these resources, it is essential to safeguard the sensitive information, equipment and network in order to ensure its reliability and robustness at all times. This policy outlines the appropriate use of information technology resources, as well as the rights and obligations of the many parties engaged in their usage, as well as the penalties for infractions.

2.2 Scope:

Applies to all users which include but not limited to staffs, faculties (Full time, part time, visitors), students, Trainees, guest (Contractors, third party vendors or anyone who was given permission to access University resources (Research council or Library access) within the A'Sharqiyah University premises and offices.

2.3 Objective:

The objective of this policy is to ensure that:

- The integrity of data and systems at ASU is Protected
- The use of IT services is in line with ASU policies.
- All the data access in ASU is controlled to meet legal obligations.

2.4 Policy

- All users who use ASU's computing and network resources to interact and support their daily operations activities must adhere to the policy. The computing resources include all the IT resources that are owned by ASU and those other resources that have been authorized to be connected to ASU's facilities. ASU users are expected to respect and uphold ASU's reputation when dealing with parties outside ASU in all electronic dealings. ASU users are expected to familiarize themselves with ASU's policies and procedures that have been set in place and are expected to comply with the outlined policies and procedures.

- All ASU users must respect the rights of other members of ASU at all times. ASU users must refrain from carrying out activities that may interfere or impair the productivity of other members of ASU. ASU IT resources must never be used for non-university related purposes.

- Credit card details, fixed log-in passwords, and other security characteristics that can be exploited to gain access to goods or services should never be communicated over the internet in readable form.

- For the protection of security parameters, the SSL encryption procedure is a suitable Internet encryption standard.

- ASU users must prohibit sharing their login passwords with others in order to assure user accountability.

- ASU users are prohibited from sharing or in any way revealing their password to others.

- ASU users are expected to comply with the password standards outlined in the Information Security Policy.

- ASU users must never use unlicensed software and must at all times, employ licensed software.

- Downloading, distributing and printing of copyrighted materials by using ASU resources shall be prohibited at all times.

- All software employed at ASU must be licensed/ open source.

- Users are prohibited from installing software on any machine without obtaining the required licenses and approval from IT department. In case if users have local administrator right where they can install any software, they should also inform IT Department and get prior approval before installing any software's and application.

- Downloaded software should be tested on a non-production machine that has recently been backed up.

- Only authorized storage media must be used in order to backup ASU internal data.

- User is responsible for carrying out regular backups in order to retain the data for future use.

- Any deliberate attempt to overload the ASU system is not allowed.

- ASU users should responsibly use their user account in a way such that it prevents unauthorized user access.

- ASU users must take appropriate safeguards in order to prevent physical theft of ASU IT resources.

- Intentional damage or destruction to ASU equipment is prohibited and is grounds for disciplinary action to be taken by ASU under HR regulations.

- Use of cameras or mobile phones in secured areas such as server rooms is prohibited

- Authentication mechanisms shall be enforced on all directories and sub directories which are shared.

3 Network Policy

3.1 Purpose:

Defines the connectivity and the access of all network devices (Wired/Wireless) in ASU.

3.2 Scope:

Applies to all users of ASU.

3.3 Objective:

To ensure the security of ASU network devices and proper usage of network by ASU users.

3.4 Policy

- Periodic vulnerability assessment will be conducted in order to minimize the threats posing ASU networks.
- All information assets will be in place to ensure that all systems have the most recent security updates installed.
- Internal and external networks will be separated, and all connections between them will be monitored, managed, and secured using firewalls and other security mechanisms.
- All network devices are physically secured and placed within locked rooms in order to prevent unauthorized access.
- All ASU users must be identified, authenticated and authorized before access to any networked service is granted.
- All ASU users are accountable for their actions related to network security violations.
- Every outbound and inbound connection to and from ASU undergoes the authorization process.
- Outbound connections from ASU will be routed through a firewall and Web filter devices.
- All outbound connections from ASU will be logged and monitored.
- The session is only re-established after the user has provided the correct password or identification.

- The use of networks is limited to ASU operations only. ASU network users must exercise judgment over the information they access.
- Only authorized ASU users will be able to access the wireless service.
- ASU users will be logged in using their user ID. The IT department will issue guests a Guest ID for authentication.
- ASU Users who seek wireless service must obtain a device that complies with the current implementation requirements.
- The IT department maintains the right to remove wireless service authorization for any individual ID, Guest ID, or equipment that is interfering with the wireless service's performance. The authorization to use the wireless service will be revoked if the Information Technology Resources policy is violated.
- ASU users are not allowed to install personal wireless networking equipment's in University network without written consent from IT Department.
- Violation of network security is prohibited, and appropriate disciplinary action may be taken in case of unauthorized access.
- Network sniffing or packet spoofing is not allowed as it results in the disruption of network services at ASU.
- ASU users are not allowed to install/use any VPN software's which bypass the ASU network connectivity/Firewall device.
- To prevent unauthorized personnel from accessing private information, all inbound real-time Internet connections to ASU internal networks are routed through a firewall.
- Firewalls include Intrusion Detection Systems (IDS). These will be configured accordingly keeping in mind the operational needs of ASU.
- Firewalls will be configured accordingly keeping in mind the operational needs of ASU.

3.5 Procedures:

- All data sent over the network will be encrypted prior transmission.
- Effective security controls will be enforced upon the network in order to prevent unauthorized access.

- ASU users requiring remote access to his office desktops/servers provided by ASU will follow the underlying procedure:
- This form No 1.5 will provide justification and need for such access.
- The IT department will evaluate the request submitted by the user after the approval from his/her line manager.
- In cases where the request has been denied, the form will be sent back to the user submitting the request providing justification for the grounds of denial.
- If approved, the IT department will grant the user remote network access.
- A secure ID will be assigned to each user which will be matched with the user's network ID.
- This secure ID will be transmitted in a secure and controlled manner.
- The host operating system will validate each user prior granting remote access.
- Network access will be revoked once the duration for such access has been completed.
- This access request will be logged for future reference purposes.

4 Internet Policy:

4.1 Purpose:

Defines how the internet is provided for ASU users and its usage and to prevent loss, modification or misuse of information exchanged on the Internet

4.2 Scope:

All ASU users

4.3 Objective:

To allow ASU users to have secure and reliable internet connectivity in ASU campus

4.4 Policy:

- ASU users are expected to use to the Internet for valid University operations purposes only.
- Users should be aware that their Internet usage may be monitored from time to time.
- Users are prohibited from posting any material that is in violation of the copyright law.
- All information/files downloaded from the Internet should be scanned for viruses prior to use.
- Internet usage is constantly logged and monitored in order to determine usage pattern and detect any inappropriate usage.
- Using background "push" Internet technology to update software or information on ASU computers is banned unless the vendor's system has been reviewed and approved by the Information Technology department.
- Users should not save fixed passwords in their web browsers or email clients since anyone with physical access to their workstations could use their identities to access the Internet and read and send information.

- All Internet activity passes through ASU's firewall/ web filter so that access controls and related security mechanisms can be applied.

- ASU users may not establish Internet or other external network connections that could provide external users access to ASU systems and information without prior consent from the IT Department.

- ASU Internet users are prohibited from using new or existing Internet connections to establish new business channels without prior approval of the senior management and DOD.

- ASU users are not permitted to use the Internet or other internal information systems in a way that reduces the productivity of other employees.

- ASU's firewalls frequently prevent users from accessing websites outside of the university. (If you don't restrict which services hosts in your internal networks have access to, malware will enter your network and exfiltrate data to a location controlled by an attacker.) Data exfiltration may sometimes be inadvertent (for example, an insider may mistakenly attach sensitive information to an email message in order to upload it to a document sharing site).

- ASU users who find they've connected to a website that contains sexually explicit, racist, or other potentially offensive content must disconnect immediately. If the user does not disconnect, the Human Resources Department will issue a written warning to the user in the first instance, and any further incidents will result in disciplinary action.

4.5 Procedures:

- The Internet connection leased through ASU's ISP will be only available for distribution within ASU.

- If a user need additional Internet access, they should contact the ASU user's department manager, who will approach the IT department on their behalf.

- It is the responsibility of ASU users to ensure that unnecessary browsing on the Internet and visiting restricted sites should not be carried out.

- The IT department monitors the Internet usage on a daily basis in order to verify any possible usage disruptions.

- ASU users shall not depend on the supposed identification of an Internet correspondent unless that entity's identity has been verified using techniques allowed by digital certificates or digital signatures.

- ASU users must not post to public discussion groups, chat rooms, or other public forums on the Internet unless University management has given them permission to do so on behalf of ASU.

- ASU users are not allowed to host their personal web-sites using ASU facilities.

- ASU users must not download software and contents that's not related to education from the Internet unless specifically authorized to do so by the IT department.

- ASU users must not send any sensitive parameters such as credit card numbers, fixed passwords or customer account numbers via the Internet unless the connection is encrypted.

- ASU users should be made aware that ASU accepts no liability for their exposure to offensive material that they may have accessed via the Internet.

- At any time, the IT department reserves the right to examine web browser activities on ASU computers with appropriate approvals.

- Electronic Data Interchange (EDI) and other electronic system designs would be prohibited unless the IT department gave permission.

- ASU users may not misrepresent, hide, suppress, or substitute their own or another user's identity on the Internet or any other ASU information system.

- Any ASU user who receives information concerning system vulnerabilities should submit it to the IT department, in order to decide whether any action is necessary.

5 Access Control Policy

5.1 Purpose:

The access control policy is developed to control access to information and prevent unauthorized users. All ASU sensitive information should be restricted such that it is only used for the intended purpose(s).

5.2 Scope:

All ASU Users.

5.3 Objective:

To safeguard the data from un-authorized user access

5.4 Policy:

- Access granting and controlling is based on the business flow and security requirements.
- ASU formalize system access control procedure and obtain its approval from DOD.

5.4.1 User Registration and De-registration

- A unique user ID and password is assigned for all staff and student.
- The use of generic user ID's is prohibited. Instead, the user ID identifies each user.
- While creating a user ID for system access, a formal request must be initiated which in turn must be approved by the HR department for academic and non-academic staffs. Student account will be created based on the student ID generated from ERP system (Student Information system).
- Guest and trainee accounts shall be created based on the request from the respective department after approval from DOD.
- Shared accounts are created and shared with departments / Committees/ Vendors for ASU internal use.
- Any request to create login on temporary basis will be approved by DVC-RIS and should be initiated by HR.
- On termination of an employee, contractor or third party service provider, the user's access to ASU's internal facilities will be restricted.
- The users account will be disabled / cancelled when an employee's service with the University ends for any reason or when a student graduates or transferred out, or is

dismissed either temporarily or permanently. When cancelling user's account IT department has the right to delete all information in the system and University will bear no responsibility of any consequences.

- For the purpose of disabling the user account HR department should send the clearance form to the IT department with details (including last working day) of terminated staffs.
- System privileges of all ASU users is restricted based on the job responsibilities.
- In order to prevent unauthorized user access, all ASU users are made aware of their responsibilities for maintaining effective access controls.
- This policy ensures that the user ID is disabled for terminated employees within 2 days of the last working day or will be opened temporarily based on approval from VC / DVCs.

5.4.2 ERP and Applications Access Control

- ASU formalize system access control procedure and obtain its approval from DOD. This shall be based on the job responsibilities the employee is assigned.
- All the required access should be sent by the DOD mentioning the menu and ERP modules / Applications which need access.
- IT department send the list of all access to DOD/Line manager which is provided to employee and DOD / Line Manager should review and confirm the access rights in yearly basis.
- The DOD/ Line Manager is responsible for reviewing user access rights periodically in order to review any known discrepancies
- New access rights can be added / revoked at any time based on DOD / Line Manager request.
- Information system privileges will be promptly revoked at the time of an employee or contractor's termination or resignation with ASU.
- Each user should only perform the activities that are assigned to them in the segregation of duties matrix.
- For All changes to ASU's information system, Line Manager should sent the change request by duly filling the Change Management Form (Form No.1.7)
- Change Management form must be duly approved as per authority manual before changes have been implemented.

- All emergency change requests may be obtained directly via email.
- The IT department is responsible for addressing ASU users change requests.
- The IT department will provide necessary justifications in case the users change request has been denied.
- Backup configuration copies must be obtained before any changes are implemented in the production environment.
- All change items will be effectively tested before they are sent for change item owner review.

5.4.3 Password Management

- All passwords must have at least 8 characters.
- Password complexity includes at least one numeric (0-9) and one character (a-z, A-Z). The usage of special characters is optional.
- All users must be forced to change their passwords at least once every 90 days.
- Passwords will be encrypted when transmitted over networks.
- Passwords should not be written down or left in an unattended place in order to prevent unauthorized users from discovering it.
- Passwords should never be shared with anybody other than the authorized user.

5.5 Procedure:

5.5.1 Procedure for Granting Access Control / ERP and Application control

- All user creation request is initiated by duly filling and submitting the User Access Form (refer FORM No. 1.5) by the user.
- All Academic / admin staff's user creation should be sent from HR department.
- Users requiring additional access to systems must fill this form and send it to their reporting manager for initial approval.

- If the request is approved, the reporting manager will forward the request to the IT department.
- The user's need for access will be evaluated by IT Department for final approval at this stage.
- In cases where the request is denied, user request will be returned to the user with adequate justification stating the reason for denial.
- Once approved, the IT department will implement the access request.
- The IT department will create the login credentials for the user which will contain a temporary password.

5.5.2 Procedure for Revoking Access control / ERP and Application control

- The Human Resources department will forward the user clearance form (Admin and Academic staffs) to the IT department in order to revoke the user's access.
- The IT department will implement the user access revocation.
- ERP access will be revoked automatically once the HR complete the end of service process in ERP system.
- Each section within the IT department will disable all the relevant access rights which were assigned to the user.
- Copy of this form is archived for records by the IT department

6 Email Account Policy

6.1 Purpose:

ASU provides email accounts to all staffs and students in the University. Email is the main channel of electronic communication between University members. The goal of this policy is to ensure that email services are available to all users without delay, that they work properly, and that they are used in the most effective way possible.

6.2 Scope:

All ASU Users.

6.3 Objective:

To facilitate communication and co-ordination among different stake holders

6.4 Policy

6.4.1 Use of ASU email accounts:

- Only authorized users will be given access to the University email services.
- The E-mail facility is a University resource and should be used for official communications only.
- At all times, ASU users must take security precautions when exchanging information within emails.
- Users must refrain from using any email account other than the University account for official email communications.
- ASU users shall not forward emails classified as confidential outside ASU networks unless prior approval has been obtained.
- All incoming emails are scanned for virus and any other malicious content.
- ASU users must refrain from digitally transmitting or displaying on their devices text, video or images that could possibly create an atmosphere of discomfort to others.
- Appropriate disciplinary action may be taken in case of non adherence to the Email policy.
- The maximum message size which can be sent outside ASU email is 20 mb.

- ASU admin and academic staff groups shall be created by IT department after the approval from DOD / Line manager and the necessary permission for the staff to send or receive will be decided by DOD/ Line Manager.

6.4.2 Department Email Accounts:

Departments providing services may request email accounts specifically created with department names. DOD of requesting department will be the owner of this email accounts.

6.4.3 E-mail Address Policy

A standard format e-mail address for staff in the form of firstname.lastname@asu.edu.om can be used. Staff may express a preference as to their username wherever applicable.

A standard format of email address for students in the form of Student ID@asu.edu.om can be used.

6.5 Procedure:

- Requests for creation and deletion of user email accounts will be based on user access control policy
- Requests for creation and deletion of email accounts for students will be based on user access control policy
- User email accounts will be deleted based on access control policy and all user email content has been backed up for possible restoration in the future.
- Each user will be assigned to the relevant department's mailing list and these lists must be denoted in the user creation form.
- Each user mailbox will be protected by a password.
- All ASU emails must be handled in a confidential and secure manner and must not be forwarded to unintended recipients.
- Users must be cautious while sending sensitive information over email.
- Users must automatically notify correspondents if they will be unable to respond to their emails for an extended period of time.

- By default, all email messages of staff will be recorded in logs and back-ups.
- ASU users are responsible for saving important messages which might be needed at a future date.
- ASU users must not use profanity, obscenities, or derogatory remarks in any email messages discussing ASU users, applicants or other involved with ASU.
- Sexual, ethnic and racial harassment including unwanted email messages will be strictly prohibited.
- In occurrence of such situations, user will be issued warning by the Human Resources Department and in case of any subsequent incident, HR should take disciplinary action against user.
- Guest email accounts will be created for external consultants and third parties working at ASU after getting approval from DOD / Line Manager.
- All Guest email accounts will be deleted/disabled on a timely basis by the IT department after notifying by DOD / Line Manager from requesting department.
- Anti-virus software will be installed on the e-mail server, in order to monitor all incoming and outgoing mails.
- These mails will be scanned in a way in order to detect any potential viruses, malicious code and phishing software.
- Deleting emails sent / received from mail server require approval from VC \ DVC's.
- Email server performance and capacity levels will be logged and monitored on a continuous basis.
- The email application will be analyzed by the IT department on a periodic basis.

7 Physical and Environmental Security

7.1 Purpose

All ASU critical or sensitive information assets should be secure from unauthorized access, damage and interference by employing appropriate physical and environmental controls.

7.2 Scope:

IT Resources, Data Centre, Patch Panel rooms and ASU users.

7.3 Objective:

To safeguard IT resources from unauthorized access.

7.4 Policy Guidelines

7.4.1 Physical Access Control

- Secure areas such as buildings, server rooms, and sensitive information printing rooms should be protected by entry controls to restrict access to authorized personnel's only.
- Information processing facilities should remain locked and protected at all times. Effective security arrangements like cipher locks, biometric, key-card door locks etc. should be used for such facilities.
- Data Center access request should be formally documented.
- Access rights should be approved by senior management.
- Temporary physical access rights assigned on a temporary basis should be revoked promptly when no longer needed.
- Visitors should be granted access only by authorized ASU personnel and their time and date of entry should be recorded for traceability.
- Access to sensitive information should be restricted on need-to-know basis.
- Use of camera's or mobile phones in secured areas such as Data center is prohibited

7.4.2 Physical Security Measures

10.5.2.1 Monitoring

- Surveillance video systems (CCTV) that are capable of monitoring all movements within sensitive information processing facilities should be installed.
- System should be capable of monitoring the area during non-operational times.
- These systems should be capable of creating an account of any user that has interacted with such information.

10.5.2.2 Power Availability

- In order to reduce the risk of spikes and surges, surge protectors should be deployed for all electrical equipment.
- Power availability at all times should be ensured by using backup generators for the unlikely scenarios of power unavailability.
- Uninterruptible Power Supply (UPS) devices should be used for maintaining continuous power flow.
- Emergency lighting should be employed in case of power failures.

10.5.2.3 Cabling Security

10.5.2.4 General Security Measures

- Information processing facility area should be clean and no combustible or harmful items should be placed in the designated areas.
- Food and drink should not be allowed near computer installations or inside the data center.

10.5.2.5 Damage, lost and penalty

- If the user causes any damage to the IT resources and system or lost any IT devices, Asset committee which will go through the violating actions referring to the terms and conditions of the Asset Committee. Based on the report it is allowed to impose
    - Financial penalty equal to the damage or lost caused. The penalty will be determined by the Directors of IT and Finance Department based on the table outlined in Appendix 1.1.
    - It is not allowed to take a decision before informing the violating user about the case and be given a chance to defend his actions.

7.5 Procedures

- Access to the Data Center and Patch Panel Room will be secured at all times.
- IT department will ensure that access to the Data Center and Patch Panel Room is restricted through individual swipe cards or biometric device to only authorized ASU IT employees.
- The list of authorized ASU IT employees must be maintained by the IT department and must be periodically reviewed by the DOD.

- Visitors may obtain permission to enter the Data center by duly filling and submitting the Visitor Access Form (refer FORM No. 1.4).
- Visitor logs should be maintained by the IT department to keep track of people entering the Data Center.
- Access privileges to visitors must be assigned on a temporary basis and must be revoked once the need is over.
- At all times, visitors entering the server room must be accompaniesd by an ASU employee authorized to enter the Data Center.
- Magnetic material should not be brought within the premises of the Data Center
- Data Center temperature, humidity and water leakage is constantly monitored by the IT department and all the necessary Servers and peripheral maintenance should be conducted on a timely basis.
- Data Center is adequately equipped with fire-fighting equipment and smoke detectors in order to minimize damage.
- In order to avoid accidental spillage and resultant damage of computer equipment, water and other liquids are not be allowed within the Data Center

  Patch Panel Rooms and computer labs.
- Sensitive documents should not be left in the open and must be contained in locked and secure cabinets.
- Telecommunication lines and network cables for information processing should be underground / above false ceiling and must be protected from unauthorized interception.
- Power going into the servers and storage, core switches, access switches, AP controllers should be through UPS systems.
- Regular cleaning of the IT equipment and storage areas must be conducted in order to protect from dust depositing over computing equipment.
- Data Center is monitored using CCTV continuously and the surveillance videos should be archived.
- Not allowed to use camera and mobile phones inside Data Center.

8 Backup and Restoration

8.1 Purpose

In order to maintain the integrity and availability of information, information processing and communication services from various environmental threats, backup of all University data must be carried out on a scheduled basis.

Scope:

Servers, Database and applications.

8.2 Objective:

To ensures availability of data in the event of a disaster or for recovering old records.

8.3 Policy Guidelines

- Backup process will be carried out regularly where all important system/applications along with their configuration, operating systems software, databases, and user configurations will be backed up.
- Backup media will be adequately labeled. The label defines the content stored on the media in such a way that it does not reveal the sensitivity of the information to an unauthorized person.
- Access to media is through authorized IT staff only.
- Activity logs will be maintained for the backup media in order to keep track of the location and chain of possessions of the media.
- Media will be transported from the onsite location to the offsite secure storage location. This activity is logged at all times.
- Backup tapes are located in a remote offsite location within fire proof vaults, in order to protect the backup media from any material damage in case of disruption at the main site and restricting access to unauthorized personnel.
- Restoration processes will be evaluated and tested on a regular basis to verify their effectiveness.

Backup Retention Period

1 Information will be kept for as long as it is necessary to meet regulatory requirements.

Backup policy for MS office 365 clients will be according the Microsoft data protection policy published in Microsoft website.

8.4 Procedures

- Backup instructions and backup schedule must be maintained by the IT department.
- Backup should be obtained on a regular basis, in order to ensure that data is readily available in the event of a system failure or a disaster.
- Backup restoration process must be tested periodically in order to review the recovery efficiency rate.
- Vendor recommendations should be considered while backing up the core University application.
- The IT department should initiate and implement the backup process.
- Incremental on-line backups should be conducted on a daily basis for the transaction logs from the database management system.
- Complete off-line backups should be conducted on a weekly basis where data on all volumes should be backed up along with the system state data.
- Backup media must be periodically examined in order to verify the readability of the data.
- Once the monthly backup process has been completed, details of the backup media should be recorded. This may be done using Backup Logs (refer FORM No. 1.6).
- These logs are mainly used for reference purposes as they make it easier to locate the required files during restoration and may be maintained manually or may be system generated logs.
- In addition to this, backup movement logs must be maintained by the personnel carrying the storage media to off-site location.

- All logs must be reviewed by the IT Director on a periodic basis.

- In cases where the backup restoration fails, the issue should be reported by filling the Incident Management Form (refer FORM No. 1.8).
- Backup restoration tests must be carried out at least two times a year in order to verify the readability of backup media.
- Once the backup process has been completed, it must be transferred to secure on-site and off-site locations.
- Three copies of the backup media must be maintained by the IT department, with one copy in a secure off-site environment.
- Off-site back-ups must be maintained at ASU's disaster recovery site.
- On-site data back-ups must be maintained within a fire-proof vault, preferably in the server room.
- Access to this vault must be only designated to specific members of the IT department.
- Efficient security controls must be maintained for the storage of backup media and backup devices.
- In cases where the backup technology has been changed, then all the backup data should be migrated to the new media type.

9 Incident management

9.1 Purpose

Incident defines the activity that has caused a damage/ misuse to IT resources and information. All incidents must be duly reported by following the Incident Management Procedure. This in turn reduces the system downtime and provides detailed logs of previous incidents.

9.1 Scope:

ASU users

9.2 Objective:

To ensure system availability and high quality of services delivered by the IT department,

9.3 Policy Guidelines

- All incidents must be reported through Line manager to IT department by duly filling and submitting the Incident Management Form without delay.
- The incidents which need reporting are classified under Appendix 1.2
- All incidents must be reported to the IT department in time and must not be delayed.
- The IT department must take immediate action depending on the situation in order to avoid any future reoccurrences.
- Incident logs must be maintained in order to track any similar incidents that may result in a potential system downtime.
- The IT department must conduct a preliminary analysis of the reported incident before any action is taken.
- This should address details such as time and cost required to potentially resolve the incident.
- An action plan must be devised by the IT department enlisting the steps that must be carried out in order to resolve the incident.
- In where the incident may not be resolved, the user reporting the incident must be informed of the situation.

- Periodic reviews must be carried out by the IT department in order to review the affected domains.
- Any major issues that may result in a potential disruption must be reported to the DOD.

9.4 Procedures

- If an ASU user suspects an incident, they should immediately report it to the IT department.
- Users reporting the incident must duly submit the Incident Management Form (refer FORM No. 1.7) before reporting the incident to the IT department.
- In cases where the incident cannot be resolved, the IT department must send back the incident management form to the user reporting the incident clearly stating reasons why the incident could not be resolved.
- If required, upgrades to the Information System or amendments to the manual may be suggested by duly filling and submitting the manual amendment request form (refer Form No.1.2.).
- All incident logs must be periodically reviewed by the IT Director on a regular basis in order to identify possible recurring and major issues.
- Such issues must be reported to the IT Director for review and obtaining their action points.

10 Educate and Train Users

10.1 Purpose

IT Department should rollout and support all Departments to get acquainted with the IT Technologies implemented in ASU and the latest technologies available in market, so they are built into and are an integral part of the University operations.

10.2 Scope:

ASU users

10.3 Objective:

To ensure the best implementation of all system and high quality of services delivered by the IT department.

10.4 Policy Guidelines

1 ASU IT Department should establish a procedure and regularly update a curriculum for each target group of ASU employees to create IT Technology awareness through training .

2 ASU Management to provide support and attend these training and educational sessions.

3 With coordination between IT Dept. and HR department, sufficient budget need to be allocated for end user IT training and education.

4 User and technical manual documents of system should be prepared and updated.

Further guidelines to be considered for end user trainings:

1 For Faculty and staff training, IT dept. should collaborate with eLearning Dept. and HR Dept.

2 Implementation of new IT infrastructure and software (i.e., packages, applications)

3 Current and future skills, competence profiles, and certification and/or credentialing needs as well as required reaccreditation

4 Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing

11 IT Acquisition and Implementation Management

11.1 Purpose

ASU management should establish and implement process for the acquisition, implementation and upgrade of the technology infrastructure. It should require a planned approach to acquire, maintain and protect the infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. IT should ensure that there is ongoing technological support for systems running in the university and satisfy university requirements.

11.2 Scope

Purchase of all IT equipment and resources

11.3 Objective

ASU should translate University requirements into a high-level design specification for all IT assets acquisition, ensuring that all legal and contractual aspects are identified and addressed for software.

11.4 Policy Guidelines

1 Acquisition procedure should be formally designed, documented and followed for all IT Assets acquisitions in an objective manner while complying with the ASU tendering requirements.

2 A Request for Proposal (RFP) document should be prepared listing functional and technical requirements of the requested solution.

3 Vendors should be asked to arrange on-site visits to demonstrate the use of their products / solutions to ASU Management. These on-site visits should focus to get information on the following points: -

- Requirements Fit: Does the product meet the University specific requirements as per the RFP?
- Reliability: Is the product reliable?
- Commitment to Service: Is the vendor responsive to problems with the product? Can it be delivered on time?
- Customization: Can the vendor customize the product within the estimated time and cost?
- Training & Support: What is the level of user satisfaction on training and support given by the vendor?

12 Business Continuity Management

12.1 Purpose

The purpose of this policy is to have a clear guidelines and safety measures to be taken to achieve Business continuity in case of any sort of disaster.

12.2 Scope

All ASU staffs, departments and IT resources

12.3 Objective

The objective of this policy document is to ensure business continuity with minimal business impact in the event of disruption. Business continuity management should include the following:

1 Business Impact Analysis and Risk Assessment

2 Business Continuity Plan

3 Disaster Recovery Plan

- Maintenance of Disaster Recovery Plan
- Testing of Disaster Recovery Plan
- Training and distribution of Disaster Recovery Plan

4 Recovery and Resumption

12.4 Policy Guidelines

Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is the process of determining the business impact on an organization in case of potential loss actually occurs in the event of a disruption. BIA should quantify when possible the impact of an interruption from a financial standpoint. BIA should also consider the following in respect to the technology functions:

1 Identification of critical University operation processes

2 Identification of critical IT resources for all areas of business to build in resilience and establish priorities in a recovery situation

3 Identification of the risk factors associated with a major disruption of all business processes

4 Identification of the level of impact of critical IT resources for each area of business due to a disruption

5 Identification of minimum resource (staff, hardware, software, data etc.) requirements for recovery

6 Identification of the recovery timeframes for critical IT functions

7 Identification of the maximum acceptable data loss that can happen during a disaster

8 Prioritization of the recovery requirements by mapping to critical University functions

Business Continuity Plan

Business Continuity Plan should describe the procedures to prepare for or recover from any disruption that may affect the critical business processes. The plan should mention the responsibilities of authorized staff, activities and timeframes to resume the business operations.

Disaster Recovery Plan

The purpose of the disaster recovery plan should define the process for recovery of IT resources that could affect the critical University functions in the event of a disaster. Disaster recovery plan should address the following:

1 Determining critical IT resources from the output of Business Impact Analysis

2 Disaster recovery committee/team - authorized personnel who have the authority to declare a disaster, accessing the offsite storage facility and carrying out recovery procedures

3 Recovery strategy – procedures for recovering from a disaster to resume normal operations

4 Plan should specify the testing and maintenance details

Maintenance of Disaster Recovery Plan (DRP)

Disaster Recovery Plan (DRP) should be reviewed and updated on periodic basis ensuring that it reflects actual business requirements

DRP must be reviewed and updated in the event of following:

1 Significant changes have been made to ASU infrastructure (software, hardware, network)

2 New technology, programs or devices are acquired

3 Issues if any occurred during last disaster recovery testing

4 Addition of new branches using the centralized information system

Testing of Disaster of Disaster Recovery Plan

1 Disaster recovery plan should be tested periodically to ensure that IT systems can be effectively recovered in the event of a disaster

2 Disaster recovery site should be in place where testing should be done utilizing actual recovery facility.

3 Testing should include integrated testing of all information systems, integrated testing with vendors and testing of single applications.

4 Procedures for performing the disaster recovery drills should be documented and shared with the disaster recovery team responsible for carrying out the recovery procedures.

5 Test results should be well documented, evaluated and action plans should be implemented to close the gaps.

6 If required disaster recovery plan and testing procedures should be reviewed and updated as per the findings of disaster recovery testing.

Training and distribution of disaster recovery plan

1 Distribution strategy should be developed to ensure that disaster recovery plan is securely distributed to all the authorized personnel/parties.

2 SLA's signed with the vendors should contain vendor commitment in case of a disaster

3 It should be ensured that plan is accessible to all relevant personnel in case of a disaster

4 Training should be provided to each recovery team member for proper execution of the plan

5 Each IT team member should be aware of their roles and responsibilities for recovery and testing procedures.

Recovery and Resumption

1 Actions to be taken during the phases of business resumption:

- Response – initial action followed after a disastrous event
- Resumption – establishing the alternative processing site and begin processing critical University functions
- Recovery – resume processing for less critical business functions
- Restoration – returning to the original processing site

2 Notification procedures for employees, vendors and customers should be documented

3 Contact information for authorized personnel responsible for carrying out the recovery procedures should be documented

4 Step by step description of actions required for recovery and resumption should be documented

5 Up to date equipment and software inventory should be in place and documented

13 Bulk SMS:

Bulk Messaging is the dissemination of large numbers of SMS messages to various mobile phone of a predetermined group of recipients.

13.1 Purpose:

At ASU Bulk messaging is used to send regular updates/alerts, reminders and announcements to students, staffs and stakeholders. Bulk Messaging is the dissemination of large numbers of SMS messages to various mobile phone of a predetermined group of recipients.

13.2 Scope:

Authorized ASU users/ Department

13.3 Objective:

To broadcast information to various stakeholder.

13.4 Policy:

- It is the responsibility of Line manager to oversee the contents of the message send using ASU bulk SMS system.
- It is the responsibility of Line manager to oversee the list of recipients of messages.
- IT department responsible for maintaining the subscription renewal of Bulk SMS system.
- Department which does not have authorized access to SMS system must send the request with list of recipients and the message to IT department with approval from Line manager to process the request.

13.5 Procedure for sending Bulk SMS through IT Department:

- The staff (Requester) should get approval from respective department head for sending SMS to students.
- The list of phone numbers and message after getting approval should be submitted to IT department. The list with numbers should be in excel sheet.

- The staff (Requestor) is responsible to check and validates the accuracy of provided information "List and SMS body"
- IT department staff should get approval from IT Director before sending the message.
- If the list of numbers is more than 1000, then the approval from DVCRIS is required.
- All SMS for public announcement should get approved from DVCRIS.
- SMS will not be send on Fridays as per the policy of operator.
- Once SMS will get sent, IT department is not responsible for the delivery of SMS, it depends on operator and mobile network availability.

14 IT Systems / Applications Ownership

14.1 Purpose

The purpose of this policy is to provide guideline for the ownership of all IT systems/ applications and database at ASU.

14.2 Scope:

ASU users

14.3 Objective:

To avoid un-authorized access to system and data.

To define the ownership of system and data.

14.4 Policy Guidelines

It is critical to determine the ownership of all of the IT systems, applications and data at ASU to avoid any confusion with regards to responsibility of data ownership and system administration task of the system/application.

Data Ownership:

Following is the guideline related to ownership of each IT System/ Application and database at ASU.

- Respective department head should have ownership of the Data
- Data entry, editing and cleaning responsibility should be with respective department head.
- Respective department head should be responsible to define segregation of duty for staff of his/her business function.
- Any Change in any system implemented in ASU should be under the responsibility of IT Department.

System Administration:

IT department should be responsible for the system administration task of each and every IT system / application installed at ASU.

System administration task includes the following:

- User access management which includes user access creation and revocation task.
- Defining roles and assigning role to business user as per respective department head instruction.
- Monitor system performance.
- Setup security policy for users.
- Installation, patching and upgrade of database, OS and IT system / Application.
- Password and identity management.
- Database Management which includes security setting and data extraction
- Modification of existing reports.
- Development of new reports.
- Installation of hardware and setting infrastructure.
- Installation of operating system and database.
- Monitoring of OS, Database and IT System logs.
- Backup and archiving of the system on frequent basis.
- Trouble shooting related to IT system/application.
- Providing day to day support to the business users.

15 IT Asset Policy

15.1 Purpose:

To encourage the faculties /administrative staff of ASU in utilizing IT resources, ASU provides IT Equipment like Desktop, Printers, Laptop, mobile phone and tablet devices to all authorized users for their assignment/programs/day to day tasks of the University. This policy defines the guideline for distribution and management of ASU equipment.

15.2 Scope:

ASU authorized Users

15.3 Objective:

To distribute and manage the IT equipment.

Assist faculties/staff for achieving their assignment/programs/day to day tasks of the University.

15.4 Policy:

- Request for IT equipment should be initiated by Line manager during the preparation of Annual Budget.
- At all times, ASU equipment except portable devices issued to ASU staffs must not leave the premises without prior approval from IT Department.
- Users are not allowed to change the location of IT equipment except portable devices without consent from IT department.
- In case of damage or loss of equipment, the custodian must promptly inform the IT department.
- All sensitive data and licensed software should be effectively removed prior to the disposal of the equipment.
- Admin rights on computers are not provided to users unless authorized by VC/DVC.
- The University has complete authority in the allocation of the IT Equipment to the staffs and staff must accept the model/brand assigned to him/her.
- The University's IT equipment is and will always be its property. Without the approval of the IT department, the equipment may not be given or transferred to other users.

- The staff must not add or remove, any hardware / Software as well as labels to or from the devices and also should not copy or alter any software's installed in the device

- The devices shall be used by the staff for education, learning and official work. The staff shall be responsible for any liabilities incurred because of the improper use of device.

- The staff shall take all reasonable steps to maintain the devices in good working condition. If any repair is necessary, the staff must bring the devices to the IT services department for service. The staff will pay the cost of repair in case the damage is caused by inappropriate usage (As outlined in Appendix 1.1).

- In the event of loss of the devices, the staff must forthwith report the incident to the IT Department. The staff must pay the penalty based to the table in appendix 1.1

- The University requires the staff to bring the portable devices to the University for official work or for the purpose of inventory and audit checking.

- Appropriate disciplinary action may be taken in case of non-adherence of the terms and conditions herein by the staff. The action would be dependent on the nature of violation of the terms and conditions of the contract.

- When the staff completes his/her work/tenure of service, the contract will be automatically terminated and the staff will be informed of the arrangement for returning the devices to the University immediately.

- For cases where staff is unable to produce and return the devices as required, they will be asked to repay the price of the device and any installed licensed software to the University, and the penalty charge as appropriate. Penalty will be according to appendix 1.1

- It is the user's responsibility to take backup of data when sending the devices to IT department for repair.

- The IT Department is responsible for issuing the mobile phone and SIM to authorized ASU users.

- Respective department head shall analyze the need of mobile communication device for staff.

- All mobile communication devices are purchased based on the requirement.

- Access to mobile phones must be password protected.

- Only approved third party applications can be installed on mobile devices. The approved list will be available on the Appendix 1.3.

- IT Department will cancel accounts for unused mobile phones and get hold the unused devices and SIM.

- User are aware that mobile phone usage will be monitored and the mobile device users may be required to justify their use.

- Return the mobile phone and SIM to IT Department if the device is no longer required.

    - If it is a requirement to take University owned mobile phone while on personal leave, the user must seek permission from the Line Manager.

15.5 Procedure:

- IT department initiate the request based on the approved annual budget or approval from VC/ DVC.

- The specification should be based to the business need.

- For portable equipment the users must adhere to the IT Asset Policy and sign a confirmation and undertaking ("Staff's Confirmation & Undertaking"). Please refer the form attached hereto before completing the application (Form 1.9).

- IT department is responsible for making sure that all necessary software and updates are installed before handing over the devices.

- IT department is responsible to evaluate the condition when the device is returned back to IT department.

- If required to change the equipment location except portable devices, IT will be looking the feasibility and if appropriate will co-ordinate with Asset Management Department to take necessary action. If IT sees the request is not possible, then it will be written back to department explaining the cause.

- The request for Mobile phone and SIM card should be send to IT department

- After procurement process the mobile with / without SIM card, IT department issue the device to Line Manager or user.

- The line manager/ user is responsible for returning the mobile phone, SIM card and accessories to IT department.

16 IT Asset (Hardware/ Software) Replacement Policy:

16.1 Purpose:

The purpose of this policy is to make sure IT equipment's are maintained properly and adequate replacement procedure are in place.

16.2 Scope:

Applies to all IT equipment's (Hardware / Software Resources)

16.3 Objective:

All the equipment's owned by ASU have a replacement process. IT department monitor and review the IT resources (Hardware /Software) periodically to make sure that all the devices are working in good condition that meets the business need of the ASU and will take the necessary replacement action.

16.4 Policy:

- For Laptops, desktops, printers, photocopiers and projectors, the life cycle will be 4 years.
- For network devices and servers, the lifecycle will be 5 years.
- Mobile phones and tablets the lifecycle will be 2 years.
- No devices will be replaced before the lifecycle unless there is a valid reason that the device will not suite the business requirements or damage / faulty which cannot be recovered.
- IT department responsible for evaluating the situation of any devices which need replacement and to initiate the procurement process based on business need and budget availability.
- All the IT resources which are under warranty should be maintained with the vendor through IT department.
- Software's must be upgraded to latest version if required.
- The equipment's which have completed life cycle and cannot be reused must be written off.

16.5 Procedures:

- IT department prepare report periodically about the ASU devices life cycle and propose the necessary action plan.
- ASU users requesting replacement should be sent to IT department with legitimate reason for the request and approval from Line manager.
- IT department will evaluate the request and escalate the request to VC/ DVC for final approval.
- The evaluation criteria will depend on continuous failure/ malfunction, warranty expiration, outdated model, support service not available from vendors and the allocated budget.
- Once the request is approved, IT department initiates the process for the replacement.
- For equipment's (IT Resources) under direct supervision of IT department, IT Director review the report and propose the plan to VC / DVC for approval.
- IT department prepares the list of equipment's which need to be written off.
- All data must be removed from the equipment which is listed in the write off list.
- The write-off list will be sent to Asset Management Department for final process.

17 Helpdesk Support Policy:

17.1 Purpose:

To provide efficient and timely IT support services for each staff and students to accomplish his/her work effectively. To assist in proper use of IT resources to enable the user to do their daily tasks.

17.2 Scope:

All ASU users, IT Dept.

17.3 Objective:

To ensure that IT helpdesk, support the administration, teaching and learning in ASU efficiently on time without delay.

17.4 Policy:

- IT Helpdesk support will be provided from 08:00 AM till 04:00 PM in the working days (Sunday to Thursday)
- End user should not raise support calls for their personal devices
- End user under his responsibility to take back up for his data before handing the equipment to IT Dept for problem solving
- For urgent case, end users can raise the issue through telephone/email to IT staff
- IT dept will not be responsible for issues arising from the misuse of IT resources and the end user will be liable for the cost incurred in fixing the issues

17.5 Procedure:

- End user must report the issues to IT support by registering in the IT helpdesk system
- Helpdesk support staff will be monitoring the call registered in IT helpdesk system and will escalate the calls to the respective IT sections.
- IT Helpdesk support includes but not limited to:
  - Desktop / Laptop support

- Printer/Projector/Photocopier
- Internet and network
- Communication devices
- ERP and Software Application Support

- End user can view the ticket number of the call registered with their status.
- IT department will keep the logs for all calls registered in Helpdesk for better service improvement
- Issue resolution for cases covered by AMC/ SLA and are not under technician's expertise will be escalated to outsourced vendor and the resolution time depends on the AMC/SLA agreed between ASU.

18 BYOD (Bring your Own device) Policy:

18.1 Purpose:

This policy offers the guiding principles and responsibilities to guarantee that the University's mobile and BYOD device objectives are realized. It also describes the University's strategy to using personal mobile devices and "bring your own device" (BYOD).

18.2 Scope:

Employees, guests, students and any other user that uses University resources through their personal device.
Information processed, accessed, manipulated, or stored (in any format) by the University as part of its operational activities

18.3 Objective:

The University's goals for this policy are as follows:
Safeguard the data of the University from security risks that can harm its operations or reputation.
Respect the University's obligation to take care of the data that has been entrusted to it.
Through the effective use of controls, safeguard the confidentiality, integrity, availability, and value of information.

18.4 Policy:

Mobile devices, including Laptops, tablets, and smartphones, that are not provided by the university must adhere to minimal security standards in order to protect university data.
Any mobile device used to store or access private or confidential data or information belonging to the University must at the very least have the following measures in place:

a- Passphrase or PIN of at least four digits.
b- Device is configured to lock automatically after a predetermined idle time.

The mobile device must additionally meet:
Software updates from the manufacturer and other third parties get software updates for security patches within one week of their availability, and only install trustworthy applications from reliable official sources.
Antivirus should be updated to latest version.
All the end user who connects their own device should abide the Network, internet, password and IT resource acceptable usage policy.
ASU will not be responsible for maintenance, backup and loss of data on a personal device.
Moreover, any data which is shared or unauthorized use of data due to lost or stolen device will be the responsibility of the Employees, guests, students and any other user that uses University resources through their personal device.

18.5 Procedure:

- End user responsible for getting the required approval for registering the devices which are connected to network (Wired/ Wifi).
- End user responsible for the data traffic generated from the networked devices.
- End user responsible for abiding all applicable laws of Sultanate of Oman
- End user responsible for protecting own privacy and privacy of others.
- All the end users who connect their own device should abide the ASU IT Policy (Network, internet, Access control and Acceptable Use of Information Technology Resources).

BYOD support services

Support services provided by IT department is limited to:

- Support on network connectivity when the devices on ASU network
- Support on email configuration and VPN connectivity for accessing ASU network

IT Dept services not responsible to provide support and are not limited to,

- Installation or troubleshooting of Operating system and software's which are not related to University work
- Hardware replacement or fixing issues
- Backup of data
- Fixing issues caused by virus / malware attacks.

19 Forms

MANUAL DISTRIBUTION CONTROL RECORD **FORM No. 1.1**

Manual Copy No. _____					
Date of issue	Custodian			Date of return	Signature of Controller
	Position	Name	Signature		

MANUAL REVISION PROPOSAL	**FORM No. 1.2**

		Serial No.	Date
Originated by:		Position:	
Matters proposed to be revised (attach photocopies if required)			
	Number	Description	
Chapter			
Section			
Paragraph No		Page No.	
Proposed revisions (use additional sheets if required)			
Reasons for proposed revisions			
Comments of Director of Purchasing & Stores			
Comments of Director of Financial Affairs			
Authorized signatories (Sign off)			
Approved	Effective date …….		
Not approved		Signature	Date

MANUAL REVISION CONTROL SHEET **FORM No. 1.3**

				Chapter	Section	Page
Release Number	Release Date	Covering Letter Reference	Manual Revision Proposal Reference	Remarks		

VISITOR ACCESS FORM	**FORM No. 1.4**

Visitor name	
Date	
Visitor Unit/Organization	
Expected duration of visit	
Name of the person to be visited	
Branch/ Campus	
Purpose of visit	
Signature	_____ _____
	(Visitor) (Director – IT)

USER CREATION FORM	FORM No. 1.5

To be filled by Employee

Name				
Designation				
Department				
Employment Type	Employee (Full Time)	☐	Employee (Part Time)	☐
	Internship/ Trainee	☐	Guest	☐

Signature Date

For HR Department use

Approved / Verified by

Name **Signature** **Date**

Note: HR department should verify and correct the details filled by employee as per HR record.

For IT Department use

Created by

Name **Signature** **Date**

Remarks

BACKUP LOG	**FORM NO. 1.6**

S. No	Date	Description	On-site/Off-site	Remarks

CHANGE MANAGEMENT FORM	**FORM No. 1.7**

Change request title		Change ID	
Change Request Owner			
Date			
Department			
Branch/ Campus			
Description of current situation			
Description of change request			
Change duration	☐ Permanent ☐ Temporary		
Description of risks associated (if any)			
Decision	☐ Approved ☐ Denied		
Denial Justification			
Approved by	_____ _____	_____	
	(Change Item Owner) (Change Request Owner)	(Director – IT)	

INCIDENT MANAGEMENT FORM	**FORM No. 1.8**

Employee name	
Incident reported by	
Date	
Department	
Branch/ Campus	
Immediate action required	☐ Yes ☐ No
Description of incident	
Department(s) affected	
Resolution time	
Estimated cost	
Incident Analysis	
Incident status	
Signature	_____ _____
	(Incident Reported By) (Director – IT)

STAFF'S CONFIRMATION & UNDERTAKING	FORM No. 1.9

STAFF'S CONFIRMATION & UNDERTAKING FOR MOBILE DEVICES

I, _____ (Name of Staff), ID Number:_____, Designation _____ hereby confirm that I have received the below item(s).

I shall at all comply with terms and conditions of ASU IT Policy which may be varied, amended, supplemented or superseded from time to time.

I understand that any violation of these policies is subject to disciplinary action by the University.

Equipment Details :	**Model & SL No.** **Accessories**

Signature: _____

Date: _____

20 Appendix

20.1 Appendix 1.1

Table of Penalty for Lost or Damage of IT Equipment

Equipment returned with Damage in less than one year of purchase	Full purchase cost of the equipment or the cost of repair estimate whichever is lower.	
Equipment returned with Damage in less than two year of purchase	80% of Purchase cost or the cost of repair estimate whichever is lower.	
Equipment returned with Damage in less than three year of purchase date	60% of Purchase cost or the cost of repair estimate whichever is lower.	
Equipment returned with Damage in less than four year of purchase date	50% of Purchase cost or the cost of repair estimate whichever is lower.	
Equipment returned with Damage in less than five year of purchase date	40% of Purchase Cost or the cost of repair estimate whichever is lower.	
Equipment returned with Damage after five years of Purchase Date	30% of Purchase Cost or the cost of repair estimate whichever is lower.	

20.2 Appendix 1.2

Incident Reporting:

Events which need incident reporting include but not limited to the following:

Damage/loss of IT Resources or data

Inappropriate IT asset movement without prior approval from IT department.

Non-Compliance with IT policy and procedures

Hacking other individual files/ system

Accessing the system / application with other staff's credentials without their permission or approval from Line manager.

20.3 Appendix 1.3

Approved services/applications for mobile phones:

- Phone call Services
- Messaging (SMS)
- Internet access through corporate networks
- Mobile office applications
- Word processing application
- Spreadsheet application
- Presentation application
- Outlook application