Aga Khan University Hospital

Document Title:	Global Information Security Policy		
Department / Division:	Information Communications Technology (ICT)		
Approved By		Document Reference/Policy No.:	ADM-P-024
Chief Information Officer		Issuance Date:	4 August 2018
		Revision Date:	24 May 2024
		Revision No.:	4.0
		Number of Pages:	42

1.0 Policy Statement: The Aga Khan University's (AKU) Information Security Policy is designed to ensure the safeguarding of information assets belonging to our housed at the University.

2.0 Terms and Definitions:

Acronym	Description
AKU	Aga Khan University
ISP	Information Security Policy
CIO	Chief Information Officer
IS	Information Security
ISP	Information Security Policy
ICT	Information Communications Technology
SIEM	Security Incident & Event Management
DR	Disaster Recovery
BCP	Business Continuity Planning
VA	Vulnerability Assessment
PT	Penetration Testing
MFA	Multi Factor Authentication

VPN	Virtual Private Network
SDLC	Software Development Life Cycle
TOR	Terms of Reference
SIRT	Security Incident Response Team
ISSC	Information Security Steering Committee

3.0 Purpose: The purpose of the Information Security Policy (ISP) is to ensure the protection of information assets and the effective management of information technology systems and services at AKU. The policy provides guidance on appropriate measures to ensure confidentiality, data integrity, availability, accountability, and responsibility across the enterprise. The ISP is owned by the Chief Information Officer (CIO).

3.1 Information is key to enabling AKU to meet its operational objectives. When utilizing ICT resources, it is therefore essential that AKU retain ownership and control of its systems and information, and that they are appropriately protected to ensure that:

3.1.1 Confidentiality of information is appropriately maintained.

3.1.2 Integrity of information and systems can be relied upon.

3.1.3 Information and systems are available when the business needs it.

3.1.4 Individual users of AKU, who process information relevant to our business, will be identifiable and accountable for their use of those resources.

3.1.5 Access to AKU ICT resources will be assigned to users based on the requirements of their job function and authorized by the Business Owners of those resources.

3.2 This Policy is consistent with the requirements and guidelines contained in the ISO 27001:2013 standard. The alignment of the ISP with ISO 27001 benefits all users of ICT resources, including, where applicable, third-party suppliers or contractors.

4.0 Scope and Applicability:

4.1 This policy is applicable to AKU employees (permanent or contractual) and third-party contractors or vendors that have been granted access to AKU information or ICT resources, regardless of:

4.1.1 How information is represented (written, spoken, electronic and other formats).

4.1.2 The methods and technologies used to handle the information (e.g. AKU information systems, databases, networks, file servers, personal computers, emails, fax machines, printers, and telephone systems).

4.1.3 The location of the information (e.g. AKU campuses, hospitals, offices, or off premises).

4.1.4 Software Development Lifecycle (SDLC) and Information Lifecycle (origination, entry into a

system, processing dissemination, storage, and disposal).

5.0 Access to Information Security Policy: The AKU ISP shall be communicated to all relevant AKU employees handling information assets. This policy shall also be provided to all external parties who are given access to AKU ICT resources, but not to any other external party without prior approval from the Information Security (IS) team.

6.0 Management of Information Security:

6.1 Management Structure for Information Security: The CIO shall ensure that a management and governance structure is established to ensure the ISP is consistent with and supportive of AKU operations and reviewed regularly. The management structure for IS with roles and responsibilities shall be as follows:

6.1.1 Information Security Responsibilities:

i. Chief Information Officer (CIO)

- The CIO shall have the overall responsibility for assigning IS roles and responsibilities and maintaining IS at AKU globally. The CIO may delegate to the Senior Manager, Information Security, all day-to-day operational aspects of IS. Further delegation of responsibilities for specific IS activities shall be the responsibility of the Senior Manager, Information Security.

- The CIO shall designate roles and responsibilities between ICT and IS to ensure segregation of duties.

- The CIO shall review the ISP and IS strategy and plans for AKU and ensure that significant ICT security related risks are addressed, and security activities are undertaken, including ICT security-related monitoring.

ii. Information Security Steering Committee (ISSC)

- The primary responsibility of the ISSC is to assess AKU global IS related issues on a regular basis, provide strategic guidance, review significant information relating to security risks, and make management recommendations regarding the cybersecurity program, including policies and procedures. The ISSC shall meet on a regular basis, but no less than quarterly.

- The ISSC shall be governed by its approved Terms of Reference (TOR).

- The ISSC will provide management support, as appropriate, on IS activities, issues, and incidents.

iii. Senior Manager, Information Security

- AKU's Senior Manager, Information Security is designated by the CIO and is responsible for managing and maintaining AKU's information security / cybersecurity across all AKU operations in alignment with ISO 27001 standards.

- The Senior Manager, Information Security is responsible for developing and maintaining the ISP and corresponding procedures and standards.

- The Senior Manager, Information Security shall identify cybersecurity risks and develop appropriate policies, procedures, and standards to address and mitigate risks.

- The Senior Manager, Information Security shall perform regular reviews of the cybersecurity program and assess compliance with the ISP.

- The Senior Manager, Information Security shall liaise with ICT personnel as appropriate.

7.0 Information Security Policy: The ISP has been developed for implementation across all AKU campuses and operations. The ISP will:

7.1 Assist AKU staff to apply the correct level of security controls to their day-to-day activities.

7.2 Assist with the development and commissioning of new processes and systems by detailing the required security settings and standards.

7.3 Management Responsibilities for the Information Security Policy: Management responsibilities for the ISP should be defined and documented.

7.3.1 Information Security Policy:

- The CIO owns the ISP.

- The Senior Manager, Information Security shall be custodian of the ISP and responsible for ensuring its alignment with ISO 27001:2013, laws and regulations, and contractual requirements. The Senior Manager, Information Security shall be responsible for maintaining, updating, communicating, and implementing the ISP, as well as for monitoring compliance with it.

- The CIO shall review and approve the ISP, assign security roles and responsibilities, and ensure the ISP is enforced and maintained across all AKU campuses and operations.

- The Information Security Steering Committee (ISSC) shall review and approve the ISP and ensure that the development, implementation, and maintenance of the ISP is consistent with AKU operations, and compliance to the ISP is enforced.

- IS shall ensure that the monitoring and review of these policies is carried out in a consistent and impartial manner. The department shall be responsible for maintaining the ISP document and communicating the ISP to staff and relevant stakeholders.

7.3.2 Information Security Policy Review:

- The ISP shall be reviewed and updated as necessary at least every two (2) years jointly by the CIO, IS and ISSC, to ensure that emerging security requirements, new threats, amendments to security-related practices, or major changes to AKU operations, infrastructure, services, and organizational structure, are accommodated in the ISP.

- Any urgent modifications to the ISP can be incorporated and implemented with the approval of the CIO.

- Periodic compliance reviews against the ISP shall be carried out by IS and reported to the CIO and ISSC.

8.0 Organization of Information Security: Information security roles and responsibilities shall be defined and allocated.

8.1 Internal Organization: The CIO shall have the overall responsibility for assigning information security roles and responsibilities and maintaining information security at AKU globally. The CIO may delegate to the Senior Manager Information Security all day-to-day operational aspects of information security. Further delegation of responsibilities for specific information security activities shall be the responsibility of the Senior Manager, Information Security.

8.1.1 Information Security Roles and Responsibilities: All information security roles and responsibilities should be defined and assigned.

i. Specialist, Information Security:

- Assist in the preparation, assessment and enforcement of information security policies, standards, guidelines, and procedures to ensure ongoing maintenance of security for all campuses.

- Monitor security trends and drive security best practices throughout the organization. Monitor for security breaches and investigate a violation when one occurs.

- Perform technology and information security risk assessments. Design and implement technology risk assessment methodology and risk reporting.

- Coordinate with internal and external auditors, third party firms and consultants for audits, security risk assessments, vulnerability scans and penetration tests.

- Organize, plan, and conduct AKU-wide security awareness and education programs that are aligned with global security policy, standards, regulatory requirements, and industry practices.

- Identifying information security weaknesses and/or gaps in the current operations and working with other teams to bring information security operations up to standard across AKU.

ii. Analyst, Information Security:

- Assist in the preparation, assessment and enforcement of information security policies, standards, guidelines, and procedures.
- Perform technology and information security risk assessments.
- Perform internal assessments and identify gaps in current documentation and operations. Work with ICT teams to fix these gaps.
- Assist in organizing information security training and campaigns for AKU staff.
- Review audit logs of servers, network equipment and firewalls on a monthly basis.
- Review SIEM logs daily to detect and identify cyber-attacks. Monitor for security breaches and investigate a violation when one occurs. Assess and respond to network security events and alerts identified through SIEM.
- Assist in remediation efforts related to security incidents, vulnerability assessments and penetration tests.
- Review configurations of network devices: Firewalls, Intrusion Detection Systems, Intrusion Protection Systems, network switches, network routers, VPN implementations for security perspective.

iii. Information Communications Technology Leadership:

- All directors, all senior managers and all managers of within ICT shall develop and maintain operating procedures in-line with AKU Global Information Security Policy and relevant internal or external guidelines for their functions along with roles and responsibilities.
- They shall be responsible for safeguarding all information, including implementing access control systems to prevent inappropriate disclosure, and making back-ups so that critical information will not be lost.
- They shall facilitate IS in Technology Risk Assessments and security reviews.
- They shall be responsible for monitoring and reporting on the security of Information Assets within their purview.
- They shall be responsible for monitoring and reporting of actual or potential security breaches/violations within their areas of responsibility.

8.1.2 Segregation of Duties:

i. Information security roles and responsibilities shall be defined in such a way that duties are segregated to avoid conflicts of interest and to reduce the opportunity for unauthorized

actions or unintentional actions or misuse of assets. The CIO shall designate roles and responsibilities between ICT and IS to ensure segregation of duties.

ii. Conflicting responsibilities shall be appropriately segregated. Compensating controls should be introduced where the segregation of duty principle cannot be implemented.

8.1.3 Contact with Authorities:

i. A list of internal personnel and service providers, as well as procedures for contacting authorities (if applicable) during information security incidents or investigations shall be maintained.

8.1.4 Special Interest Forums:

i. IS shall maintain appropriate contact with special interest groups (for example, ISACA, Pakistan Information Security Association, etc.) and other information security and data privacy forums for receiving and distributing updates on new vulnerabilities, security and continuity threats, regulations and/ or risks.

ii. IS will maintain details regarding the applicable special interest groups, contact information for these groups, the frequency and method of contact with these groups, identification of the AKU personnel who are responsible for this contact, and identification of how information derived from these groups will be integrated into the relevant information security processes/ controls.

8.1.5 Information Security in Project Management: Information security shall be incorporated into all phases of every technology project managed by AKU. The project management methods in use must require that:

i. Information security objectives and roles/responsibilities shall be defined at the onset of each project.

ii. Information security risk assessment shall be conducted at the onset of each project to identify risks and controls.

iii. Analysis of information security requirements shall be included in all phases of the SDLC.

iv. Responsibilities for information security at all phases of the SDLC must be defined and allocated to specific roles within the project management process.

8.2 Mobile Devices and Working Outside of the Office: The security of teleworking mobile devices should be defined and documented.

8.2.1 Mobile Device Risk Management: Security measures shall be defined to ensure the security of mobile devices and working off AKU premises, particularly in unprotected or high-risk areas. Users must take precautions when using mobile devices to ensure AKU business information is not compromised. Consider the risks associated with the use of mobile devices. Following minimum controls should be implemented:

i. Only approved mobile devices may be used.

ii. No “jail broken” software may be downloaded on the device.

iii. Mobile devices may never be left unattended or left on the seat or where visible in a vehicle; mobile devices should be locked in the trunk of a vehicle if left unattended.

iv. Mobile devices must never be checked in luggage.

v. Mobile devices must be secured in a hotel safe or cabled to a desk if left unattended in a hotel room.

vi. Confidential information stored in files on official mobile devices should be password protected to ensure the confidentiality of information in case of device loss or theft.

vii. Mobile device data should be backup to ensure availability of information in case of loss of the theft of the device.

viii. AKU’s proprietary and confidential data must be permanently erased by the relevant department in case a user left AKU, or the mobile device should be disposed of.

ix. Official data should not be stored on user’s personal devices.

x. The loss or theft of a mobile device should immediately be reported to Safety and Security through online incident reporting systems (AEMS) and ICT Service Desk.

8.2.2 Working Outside of the Office: The ISP shall be observed when working outside of AKU premises. Users shall follow appropriate security controls to mitigate risks associated when working outside of the office to protect AKU data that is accessed, processed, or stored while working offsite.

i. AKU information cannot be stored on any mobile device unless it is password protected and/or encrypted with approved methods.

ii. Devices configured for access to the AKU network remotely should use secure VPN connection.

iii. Users must not disclose their login details (username and/or password) to anyone under any circumstances.

9.0 Security and Human Resources: The security of AKU Human Resources (HR) shall be defined and documented.

9.1 Information Security before Beginning Employment: IS shall ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

9.1.1 Candidate Screening:

i. All new employees who will access AKU information are subject to background verification prior to being hired in accordance with relevant laws, regulations, and AKU procedures. Such background checks shall be proportionate to the job responsibilities and classifications of information to be accessed/handled.

ii. The AKU HR department is responsible for executing all background checks. All information gathered during the background check shall be handled and protected in accordance with applicable laws, regulations, and AKU procedures.

9.1.2 Information Security in Terms of Employment:

i. Information security responsibilities shall be communicated to all employees both permanent and contractual during the hiring process.

ii. Employment agreements should include the person's responsibilities for information security, including the classification and management of information assets, handling of information received from external parties, and the consequences of violating the information security policy.

iii. All employees must read the ISP and sign their understanding of the ISP and their requirement to comply with the ISP and associated standards and procedures as part of the HR onboarding process and before they are provided access to AKU systems and data.

9.2 Information Security during Employment: IS shall ensure that employees and contractors are aware of and fulfil their information security responsibilities.

9.2.1 Management Requirements for Information Security: AKU management shall require that all employees comply with the ISP and associated standards and procedures. Management responsibilities include ensuring that AKU personnel:

i. Are given access to the ISP and associated standards and procedures relevant to their position, and that they understand their information security roles and responsibilities prior to being granted access to confidential data.

ii. Are advised regarding expectations of their information security role within AKU.

iii. Are instructed on how to report information security incidents directly and anonymously.

9.2.2 Information Security Awareness and Training: Information security training and awareness shall be provided to all employees and contractors at onboarding and on a regular (but no less than annually) basis thereafter in order to create information security consciousness and a security-oriented culture within AKU. Training shall also cover updates to the ISP, standards, and procedures. Training content should include:

i. The importance of understanding and complying with the ISP and associated standards and procedures.

ii. The role of each individual in protecting and securing AKU systems and data.

iii. Updates on the threat environment and controls necessary to counter threats (clean desks, clear screens, strong passwords, and multifactor authentication etc.

iv. How to report information security incidents.

v. Contact points for IS to obtain assistance and advice.

9.2.3 Violations of Information Security Policies and Internal Investigations: Any employee or contractor that has violated the ISP or associated standards and procedures may be subject to a formal disciplinary process, which may result in disciplinary action up to and including termination of employment or contract. The disciplinary process shall be fair and take into consideration whether the violation was a first offense, whether it was intentional, whether the person had received appropriate training, and the impact of the event.

9.3 Termination and Change of Responsibilities: IS shall protect the organization's interests as part of the process of changing or terminating employment.

9.3.1 Termination, Role Changes, and Information Security Duties: HR and managers shall advise personnel of information security responsibilities that carry forward after termination or a change of position within AKU. In addition, managers should obtain from ICT the list of ICT equipment and assets given to the employee and shall ensure that all assets are returned upon termination of their employment, contract, or agreement. HR shall ensure the termination is coordinated with IS so access to AKU data and systems can be terminated.

10.0 ICT Asset Management: ICT Asset Management shall be defined and documented.

10.1 Responsibility for ICT Assets: Responsibility for ICT Asset shall be defined and documented.

10.1.1 ICT Asset Inventories: Inventories of all hardware, software (including operating systems), and data shall be developed and maintained. ICT shall own the hardware inventory and software inventory. Each inventory shall adhere to best practices and contain the required information. Inventories are particularly important for effective incident response, disaster recovery, and business continuity. Therefore, it is important that, at a minimum, the inventory should contain the name of the asset, its description, the assigned owner, the assigned custodian, the location of the asset, the type of asset (e.g., SQL database, SAP enterprise application, firewall, etc.), and its risk categorization. Hardware inventories should contain the manufacturer, product name, version or model, date acquired/retired, license information, and location.

10.1.2 Asset Ownership: All information and assets (applications and software, hardware, and operating systems) associated with information processing facilities shall be owned by a designated individual within the AKU business unit responsible for the asset. The asset owner shall be entered in the inventory. AKU employees and university members shall actively support implementation of AKU global information security policies and procedures across all university campuses. They will act in one or more specific roles when collecting, maintaining, accessing, or using institutional systems and data and must understand and fulfill the responsibilities associated with their roles.

i. Application Owners:

- The business unit executive is primarily responsible for an application. The Application Owner ensures that information used by the application is correctly classified and the application is correctly assigned a risk categorization.
- Approves and periodically reviews access to the asset.
- Ensures appropriate handling of the asset through the system development lifecycle.

ii. Data Trustees: Senior university executives with management responsibility for areas of institutional data. Data Trustees work with the CIO to ensure that the appropriate resources (staff, technical infrastructure, etc.) are available to support the data needs of the entire university. Their responsibilities include but are not limited to:

- Assigning and overseeing Data Stewards.
- Overseeing compliance with the AKU ISP.
- Determining legal and regulatory requirements for data in their areas.
- Developing, implementing, and maintaining a Business Continuity Plan for institutional data under their control.
- Promoting appropriate data use and data quality.
- Institutional data covered by this policy include but are not limited to:

Institutional Data Segment Type	Data Trustee
Research Data	Dean of Research and Graduate Studies
Teaching data and material	Provost
Administrative data	Vice President, HR
Patient care data	Vice President, Health Services

iii. Data Stewards: University officials with direct operational responsibility for one or more types of institutional data. Their responsibilities include but are not limited to:

- Develop a data access plan.
- Create and perform processes to capture and fix inconsistent or erroneous data.
- Certify data stored in University's Data Repository
- Participate in security access audits.
- Interpreting and assuring compliance with university policies and regulations regarding

the release of, responsible use of, and access to institutional data. Providing communications and education to data users on appropriate use and protection of institutional data.

iv. Data Custodian: University units or employees responsible for the operation and management of systems and servers which collect, manage, and provide access to institutional data. Their responsibilities include but are not limited to:

- Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody.
- Complying with applicable university policies.
- Maintaining Disaster Recovery plans and facilities appropriate to business needs and adequate to maintain or restart operations in the event systems or facilities are impaired, inaccessible, or destroyed.
- Managing Data User access as prescribed and authorized by appropriate Data Stewards.
- Complying with all laws, regulations, and policies applicable to the institutional data in their custody.

v. Data Users: University units or members use institutional data in the conduct of university business. Their responsibilities include but are not limited to:

- Complying with laws and regulations as well as university policies, procedures, and standards associated with the institutional data used.
- Using institutional data only as required for the conduct of university business within the scope of employment.
- Complying with safeguards prescribed by appropriate data stewards for Confidential and Highly Confidential data.
- Ensuring the appropriateness, accuracy, and timeliness of institutional data used for the conduct of university business.
- Reporting any unauthorized access, data misuse, or data quality issues to the appropriate ICT Service Desk for remediation.

10.1.3 Acceptable Use of ICT Assets:

i. All ICT assets are the data, applications and operating systems, communications networks, and hardware used in AKU operations. Acceptable use of ICT assets shall be consistent with AKU's mission of education, research, service, and patient care, and must be legal, ethical, and honest. They must be used in an acceptable and appropriate manner and in accordance with the following policy statements.

ii. All users must comply with all laws, regulations, or contractual obligations applicable to ICT

assets. If a user has any question about what may be an acceptable use of data, applications, devices, or ICT processing facilities, they should contact the ICT Support Desk or their manager for further directions.

iii. All ICT assets are the property of AKU and are intended to be used for conducting AKU operations, interacting with internal and external networks, and achieving AKU's operational goals and objectives. Only authorized use of these ICT assets is allowed.

iv. Users have no expectation of privacy with respect to the use of AKU's ICT assets.

v. Limited personal use of the ICT assets is allowed, provided such use is within the parameters of the ISP contained herein. AKU expects personal use to be reasonable and reserves the right to limit personal use with or without cause or notice at any time. Personal use may be terminated or restricted when such use:

- Conflicts with an employee's ability to perform their job.
- Puts AKU ICT systems or data at risk in any way, regardless of the degree.
- Uses large amounts of ICT resources or hinders the performance of any system.
- Does not conform to AKU's values or mission; or
- Violates any part of the ISP or associated standards or procedures.

vi. AKU does not imply or express any warranty regarding its ICT assets or suitability for use for personal purposes and is not liable for any damages, consequential or otherwise, incurred by any user when using AKU ICT assets for personal purposes.

vii. Personal use of AKU data and/or applications is strictly forbidden.

viii. Storage of personal information on AKU system or devices will be considered the property of AKU and managed as the organization sees fit. AKU is not responsible for ensuring the confidentiality of such personal information. Without notice, AKU may delete, move, copy, or remove any personal information as deemed necessary.

ix. AKU does not imply or express any warranty regarding its ICT assets or suitability for use for personal purposes and is not liable for any damages, consequential or otherwise, incurred by any user when using company ICT assets for personal purposes.

x. The following are discouraged except where necessary:

- Accessing or viewing social media sites during work hours.

xi. The following activities are strictly prohibited:

- Accessing personal email through webmail interfaces to personal email sites.
- Disguising one's identity, the identity of their account or the system(s) they use.

- Sharing passwords and any other secret authentication information.
- Using another user's credentials.
- Impersonating another user or organization.
- Unless authorized to do so, using AKUs name, logos, trademarks, service marks, or any other information that would cause others to mistake the user as acting on behalf of AKU.
- Streaming non-work-related video, radio, or music.
- Using AKU's Internet number space with their own domain.
- Accessing another's computer, device, or data without authorization.
- Reading, copying, altering, or deleting another user's data, except as allowed upon departure from the company or with permission from AKU's legal counsel.
- Copying or violating the intellectual property rights of any person or company protected by copyright, trade secret, patent, or other similar rights, without express permission. This includes copying software in violation of any software license agreement. (In the case of authorized copying of intellectual property or protected data, copies will only be made to AKU-approved equipment.)
- Installing, downloading, or distributing "pirated" software or any other software not specifically approved by AKU.
- Installing any equipment on AKU's network; installations are restricted to authorized devices/hardware and must be performed by AKU's ICT personnel.
- Obtaining files from unauthorized external networks.
- Establishing or using unauthorized external storage areas, such as Drop Box etc.
- Sending, placing, or keeping any AKU data on any unapproved personal equipment or storage devices, in personal email, or on any site or media not owned by AKU.
- Committing acts that would disrupt or interfere with the legitimate activities of other users.
- Using AKU's ICT Resources to possess, distribute, or send unlawful communications or information. Such information or communications may include, but are not limited to, threats of violence or destruction of property, obscenity, child pornography, harassment (as defined by law), discrimination, or participating or facilitating the same of others, or the furtherance of other illegal or fraudulent activities.
- Sending unsolicited email messages, including the sending of "junk mail," "phishing" or other advertised material to individuals who did not specifically request it (email spam).

- Unauthorized use of or forging of email header information.
- Creating or forwarding "chain letters," Ponzi or other pyramid schemes of any type.
- Posting identical or similar non-business-related messages to blogs or large numbers of Usenet newsgroups (newsgroup spam).
- Attempting to bypass or circumvent AKU's security safeguards.
- Attempting to degrade the performance of any AKU system.
- Accessing content inappropriate for the workplace. Such content shall include, but not be limited to:
    - Pornographic and obscene material
    - Gambling, gaming, dating sites.
    - Chat rooms.
    - Sites with violent content
    - Sites with content focused on sexual interests and activities.
    - Sites with pirated or peer-to-peer content.

xii. AKU may contact law enforcement authorities to investigate any matter at its sole discretion without notifying the user.

xiii. Users must immediately report any suspected or known violations of the ISP or associated standards, or procedures, computer performance issues or system or service weaknesses, or computer hardware or software malfunctions by contacting the ICT Service Desk. All such reports shall be documented by the ICT Service Desk.

xiv. Acceptable use of the AKU email facility includes the following:

- The AKU email system must not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
- It is strictly prohibited to use AKU emails for activities including but not limited to:
    - Using email for conducting personal business.
    - Using email for purposes of political lobbying or campaigning.
    - Violating copyright laws by inappropriately distributing protected works.

- Posing as anyone other than oneself when sending email.
- The unauthorized use of email software.
- Revealing your account password to others or allowing use of your account by others.
- Providing unauthorized information including email addresses to parties outside the University.
- Disclosure or circulation of any AKU emails outside of AKU which potentially may have a negative impact on AKU operations or reputation or cast aspersions on the integrity or character of someone employed in AKU.
- Sending or forwarding chain letters.
- Sending unsolicited messages to large groups except as required to conduct AKU business.
- Messages intended for groups of personnel, for example, congratulatory or obituary notes, should only be sent with manager approval.
- Sending or forwarding email that is likely to contain computer viruses.
- Sending or forwarding email that contains videos, audio, and presentations files greater than 35MB. Users must not forward, store or receive AKU data on non-AKU email addresses including, but not limited to, Gmail, Hotmail, and Yahoo.

10.1.4 Acceptable use of social media: Use of WhatsApp, Facebook Messenger, Hangout, Skype, or any other social media platform to share AKU's internal information including but not limited to patients, students, or employees personal, healthcare or any other sensitive information is strictly against AKU ICT policy, unless prior approvals have been granted by the CIO. Microsoft Teams is the approved and secure application for calls, chats, and for sharing of such information. This does not apply to the public information, which is usually available on AKU website and social media channels. Please refer AKU Social Media policy for details (https://one.aku.edu/communications/Pages/social-media-policy.aspx)

i. Return of ICT Assets: All AKU employees shall return all of the ICT assets provided to them upon termination of their employment.

10.2 Information Classification**:** IS shall ensure that information receives an appropriate level of protection in accordance with its importance to AKU.

10.2.1 Information Classifications:

i. AKU information assets owners are responsible for assessing information assets and assigning an information classification appropriate to its value, importance to AKU operations, sensitivity, and any legal requirements applicable to the data and risk to the organization in the event of unauthorized disclosure.

ii. They are also responsible for coordinating with IS to determine appropriate controls to protect information and develop any special user procedures or safeguards, including guidelines and/or instructions for handling, processing, or storing electronic information.

iii. AKU information assets shall be classified into one of the following four classifications:

- Public: This classification covers information that may be disclosed to the general public, whether inside or outside AKU. It covers all the information that is not classified as failing in any of the defined classes. Although security mechanisms are not needed to control disclosure and dissemination of public information, they are still required to protect this information against unauthorized modification and/or destruction of information. Examples include public web pages, course listings, marketing materials, brochures, and external job vacancy notices.

- Internal: This classification covers information that requires protection against unauthorized disclosure, modification, destruction, and use, such that the harm or loss of this data could be expected to have a slight or moderate impact on AKU business activities or reputation. Examples of Internal-use-only information include but not limited to internal memos, correspondence, and other documents whose distribution is limited as intended by the data owner. This classification applies to data that otherwise requires protection from general access by the public. Examples of internal data include personnel directories, status reports, expense reports, work instructions, internal memos, minutes of the meetings etc.

- Confidential: This classification covers sensitive information about individuals and sensitive information about AKU operations and personnel, such that the harm or loss of this data could be expected to have a serious impact on AKU operations or reputation. Such information has the potential to cause a negative impact on individuals' or the University's interests. Information receiving this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include personally identifiable information about:

    - Current and former student academic, disciplinary, and financial records.

    - Information about current, former, and prospective employees, including employment, pay, benefits data, and other personnel data.

    - Pricing lists and supply sources.

    - Internal memoranda and operational documents.

    - Certain AKU business memoranda, policies and procedures, financial documents, and academic materials.

- Highly Confidential: This classification covers AKU information, the harm or loss of which, (1) could be expected to cause exceptionally grave damage to AKU's operations or reputation, or (2) creates risk for identity theft and has the potential to cause serious damage or distress to individuals. This information includes (but is not limited to):

- National Identity Card information
- Driver's license numbers
- Medical records
- Investigations/disciplinary proceedings
- Bank details (sort code/account number)
- Credit card data (PAN/CVV2/Expiry Date/PIN)
- Passport information
- AKU strategies and plans
- Data on donors, potential donors and other AKU clients
- Financial records
- Ongoing research data / papers
- Access codes for higher risk areas
- Username, passwords, and other credentials
- Research information related to a research project or a potential or pending patent application.
- Information security data, including information about security-related incidents.

10.2.2 Labeling Information: AKU Information Owners shall ensure that information, whether in physical or electronic format, is labeled in accordance with its information classification. All Internal, Confidential, and Highly Confidential information shall be prominently labeled so the person possessing the information knows its classification and required handling. This communicates to information users the level of sensitivity and required safeguards. Additional details are provided in the Data Labeling & Handling Matrix presented further in this document.

i. Handling Information: It is the responsibility of all users to protect AKU information from unauthorized creation, access, modification, disclosure, transmission, or destruction throughout the lifetime of the data. All data must be protected and handled in a manner which safeguards and protects the confidentiality, integrity, and availability of the data. AKU shall develop and implement procedures for handling ICT assets and AKU management shall be responsible for: (1) ensuring that departmental policies and procedures are aligned with this and other Information Security Policies, Standards, and Procedures; and (2) facilitating compliance with the said departmental policies and procedures. See the Data Labeling & Handling Matrix below:

AKU Data Labeling & Handling Matrix

	Public	Internal	Confidential	Highly Confidential
Example	Schedule of Classes	Memos and minutes	Academic records	Bank Account Numbers
Access	Minimal controls to prevent unauthorized modification/ deletion	Determined by data owner	Limited based upon need to know, named users only, training and confidentiality agreement required	Provide access only when no alternative exists. Treat as toxic. Named users only, training and confidentiality agreement required
Use	Post as needed	Determined by data owner	No posting, limited reporting and copying	Use only when no alternative exists. Treat as toxic. No posting, limited reporting and copying
Transmission	Minimal controls to prevent unauthorized modification	Determined by data owner	Confidential envelope; encrypted transmission	Hand deliver; encrypted transmission
Storage	Minimal controls to prevent unauthorized modification	Determined by data owner	Locked private office or cabinets; secure server room; should encrypt on desktops, laptops, media	Locked private office or cabinets; secure server room; should encrypt on desktops, laptops, media
Destruction	No Controls	Determined by data owner	Shred paper; secure delete files, wipe media	Shred paper; secure delete files, wipe media

10.3 Handling of Media: Handling of media shall be defined and documented.

10.3.1 Removable Media: Removable media includes thumb drives, external hard drives, or any other external storage device. All removable media should be encrypted, or password protected. Data on removable media shall be removed when no longer needed on that device. ICT will wipe removable media upon request and check it for malware prior to re-use. AKU Information Owners shall ensure that:

i. Electronic information (e.g. files) stored on a removable media should be encrypted using an approved encryption method such as BitLocker etc.

ii. Where applicable, the media should be protected through a strong password applied in accordance with AKU password policy.

iii. Removable media containing Confidential or Highly Confidential data must be labeled.

iv. Removable media should be transported securely and must not be left unattended.

v. Users who are authorized to use removable media are aware of the need to safeguard AKU information in accordance with this policy. See Data Labeling and Handling Matrix above.

vi. Loss or theft of removable media containing confidential information must be immediately reported to the information owner and ICT Service Desk as an Information Security Incident.

10.3.2 Sanitization and Disposal of Media: Media containing Confidential or Highly Confidential information must be disposed of securely using documented procedures. As soon as a device is no longer needed, the user shall return it to their relevant department. Its return shall be noted in the inventory of equipment checked out to personnel. Media shall be disposed of according to documented Standards and Procedures by the disposal department. Records of media disposal should be kept.

10.3.3 Physical Transportation of Media: Media, including removable media, containing AKU Confidential or Highly Confidential data shall be encrypted and packaged appropriately to protect the asset from unauthorized access, misuse, corruption, or damage during transit. Only approved transport companies or couriers shall be used. Data on the device must be encrypted.

10.4 Application Risk Categorization**:** All applications shall be assigned an application risk categorization.

10.4.1 Assignment of Application Risk Categorization:

i. Applications shall be assigned risk categorization, taking into account business needs for sharing or restricting access to these assets and the business impacts associated with unauthorized access, theft, sabotage, or damage to them. AKU defines three levels of potential impact on the company or business units caused by a breach of security (i.e., a loss of confidentiality, integrity, or availability). The Application Owner should examine each area (confidentiality, integrity, and availability) separately and arrive at a potential impact for each, recording it as follows:

Application Criticality/Asset Value = Confidentiality + Integrity + Availability

ii. The highest impact level of the three will determine the overall risk categorization level of the application. For example, if the confidentiality impact was High, the integrity was Medium, and the availability was Low, the overall risk categorization for that particular application would be high. The following chart is useful in determining the impact level for each (confidentiality, integrity, and availability):

Risk Categorization Based Upon Potential Impact

		Confidentiality	Integrity	Availability
1	**Low**	Information can be disclosed to any individual, entity, or process.	Information can be modified by all individuals, entities, and processes.	No requirement to have continuous access to information.
2	**Medium**	Information is not public and available to a group of authorized individuals, entities, and processes.	Information can be modified by a set of authorized individuals, entities, and processes.	Short periods of information unavailability are tolerable but normally authorized individuals, entities and processes require access.
3	**High**	Information can only be disclosed to a privileged group of authorized individuals, entities, and processes.	Information can only be modified by the owner or a privileged group of authorized individuals, entities, and processes.	Information must be accessible to authorized individuals, entities, and processes at all times.

11.0 Access Control: AKU shall limit access to information and information processing facilities.

11.1 Restrictions on Access Control: Access to AKU information, equipment, networks, and network services must be authorized, managed, monitored, and controlled on the basis of business needs and security requirements.

11.1.1 Access Control Policy: The security requirements for access to AKU systems, applications, and data shall be defined and used as the basis for managing access controls. Security controls shall safeguard the confidentiality, integrity, and availability of information, including protections against unauthorized access, disclosure, misuse, or theft. Access shall be granted on the least-privilege principle of need-to-know / need-to-use basis and shall require approvals from application owners or direct managers, and in certain cases, IS. All access shall be logged and regularly reviewed. The controls and guidelines described in this policy are the minimum requirements that shall be applied to all AKU information systems:

i. Users must not share their login credentials with anyone, not even family members.

ii. Only authorized users should have physical or logical access to ICT resources.

iii. It is the shared responsibility of all information system users to prevent unauthorized access to systems at AKU.

iv. Administrators are primarily responsible for establishing, documenting, and managing access control policies and processes.

v. Users' access shall be reviewed and updated if there is any change in job function, student status, transfers, and referral privileges etc.

vi. Role-based access control should be applied to secure access to information assets.

vii. Generic user credentials or shared credentials are prohibited.

viii. It is strictly prohibited to share user access accounts even if individuals share certain responsibilities.

ix. Administrative and privileged user access shall be restricted and controlled.

x. Access to AKU information assets must be in accordance with the information classification. See the Data Labeling and Handling Matrix above to determine if a non-disclosure agreement is required.

xi. Access should only be provided to authorized and authenticated individuals.

xii. Access must be limited to specific resources, tasks, and functions only for the time period required to accomplish approved tasks. Access must be terminated upon completion of or removal from approved tasks.

xiii. Vendors are required to comply with AKU Information Security Policies, Procedures, and Standards. They must take all reasonable steps to protect AKU ICT Resources from unauthorized access, disclosure, corruption, tampering, or other damage.

xiv. It is strictly prohibited to share user access accounts even if individuals share certain responsibilities.

xv. Upon request, the vendor must be prepared to do the following:

- Identify ICT resource(s) and information to which access is required.
- Identify the business purpose for which access is required and limit access to that purpose.
- Complete AKU access logs that capture individual identity, timing, and duration of access.

xvi. Remote Access:

- Users are responsible to ensure the security of their remote access credentials/privileges and will be held accountable in case of any misuse.
- Users' personal equipment is subject to the same rules, regulations and policies that apply to AKU-owned equipment. Therefore, their machines must be configured to comply with AKU's information security policies and standards. For example, antivirus software must be up-to-date, unlicensed software must not be used etc.
- Remote access must be secured and strictly controlled. Remote access to AKU's network must be encrypted, approved by ICT management, and the employee's or contractor's supervisor and limited to the minimum set of services necessary to conduct business.

- Remote access must be secured and strictly controlled. Control must be enforced via password authentication and/or encryption with strong passphrases.

- Devices configured for remote access to the AKU must have strong authentication.

xvii. Software Applications:

- Application support personnel will have view-only access to systems/modules supported, together with access to system monitoring pages, application configurations and interfacing parameters on the live instances. To resolve system issues, access to the application may be granted on a temporary basis by the CIO. They should not have access to production systems unless in highly unusual circumstances. Test environments should be used to resolve system issues and sign off by application owner before moving fix to production.

- Developers should not have access to deploy changes or make changes to access security in the production environment. The deployment and application security privileges will remain with designated team members in the software team.

- Access to program source code is given to authorized personnel after the approval of department lead and IS.

- Version control must be maintained over source code to support recovery from prior versions. It is the responsibility of the application developer to regularly perform file check in and check out.

- Access to the production database will only be provided to the developer when the database team receives a DB-SRF (Special Request Form) approved and signed by the application owner, department head and Director Software development. Time-bound access will be provided for a specific date and access rights will be immediately revoked afterwards.

11.1.2 Access to Networks and Network Services: Only authorized users shall be provided access to the AKU networks and services in accordance with the Access Control Policy (section 9.1.1 above). All access shall adhere to the AKU ISP for access control. Any attempt to access AKU networks or network services without authorization or from a device which has not been authorized shall be deemed a violation of this Policy. Information system owners and ICT must ensure that: All access to AKU networks and network services must be via approved software, such as VPN for remote access, and provided credentials. Network services shall be monitored for compliance and unauthorized access attempts.

11.2 User Access Management: Formal Procedures that govern the lifecycle of user and administrator access must be followed to protect against unauthorized access to systems and services and control the allocation, change, and removal of access rights to ICT systems and services.

11.2.1 User Registration and De-registration: AKU shall develop and implement formal user and administrator registration and de-registration processes for granting, reviewing, and revoking access to all AKU information systems and services. Users who are leaving AKU or no longer

require access shall have their user accounts disabled and removed.

11.2.2 User Access Provisioning Process: AKU shall develop and implement formal user access provisioning process for assigning or revoking access rights to all AKU information systems. The provisioning process should include:

i. Obtaining authorization from the owner of the information system or service for the use of the information system or service.

ii. Verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties.

iii. Ensuring that access rights are not activated before authorization procedures are completed.

iv. Updating access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left AKU.

11.2.3 Privileged Access Rights: The assignment of privileged access rights on AKU information systems must be strictly controlled in accordance with established Procedures. Privileged users must have defined roles and responsibilities and adhere to defined Information Security Standards and Procedures. All privileged user activity must be logged, and segregation of duties shall be carefully observed. Privileged access rights shall include following requirements:

i. Privileged access rights associated with each system (e.g. operating system, database management system and each application) shall be identified.

ii. A record of all privileges allocated shall be maintained and reviewed at least annually.

iii. Privileged access rights must never be shared or disclosed.

iv. Any access to escrowed password should be authorized by respective ICT lead / manager. After using the escrowed password, administrative password shall be changed, and the administrator shall again secure it in a sealed envelope.

11.2.4 Secrecy of Authentication Data: There shall be a formal process for allocation and distribution of passwords and other sensitive information used for authentication. Users must keep their personal authentication information confidential and not share it with others, even supervisors or managers. Users must not write down their user ID and/or password or record them in unencrypted electronic files or documents.

11.2.5 Review of User Access Rights: A formal process should be developed and implemented for business-critical information systems to ensure that user access rights are reviewed on a regular basis. This is to ensure that the rights an individual has been granted in the past remain valid and that the user has a continued business need to retain them.

11.2.6 Termination and Changes to Access Rights: The access rights of AKU employees to information systems must be removed upon termination of employment. Upon change of a user's employment status or role (e.g. transfer, promotion, termination), owners of the AKU information systems shall be notified by AKU Human Resources with the employee's last

working date. Access privileges shall be immediately revoked or reassigned (as appropriate) upon notification.

11.3 User Responsibilities for Access: Users accountable for safeguarding their authentication information shall be defined and documented.

11.3.1 Use of Passwords and other Authentication Credentials: AKU employees are responsible for protecting their authentication information and affording appropriate protections (e.g. terminating active sessions, logging-off systems when not in use, activating screen savers, and preventing unauthorized access) of unattended equipment, and following good security practices in the creation and use of passwords in accordance with section 9.4.3 (Password Management). Do not use the same passwords for AKU and personal use.

11.4 Access Controls for System and Application: Access to systems and applications must be restricted.

11.4.1 Restrictions on Information and Application Access: AKU information systems must have access management restrictions that specify access permissions, system roles, and application functions. Application owners are responsible for developing and implementing the access control procedures, including:

i. Controlling access to application system.

ii. Types of access permissions permitted (e.g. View, Insert, Update and Delete).

iii. Mechanism for assigning roles and permissions to users.

iv. Information system access controls must be configurable so that access permissions can be modified without making code changes.

11.4.2 Secure Log-on Requirements: Access to AKU information systems must use a secure logon process and should be configured to:

i. Comply with AKU password policy in section 9.4.3 (Password Management) and application authentication requirements which minimize possible unauthorized access.

ii. Validate logon information only upon completion of all input data.

iii. Record unsuccessful logon attempts on information systems and limit the number of unsuccessful logons attempts before locking the account.

iv. Not transmit passwords in clear text over a network.

11.4.3 Password Management: Password management systems shall be interactive and shall ensure quality passwords in accordance with AKU ICT password policy.

11.4.4 Application / Database Service Accounts: All Application / Database service accounts created for software applications are exempted from AKU Password Policy. All service accounts should be approved by the respective ICT Director / Senior Manager.

11.4.5 Restrictions on Use of Privileged Utility Programs: The distribution and use of privileged utility programs must be restricted and tightly controlled. The use of such utility programs must be pursuant to corresponding Information Security Standards and Procedures. Vendor-default utilities must be disabled during new-server commissioning, as per Information Security Standards and Procedures.

11.4.6 Access to Source Code: Access to program source code of AKU information systems shall be restricted and only given to authorized personnel after the approval of the CIO. Access to source code shall be granted though a formal access request process and recorded.

12.0 Cryptography: Cryptography should be defined and documented.

12.1 Use of Cryptography:

12.1.1 Policy on Use of Cryptography:

i. Cryptographic controls shall be used to protect the confidentiality and integrity of certain data that is both stored, at rest, in-transit, and to verify software, firmware, and information integrity. Cryptographic controls are also deployed to provide authentication and non-repudiation services. Cryptographic controls must be deployed based on assessed risk and in accordance with the data classification Policy. Data residing in mobile devices or removable media devices is at higher risk of loss and must be encrypted. Cryptographic Keys must be managed in accordance with the Cryptographic Key Management Policy.

ii. AKU must have a Cryptographic Controls Standard that provides for effective, organization-wide implementation of this Policy.

iii. AKU information stored on laptops should be encrypted by appropriate encryption methods such as Windows BitLocker.

12.1.2 Cryptographic Key Management:

i. A cryptosystem is only as strong as the cryptographic keys that are used to protect data and transactions. Therefore, cryptographic keys must be protected against corruption, modification, and loss at all times.
ii. Cryptographic key management procedures shall be in place to support the use of cryptographic controls mentioned in section 10.1.1. The procedure should ensure that all keys shall be protected against modification and loss.

13.0 Physical and Environmental Security: Physical and environmental security should be defined and documented.

13.1 Physical Security: AKU physical security should prevent unauthorized physical access, damage, and interference to the AKU information.

13.1.1 Physical Perimeter Security: AKU ICT facilities shall have defined perimeters and adequate protections against unauthorized physical access, environmental threats, or damage to physical facilities, including those housing information processing. Controls shall include perimeter controls (e.g., barriers such as walls, construction requirements, locks on doors and windows,

card-controlled entry gates, manned reception desks, or physical barriers). Controls shall be defined for areas that contain information processing facilities. (Please refer to Physical and Environmental Security Standards and Procedures for further information.) Controls must adhere to AKU compliance requirements.

13.1.2 Physical Entry Controls:

i. AKU facilities must be protected by appropriate physical entry controls to protect against unauthorized access. The following controls shall be implemented. Access to facilities must be restricted to authorized personnel only.

ii. Authentication controls, e.g. access control card system, must be used to authorize and validate all access.

iii. Visitors must be escorted by authorized personnel and not left unattended.

iv. Date and time of entry and departure of visitors must be recorded.

v. Vendor support personnel may be granted restricted access only when required; their access must be authorized and monitored; and

vi. Access rights must be regularly reviewed and updated and revoked when necessary.

13.1.3 Security of Offices, Work Areas, and Facilities: AKU physical security shall be configured to prevent AKU non-public information or activities from being visible and audible from the outside. Access to ICT processing facilities or areas containing AKU sensitive data shall be restricted to authorized personnel only.

13.1.4 Protection against Environmental and External Threats: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters, malicious attacks, and accidents shall be to ensure AKU's data and systems are not interrupted, and their confidentiality, integrity, and availability are assured.

13.1.5 Working in Secure Areas: Physical protections and Procedures for working in secure areas of AKU ICT facilities shall be developed, implemented, and enforced for working in secure areas based upon the principles of need-to-use / need-to-know.

13.1.6 Location of ICT Processing, Delivery and Loading Areas: Access points where unauthorized persons may enter AKU's secured premises, such as loading docks and delivery areas, should be located away from ICT processing facilities. The movement of all incoming and outgoing computer related items shall be documented, and incoming computer items shall be inspected for potential threats.

13.2 Physical Security of ICT Equipment's: Physical security of ICT equipment shall be defined and documented.

13.2.1 Sitting and Protection of Equipment: AKU ICT shall ensure that all ICT equipment (e.g. servers, routers, firewalls, and switches etc.) shall be physically secured from physical and environmental threats or unauthorized access. Physical access to such ICT equipment and AKU

data centers must be restricted to authorized personnel only. Equipment shall be placed to avoid the risk of theft, fire, smoke, water, dust, chemical effects, vibration, or interference with the electrical supply. Eating, drinking, or smoking shall be prohibited in information processing facilities.

13.2.2 Protection of Supporting Utilities: All critical AKU ICT equipment's shall be protected from power failures and other disruptions caused by failures in supporting utilities (e.g. electricity, telecommunications, ventilation, and air conditioning). Supporting utilities shall be regularly inspected and tested and provide alarms in the event of malfunction.

13.2.3 Security of Cabling: Adequate protection shall be applied to protect power and telecommunications cabling carrying data or supporting information services from interruption, interception, or damage. Cables connecting computing equipment and other support equipment shall be structured and neatly organized.

13.2.4 Maintenance of ICT Equipment:

i. ICT equipment shall be properly maintained to ensure its continued availability and integrity. Service level agreements (SLA) should be maintained with relevant ICT vendors and service providers to ensure that maintenance activities are carried out regularly. Only authorized vendor personnel are allowed to perform maintenance on ICT equipment. All such maintenance shall be documented and inspected prior to implementation into the production environment.

ii. All onsite vendor maintenance personnel must be accompanied by ICT personnel at all times. If possible, maintenance personnel should have security background checks. In some circumstances, Confidential or Highly Confidential data on the equipment may need to be cleared of the equipment prior to maintenance. Remote maintenance of ICT assets may be performed if approved, logged, and performed in a manner that prevents unauthorized access.

13.2.5 Removal of ICT Assets while Off-AKU Premises: ICT assets (data, applications, or equipment) shall not be removed from AKU premises without prior authorization from the asset owner or direct manager. All such movement of ICT assets off premises and return to premises shall be recorded.

13.2.6 Security of ICT Assets while Off-AKU Premises: AKU personnel are responsible for protecting AKU ICT assets provided to them when authorized to remove them from AKU premises. This includes the removal of laptops, computers, phones, etc. from AKU premises. AKU equipment and data must never be left unattended in public areas, left unsecured in hotel rooms, or left visible in automobiles, trains, or planes. AKU equipment or data must never be checked in luggage; it must always be shut down and carried in person or secured in a safe. Any loss or compromise of ICT asset or data must be reported immediately. The loss or theft of any device or data or known or suspected access by any unauthorized person to the device or AKU email, data, or systems must be reported as soon as the loss or theft is noticed to the ICT Service Desk. Delays in reporting a lost or stolen device may be deemed to constitute a violation of this Policy. AKU may choose to remotely wipe data on mobile devices.

13.2.7 Secure Disposal or Re-use of ICT Equipment: AKU shall ensure that all Confidential or Highly Confidential data has been removed from a device or securely overwritten prior to

disposal or re-use of the equipment. This includes hard drives, tapes, external storage devices, etc.

13.2.8 Security of Unattended ICT Equipment: AKU staff shall ensure that unattended ICT equipment's and devices must be safeguarded by:

i. Logoff computers and other devices and terminate active sessions when finished.

ii. Lock the session with a password protected screen saver or other approved mechanism.

iii. Enable password protection on mobile devices and portable storage devices.

13.2.9 Clear Desk and Clear Screen Policy:

i. Users must secure their workspace when it cannot be monitored by authorized personnel and secure the workspace by removing data from desks when not required or at the end of each day and secure it in desks or file cabinets or a locked office. While working in the office, all Confidential and Highly Confidential documents shall be placed face down on desks when unattended for periods of thirty minutes or more. Users shall take care to immediately remove all Confidential or Highly Confidential data from printers and copiers.

ii. The clear screen policy for office equipment requires all computers and terminals to be logged off at the end of each day and an automatic password-protected screen saver or other authentication mechanism to be activated after periods of inactivity of fifteen (15) minutes. Users should also safeguard incoming and outgoing mail and ensure that Confidential and Highly Confidential documents are placed in shredding bins for disposal.

14.0 Operations Security:

14.1 Security of Information Processing Facilities: Information processing facilities shall be operated according to documented operational Standards and Procedures and assigned responsibilities.

14.1.1 Operating Procedures: ICT operating Procedures should be documented, maintained, and made available to all users who need them. While documenting operating procedures, segregation of duties shall be considered. Operating Procedures shall include:

i. System start-up and shut down.

ii. System installation and configuration and documentation of configuration.

iii. Information processing.

iv. System backup.

v. System scheduling, including interdependencies.

vi. Handling of errors or exceptional conditions.

vii. Restrictions on the use of system utilities.

viii. Support and escalation procedures.

ix. System restart and recovery.

x. System logging and audit information.

14.1.2 Change Management: Formal change management procedures should be implemented in order to ensure that all changes to information systems are documented and tested before implementation. Introduction of new systems, major and minor changes to existing systems and installing system patches shall follow the change management procedure. The following items should be included in the change management procedure:

i. Identification and recording of changes.

ii. Planning and testing of changes.

iii. Assessment of the potential impacts, including information security impacts of such changes.

iv. Formal approval for proposed changes.

v. Verification that information security requirements have been met.

vi. Communication of change details to all relevant persons.

vii. Provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident.

viii. Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

ix. Use of audit logs to record all changes.

x. Definition of roles and responsibilities within the change management process.

14.1.3 Capacity Management: ICT shall monitor the use of all ICT resources (applications, hardware, networks, and operating platforms) to ensure that ICT systems are operating efficiently and with adequate capacity to handle future requirements or surge periods. Use of resources should be monitored, tuned, and projections made of future requirements to ensure required system performance. The use of the resources shall be monitored, and projections of future capacity requirements of the existing and/or new systems shall be performed by the ICT department. Capacity planning should consider short-, medium- and long-term business requirements, business criticality of the system, and availability requirements.

14.1.4 Development, Testing and Operational Environments: The production environment shall be logically and physically separated from the development and test environments to reduce the risks of unauthorized access or changes. The Change Management process shall be followed for implementing any change to the production environment.

14.2 Protection against Malware: All AKU ICT assets must be protected from malware. Controls against malware will include Policies, Standards, and operating Procedures, training, and the deployment of security technologies, including anti-malware software for all devices and an enterprise version for the corporate system. It is the responsibility of every user to help prevent and block the introduction of malware into AKU's systems and operating environment.

14.2.1 Controls to Protect Against Malware: AKU ICT shall ensure all Internet gateways, servers, laptops, and workstations are protected against malware. Protections shall include, but not be limited to:

i. Anti-virus protection must be provided on all AKU devices including, but not limited to, servers, laptops, and other workstations in order to stay protected from computer viruses and malicious codes. Virus signatures, malicious code definitions as well as their detection and repair engines should be updated regularly and whenever necessary.

ii. Storage media and files from unknown sources or origin must not be copied or used unless checked and cleaned for computer viruses and malicious codes.

iii. Users shall not intentionally write, generate, copy, propagate, execute, or involve in introducing computer viruses or malicious codes.

iv. Checking files, email attachments and file downloads for malicious code before use.

14.3 Information Backup: To protect against loss of data regular backups of AKU ICT assets shall be taken and appropriate retention of such data maintained. Regular reviews of storage requirements shall be undertaken to ensure adequate capacity for backups.

14.3.1 Information Backup and Recovery Testing:

i. Backup and recovery procedures must be defined and documented to ensure that all AKU information is backed up at regular intervals based on the integrity and availability requirements of the data. Backups shall be monitored to confirm they are executed completely and accurately. Backups shall include all information needed to restore the complete system.

ii. Backups shall be protected accordingly based on the confidentiality risk of the data and retained in accordance with the legal, contractual, and regulatory requirements. Backups shall be tested periodically to confirm they can be used for recovery purposes in the event of a disaster or media failure. Regular reviews of storage requirements shall be undertaken to ensure adequate capacity for backups.

14.4 Logging and Monitoring: ICT activities and events shall be recorded and analyzed.

14.4.1 Event Logging: Logs must be created of user activities, exceptions, faults, and information security events. The logs may be reviewed on a regular basis to detect anomalies, unauthorized actions, potential intrusions or malware, or other incidents indicative of a security issue. All logs shall be kept for a defined period.

i. Access logs should be used to:

- Identify questionable data access.
- Investigate possible breaches.
- Respond to potential weaknesses.
- Access effectiveness of implemented security controls.

ii. Audit logging should be deployed in layers: at the network, application and back-end database level and incorporate the following:

iii. Activity logs of user activity (e.g. data insertions, revisions, or deletions) may be logged and reviewed for high-risk data elements or systems.

iv. System monitoring should be coordinated with other monitoring tools and practices including, for example, monitoring of systems performance, network traffic, and intrusion detection.

14.4.2 Security of Logs: Logs shall only be accessed by authorized personnel and must be protected against unauthorized modification, access, compromise, or destruction.

14.4.3 Administrator and Operator Logs: System administrator and system operator activities should have separate logging, review, and monitoring requirements to help ensure accountability of privileged account users. Privileged credentials shall not be used for ordinary ICT usage. The activities of system administrators, operators and other privileged user must include:

i. The time an event (e.g. success or failure) occurred.

ii. Event details including files accessed, modified, or deleted, errors and corrective action taken.

iii. The account and the identity of the privileged user involved.

iv. The systems processes involved.

14.4.4 Clock Synchronization: AKU shall confirm that the clocks of all the infrastructure devices used by AKU are synchronized to a single time source.

14.5 Controls on Software: The integrity of operational systems shall be preserved through controls on the installation of operational software.

14.5.1 Installation of Software on Operational System: Only trained and authorized personnel may install software or make changes to operational systems. This may only be performed by authorized personnel upon approval from the Application Owner. All installations of software shall be documented, and a configuration control system maintained of all implemented software. Vendor-supplied software shall be maintained at a level supported by the vendor. When software goes out of vendor support, the CIO and Application Owner must sign off on an

exception to allow the application to continue to operate.

14.5.2 Configuration of Software on Operational Systems: Only trained and authorized personnel may configure software or make changes to operating systems or software. This may only be performed by authorized personnel upon approval by the relevant and authorized team lead Change management, user access management and process/technical controls shall be employed to restrict the installation of software on operational systems.

14.6 Vulnerability Management: Technical vulnerabilities will be managed to prevent their exploiting or compromising AKU's infrastructure, operating systems, applications, and data.

14.6.1 Technical Vulnerability Management:

i. Regular vulnerability assessments of AKU information systems must be conducted to identify and evaluate vulnerabilities and the management of associated risks. Vulnerabilities which impact AKU information systems must be addressed in a timely manner to mitigate or minimize the impact on ICT operations.

ii. Exposure to vulnerabilities shall be evaluated on a regular basis. IS will develop Information Security Standards and Procedures for the management of vulnerabilities of AKU's infrastructure, systems, and applications, including mitigation of harm. Intrusion prevention and detection measures, including logging and alerting functions, may be implemented by IS. The CIO or Senior Manager, Information Security must approve the use of any network probe, scan, operating system fingerprinting, or other security vulnerability tool used on AKU's network.

iii. Response measures shall be based upon severity of the threat or vulnerability and documented in Information Security Procedures.

iv. Vulnerability scans should be run on AKU's systems periodically and critical, high, and medium vulnerabilities shall be remediated in a timely manner unless the CIO signs an exception to such remediation.

v. Patches to AKU's applications, operating systems, and hardware should be applied in a timely manner in accordance with vendor requirements or specifications. Patches shall be tested and applied as appropriate and according to AKU's change management process. Regular reviews of operating system patches will be conducted on a sample basis by ICT and/or Information Security staff at least yearly.

14.6.2 Restrictions on Installation of Software: Only software approved by ICT shall be installed on AKU's systems. The installation of all approved software shall only be performed by authorized ICT personnel.

14.7 Audit of Information Systems: The impact of ICT audits on operational systems must be minimized.

14.7.1 ICT Audit Planning: Auditing AKU information systems shall take into consideration the risks and the impacts on all the in-scope systems (e.g. potential for disruption). Audit requirements for access to systems and data should be agreed with appropriate management. The scope of technical audit tests should be agreed and controlled. Audit tests should be limited

to read-only access to in-scope systems and data.

15.0 Communications Security: ICT shall ensure the protection of information in networks and its supporting information processing facilities.

15.1 Network Security: Network security shall be managed to help ensure the protection of AKU information and systems.

15.1.1 Network Controls: AKU's networks should be maintained and controlled by suitably authorized and qualified staff to oversee its day-to-day running and to preserve its security and integrity. Network controls shall include:

i. Use appropriate tools and practices to protect AKU's networks against intrusion and misuse.

ii. Networks must be designed and configured to deliver high performance and reliability to meet the University's needs, while providing a high degree of access control and a range of privilege restrictions.

iii. Appropriately configured firewalls should be used to protect networks supporting the University's systems.

iv. Access to resources on AKU networks must be strictly controlled to prevent unauthorized access and access control procedures must provide adequate safeguards through robust identification and authentication techniques.

v. The implementation of new or upgraded software or firmware must be carefully planned and managed.

vi. Formal change control procedures should be used for all changes to critical systems or network components. All changes must be properly tested and authorized before moving to the living environment.

vii. Moves, changes and other reconfigurations of network access points must only be carried out by authorized staff according to agreed procedures.

viii. All wireless access points, including wireless routers, that are within AKU must be approved and centrally managed by ICT. The addition of new wireless access points within AKU will also be managed by ICT. Network components such as personal wireless access points that are not installed and managed by ICT are strictly prohibited, as they are a security breach and risk. Any such devices found will be removed. Furthermore, ICT personnel are not allowed to help install or support such devices procured directly by the end-users.

ix. The network infrastructure must be adequately configured and safeguarded against both physical attack and unauthorized intrusion.

15.1.2 Security of Network Services:

i. Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements wherever possible.

ii. The ability of network service providers to manage services in a secure way shall be determined and regularly monitored.

iii. The security arrangements necessary for particular services, such as security features, service levels and management requirements, shall be identified.

15.1.3 Segregation in Networks: AKU network should be segregated into separate network domains, with well-defined perimeters and internal firewalls or filtering routers. Access to the segregated areas should be strictly controlled. Wireless networks shall also be considered to determine whether authentication, encryption, and user level access controls are sufficient or whether wireless access should be treated as external connections segregated from internal networks. ICT shall develop Standards and Procedures for network segregation.

15.2 Security of Transferred information: Security of information transferred within AKU and/or with any external entity must be maintained.

15.2.1 Information Transfer Policies, Procedures and Controls: AKU ICT shall develop and maintain appropriate Standards and Procedures and controls to protect the transfer of information through digital communication facilities. Protections must be aligned with Information Classification and Risk Categorization of assets. When using communication facilities for information transfer, the following shall be taken into consideration:

i. Protecting information from interception.

ii. Protection against malware that may be transmitted through the use of electronic communication services.

iii. Protecting sensitive information that is in the form of an attachment.

iv. Encrypting information to protect confidentiality and integrity.

15.2.2 Information Transfer Agreements: Service level agreements or contracts shall address the secure transfer of business information between AKU and external parties.

15.2.3 Security of Data in Electronic Messaging: Information transmitted by electronic messages shall be protected from unauthorized access, modification, or denial of service. Correct addressing and transportation of the message shall be confirmed. Electronic signatures shall be incorporated in all electronic messages.

15.2.4 Confidentiality and Non-Disclosure Agreements:

i. Requirements for confidentiality or non-disclosure agreements (NDAs) reflect the protection that AKU information must be accorded. Such requirements shall be documented and regularly reviewed. All ICT vendors shall be required to sign a NDA, which includes a confidentiality clause that is legally enforceable, when they require access to confidential AKU information or have access to proprietary AKU information.

ii. AKU HR shall ensure that all AKU employees sign an employment contract that includes a

NDA.

16.0 System Acquisition, Development and Maintenance: System Acquisition, Development and Maintenance should be analyzed and recorded.

16.1 Security Requirements for Information Systems: Information security must be considered throughout the entire lifecycle of information systems, including services over public networks. The lifecycle of information systems includes planning and acquisition, project management, development, testing, implementation, maintenance and modification, and retirement. This is commonly referred to as the System Development Lifecycle (SDLC).

16.1.1 Security Requirements for New and Existing Systems:

i. The information security requirements shall be included in the requirements for new information systems or enhancements to existing AKU information systems. Results of the identification shall be documented and reviewed by relevant stakeholders. Information security requirements and controls shall reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security. Such requirements shall consider, among other things, authentication required, access provisions and authorization processes, training required, required protections of assets involved, logging or monitoring requirements, formal testing of acquired products, and use of public networks.

ii. Identification and management of information security requirements and associated processes shall be integrated in the early stages of information systems projects..

16.1.2 Security of Application Services over Public Networks: Information in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

16.1.3 Security of Application Services Transactions: Information involved in application service transactions shall be protected to prevent incomplete transmission, unauthorized message alteration, unauthorized disclosure, and unauthorized message duplication.

16.2 Security in Development and Support: Information security shall be designed and implemented as part of the development of information systems. All software must be developed in accordance with Information Security Policies, Standards, and Procedures. Separate development, test, and operational environments will be maintained, as appropriate, to reduce the risk of unauthorized access or changes to the production environment.

16.2.1 Secure Development Life Cycle Policy: AKU ICT shall follow secure development Standards and Procedures for both new developments and program changes in the existing systems. These shall include, among other things, security of the: (a) development environment, (b) software development, (c) design phase, (d) project milestones, (e) data and code repositories, and (f) version control. A baseline configuration of ICT systems shall be created and maintained.

16.2.2 System Change Control Management: AKU ICT shall enforce formal change control procedures in order to minimize the risk of corruption in software systems and unauthorized changes. Introduction of new systems and major changes to existing systems and installing

critical system patches shall follow change management Standards and Procedures.

16.2.3 Application Review after Operating Platform Changes: Changes to the software system operating platforms shall follow the change management process and the applications hosted on an operating platform shall be subjected to a technical security review as a part of the testing phase of the change management cycle to confirm the database and application layers hosted on the operating platform are not adversely impacted by the change.

16.2.4 Changes to Software Packages: AKU strictly controls changes to software packages. The vendor shall be consulted prior to approval of any change as and when required, and changes must be made through the change control process. The CIO and Application Owner must approve changes to vendor software.

16.2.5 Secure System Engineering Principles: AKU ICT shall ensure that principles for engineering secure software systems must be established, documented, maintained, and applied to any information system implementation efforts. The following guidelines and requirements must be considered:

i. Ensure that secure information system engineering procedures based on security engineering principles are established, documented, and applied to SDLC.

ii. Ensure that security is designed in all architecture layers: business, database, applications, and technology.

iii. Analyze new technology for security risks and review the design against known security threats and vulnerabilities.

iv. Ensure that security engineering principles are reviewed and updated regularly.

16.2.6 Secure Development Environment: The development environment shall be logically and physically segregated from the test and production environment. Also, different users shall have access to development and production environment to help ensure segregation of duties.

16.2.7 Security of Outsourced Development: I Outsourced system development shall be supervised and monitored.

16.2.8 Security Functionality Testing: AKU in-house developed systems shall be subject to security reviews to confirm that they are compliant with security requirements. Security reviews shall be performed during system development and the results of these tests shall be maintained. Furthermore, the use of security tools is recommended for conducting vulnerability assessments. If required, application source code reviews shall be conducted in order to detect functional defects and security issues.

16.2.9 System Acceptance Testing: All in-house or vendor provided applications shall be subject to user acceptance and system acceptance testing before being moved to a production environment. User acceptance testing shall be conducted by end-users and system acceptance testing shall be performed by relevant system administrators. The extent of the testing shall depend on the size, nature, and risk of the change.

16.3 Test Data: Test data must be carefully selected, anonymized, and protected.

16.3.1 Protection of Test Data: Production data shall be sanitized and masked if it is used in test or development environments. Personally identifiable information shall be anonymized, and Confidential information shall not be used for testing purposes unless a written exception is given by the CIO and Application Owner, and access controls shall be applied, transfer of the data shall be authorized and logged, and the data shall be erased immediately after testing is complete.

17.0 Supplier Relationships: ICT shall ensure the protection of the AKU assets that are accessible by suppliers.

17.1 Supplier Security: AKU ICT assets that are accessible by suppliers shall have appropriate protections. Each vendor's role in the AKU supply chain shall be identified and documented.

17.1.1 Security Policy for Outsource Providers: AKU shall identify and mandate minimum information security requirements for mitigating risks associated with ICT suppliers' access to the AKU information assets. These requirements for mitigating risks associated with supplier access to AKU information assets shall be documented and agreed with relevant suppliers.

17.1.2 Security Risks in Supplier Services: AKU shall include information security requirements that apply to information and communication technology product or service acquisition, in addition to the general information security requirements for supplier relationships.

17.1.3 Security in Supplier Agreements: Vendor information security requirements to mitigate risks associated with the services provided shall be documented and included in vendor agreements to the extent possible. Supplier agreements should include standard security provisions as jointly determined by IS, the CIO, and legal counsel. All ICT suppliers of AKU shall be bound by confidentiality and non-disclosure provisions that obligate suppliers to maintain the confidentiality of AKU information.

18.0 Information Security Incident Management: Information Security Incident Management shall be defined and documented.

18.1 Incident Management and Post-Event Analysis: Cyber incidents should be managed consistently and effectively, including communication regarding events and weaknesses, to protect AKU data, systems, processes, operations, and reputation. Incident response plans must be developed, maintained, managed, and tested. Incident response plans should adhere to and incorporate where necessary Information Security Standards and Procedures.

18.1.1 Responsibilities and Procedures for Incident Management: Responsibilities and procedures should be established to manage quick, effective and orderly responses to information security incidents.

18.1.2 All employees shall report information security events that might have an adverse impact on the security of AKU's information assets to the IT Service Desk immediately.

18.1.3 Reporting Information Security Weaknesses: All AKU employees shall be required to note and report any observed or suspected information security weaknesses in AKU information

systems or services.

18.1.4 Assessment and Decision-making: Information security events shall be assessed and classified by Information Security. If any particular event is classified as an information security incident, then it shall be dealt with accordingly.

18.1.5 Incident Response: Information security incidents shall be responded to in accordance with the documented and approved incident response plan and procedures. Incidents shall be identified and prioritized.

18.1.6 Post-Event Analysis: A post-event analysis shall be performed after security incidents are resolved to reduce the likelihood or impact of future incidents. For serious incidents, impacted stakeholders shall participate in the analysis. All post-event analysis shall follow established procedure. The Incident Response Plan and Procedures shall be updated to incorporate lessons learned if required. Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.

18.1.7 Collection of Evidence: IS shall develop and maintain formal procedures for the collection, handling, storage, and preservation of information to help ensure that the evidence is acceptable for evidentiary purposes and admission in court, if needed. Such procedures shall consider chain of custody, security of evidence, safety of personnel, roles and responsibilities of personnel involved and competency requirements, and documentation.

19.0 Information Security Aspects of Business Continuity: Information security continuity should be embedded in the AKU business continuity management systems.

19.1 Continuity of Information Security: Information security continuity should be integrated in AKU's business continuity plans and procedures.

19.1.1 Information Security Continuity Requirements: AKU shall determine its requirements for information security and the continuity of information security management in a crisis, disaster, or other adverse situations. Information security requirements must be determined when planning for business continuity and disaster recovery.

19.1.2 Implementing Information Security Continuity: AKU shall establish and maintain procedures and controls to ensure the required level of continuity for information security during an adverse situation. Following guidelines and requirements shall be considered:

i. Information security controls within business continuity or disaster recovery processes, procedures and supporting systems.

ii. Procedures and implementation changes to maintain existing information security controls during an adverse situation.

iii. Compensating controls for information security controls that cannot be maintained during an adverse situation.

19.1.3 Verification of Information Continuity Controls: AKU shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that

they are valid and effective during adverse situations. Following guidelines and requirements shall be considered:

i. Testing the effectiveness of information security continuity processes and controls to ensure that they are consistent with the information security continuity objectives.

ii. Reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

19.2 Redundancies: Information processing facilities must be able to ensure availability of ICT services and operations.

19.2.1 Redundancy Sufficient for Continuity: Information processing facilities shall be implemented with redundancies sufficient to meet business continuity requirements. Where applicable, redundant systems shall be implemented to help ensure continuity of ICT services.

20.0 Compliance:

20.1 Information Security Compliance Requirements: Requirements for contractual obligations related to information security shall be defined and documented to help avoid breaches of legal, regulatory, and contractual security obligations.

20.1.1 Identification of Security Compliance Requirements: Where applicable, AKU shall ensure that statutory, regulatory, policy and contractual requirements of each information system is identified, documented, and maintained before commencing a system development, authorizing the system to be operational, or a major enhancement initiative.

20.1.2 Protection of Intellectual Property Rights: Controls shall be implemented to ensure compliance related to intellectual property rights and proprietary software licensing by:

i. Acquiring software from reputable vendors.

ii. Maintaining proof and evidence of ownership or right to use.

iii. Carrying out checks to verify that only authorized software and licensed products are installed.

iv. Adhering to license terms and conditions.

v. Detecting and removing unlicensed software.

vi. Ensuring intellectual property, licensed software and information are removed from digital media prior to disposition.

20.1.3 Protection and Retention of Data: AKU data shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release. Controls should be established on the retention, storage, handling and disposal of digital records and information.

20.1.4 Protection of Personally Identifiable Information: Privacy and protection of personally identifiable information shall be confirmed as required.

20.2 Information Security Reviews: Information security shall be implemented in daily operations in accordance with Information Security Policies, Standards, and Procedures.

20.2.1 Independent Reviews: Independent reviews shall be conducted regularly or when significant changes occur to assess the effectiveness of the organization's approach to managing information security and its implementation. Such reviews may be conducted by internal personnel, such as internal audits, or outside experts. The results of the review must be documented, and any noted gaps or deficiencies should be remediated in a timely manner.

20.2.2 Compliance with Information Security Policies and Standards:

i. Compliance with AKU Information Security Policies is mandatory. Any violation of these Policies may be grounds for disciplinary action as per HR policy, up to and including termination or expulsion. All AKU faculty and managers shall ensure that information security policies, procedures and standards are effectively followed in their areas of responsibility and facilitate regular reviews of operations to ensure compliance.

ii. In certain cases, compliance with specific Policy requirements may not be immediately possible or an exception may be warranted for specific circumstances. Reasons include, but are not limited to:

- Required software or other software in use is not currently able to support the required features or functions of the application.

- The cost for reasonable compliance is disproportionate relative to the potential damage.

20.2.3 Technical Compliance Review: AKU Information systems should be regularly reviewed. AKU information systems shall be periodically tested for technical control compliance using automated tools to:

i. Conduct vulnerability assessments and/or penetration testing.

ii. Detect network intrusion.

iii. Determine if information system patches have been applied;

iv. Confirm that technical controls have been implemented and are functioning as intended.

21.0 Compliance Reference: ISO/IEC 27001:2013 Standard.

22.0 Measures of Compliance: Compliance with this policy will be verified through internal and external audits.

23.0 Related Institutional Documents: N/A

24.0 Annexures: N/A

25.0 Author(s):

Name	Designation
Suneel Kumar Panjwani	Head of Information Security
Saad Ameen	Information Security Specialist
Atif Ali	Information Security Analyst
Samra Sabir	Information Security Analyst

26.0 Key Searchable Terms: CIO, ICT, Global Information Security, Policy Statement, Scope, Purpose.

27.0 Revision History: This policy is subject to review and revision every two (2) years to ensure its effectiveness and alignment with changing organizational requirements and regulatory obligations.

28.0 Documents Change Record:

Review #	Review Date (dd-mm-yyyy)	Description Of Change	Identification of Change
1	2 April 2018	Draft policy documented for review.	All Format
2	4 August 2018	Final policy published on AKU Portal.	All Format
3	March 2022	New section added "Acceptable use of social media" (8.1.4)	All Format
4	June 2023	Review and Approval section updated.	All Format
5	24-May-24	Reviewed and updated the document in accordance with the latest policy document template.	-