الجامعة الأمريكية بالبحرين AMERICAN UNIVERSITY OF BAHRAIN

Policies and Procedures

Policy Title	ICT Policy	Policy Number	230
Section	Financial Affairs and Administrative Services	Approval Date	3 September 2024
Subsection	Information Technology and Security	Authorizing Entity	BoD
Responsible Office	ICT Department	Effective Date	10 September 2024
Distributed To	All AUBH staff and Faculty	Next Review Date	3 September 2026

TABLE OF CONTENTS

1.0 PURPOSE

The purpose of the American University of Bahrain's ("AUBH" or the "University") ICT Policy (the "Policy") is to define and standardize the management, security, and usage of information technology resources across the University. These policies provide the framework for:

- Ensuring the confidentiality, integrity, and availability of AUBH's information assets.
- Guiding the proper implementation of information technology tools and systems.
- Clarifying the roles and responsibilities of all stakeholders, including staff, students, and third-party vendors, in the secure and efficient use of IT resources.

The Policy aims to safeguard the University's digital and technological infrastructure from potential risks and threats, while promoting a culture of security awareness and compliance with applicable laws and regulations.

This policy applies to all AUBH stakeholders, including full-time and temporary staff and faculty ("Employees" or "Employee"), students, contractors, consultants, and vendors.

This policy does not stand in isolation and must be implemented in conjunction with other AUBH policies.

2.0 ABBREVIATIONS

AUBH	American University of Bahrain
CIA	Confidentiality, Integrity, Availability
CSP	Cloud Service Provider
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial of Service
DoS	Denial of Service
ETL	Extraction, Transformation, and Loading
GDPR	General Data Protection Regulation
HR	Human Resources
HTTPS	Hyper Text Transfer Protocol Secured
IaaS	Infrastructure as a Service
IAO	Information Assert Owner

ICT	Information and Communications Technology
IRT	Incident Response Team
IT	Information Technology
LAN	Local Area Network
MFA	Multi-Factor Authentication
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PDPL	Personal Data Protection Law
SaaS	Software as a Service
SCCM	System Center Configuration Manager
SDLC	Software Development Life Cycle
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secured Shell
UPS	Uninterrupted Power Supply
VPN	Virtual Private Network

3.0 DEFINITIONS

Accessibility: Accessibility concerns the ease of locating, retrieving, and using the data. Accessible data is readily available to authorized users promptly, without unnecessary barriers or restrictions.

Accuracy: Data accuracy refers to how closely the data values reflect the true values they are supposed to represent. Inaccurate data can result from errors during data entry, processing, or integration.

Business Continuity (BC): Refers to an organization's ability to maintain essential functions and operations during and after a disruptive event, ensuring the continued delivery of products and services to customers. It encompasses the processes, strategies, and plans put in place to identify potential threats and risks to the organization, develop resilience measures, and effectively respond to and recover from disruptions.

Cloud Service Provider (CSP): A cloud service provider is a company or organization that offers cloud computing services and solutions to individuals, businesses, and other entities over the Internet.

Completeness: Completeness measures whether all the required data is present. Missing data can lead to biased analyses and incorrect conclusions. Ensuring completeness involves verifying that all necessary data points are collected and recorded.

Confidentiality, Integrity, Availability (CIA): In the realm of information security, confidentiality, integrity, and availability are the three fundamental principles used to evaluate and ensure the security of information assets. They are defined as follows:

- **Confidentiality:** Confidentiality refers to the assurance that information is only accessible to those who are authorized to view or use it. It involves preventing unauthorized access, disclosure, or exposure of sensitive information to individuals or entities who are not supposed to have access to it. Measures such as encryption, access controls, and data classification are commonly employed to maintain confidentiality.
- **Integrity:** Integrity concerns the accuracy, reliability, and trustworthiness of information and its handling throughout its lifecycle. It ensures that data remains intact, unaltered, and consistent, both in storage and during transmission or processing. Protecting data integrity involves preventing unauthorized modifications, deletions, or tampering with information. Techniques such as data validation, checksums, digital signatures, and access controls are used to maintain data integrity.
- **Availability:** Availability refers to ensuring that information and resources are accessible and usable when needed by authorized users. This involves preventing or mitigating disruptions, downtime, or unavailability of systems, networks, or services due to various factors such as hardware failures, software errors, natural disasters, or malicious attacks. Redundancy, backup systems, disaster recovery planning, and robust infrastructure design are strategies employed to maintain availability and minimize service interruptions.

Conformity: Conformity measures how well the data adheres to standard formats, structures, and definitions. Conforming to established data standards facilitates interoperability, data exchange, and integration across systems.

Consistency: Consistency refers to the uniformity and coherence of data across different sources or over time. Inconsistent data may arise from discrepancies in data formats, units of measurement, or naming conventions.

Cross-site Request Forgery (CSRF): Cross-site request Forgery (CSRF) is a type of malicious exploit where an attacker tricks a user into unknowingly executing unauthorized actions on a web application in which the user is authenticated.

Cyber: A prefix used to describe things related to computers, information technology, virtual reality, and the internet. It often pertains to electronic communication networks and interactive systems, emphasizing the digital and networked aspects of these environments.

Cyber Attacks: Malicious attempts to access, alter, steal, or destroy data, disrupt digital operations, or harm information systems through unauthorized digital means.

Cybersecurity: The protection of digital systems, networks, and data from unauthorized access, attacks, or damage. It involves implementing technologies and practices to secure information and ensure system integrity and availability.

Cyber Resilience: An organization's ability to continuously deliver the intended outcomes despite adverse cyber events. It encompasses the ability to prepare for, respond to, and recover from cyber-attacks, ensuring the preservation of business operations, data integrity, and service availability under various conditions.

Data Breach: Unauthorized access, disclosure, or acquisition of sensitive or confidential information.

Data Governance: Data governance is a set of processes, policies, standards, and practices that ensure the effective and responsible management of an organization's data assets throughout its lifecycle. It encompasses the strategies and frameworks put in place to ensure that data is accurate, consistent, secure, accessible, and compliant with relevant regulations and policies.

Data Subject: The person or individual subject of the data.

Denial of Service (DoS): Denial of Service (DoS) is a type of cyber-attack aimed at disrupting or preventing legitimate users from accessing a service, network, website, or system. In a DoS attack, the attacker floods the target with a high volume of malicious traffic, overwhelming its resources such as bandwidth, memory, or processing power. As a result, the target becomes slow, unresponsive, or completely inaccessible to legitimate users, effectively denying them access to the service or resource.

Disaster Recovery (DR): Refers to the process, policies, and procedures an organization employs to recover and restore its critical IT infrastructure and operations after a natural or man-made disaster. Disaster recovery aims to minimize downtime, data loss, and disruptions to normal business activities, ensuring continuity and resilience in the face of adverse events.

Distributed Denial of Service (DDoS): A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. Unlike a traditional Denial of Service (DoS) attack, which is typically carried out from a single source, a DDoS attack involves multiple sources, often distributed across various geographic locations. These sources are usually compromised computers, servers, or other internet-connected devices that are part of a botnet controlled by the attacker.

Firewall: A firewall is a network security device or software application that monitors and controls incoming and outgoing network traffic based on predetermined security rules

IaaS: Infrastructure as a Service (IaaS) is a cloud computing model that provides virtualized computing resources over the internet. In an IaaS model, instead of owning physical servers, storage, networking, and other infrastructure components, users rent or lease these resources from a cloud service provider on a pay-as-you-go basis.

Incident Management: Phases definition:

- **Preparation:** Preparation involves activities and measures taken proactively to prepare an organization for potential incidents or emergencies. This includes developing plans, procedures, and resources, conducting training and drills, implementing security measures, and establishing communication channels to ensure readiness to respond effectively to incidents when they occur.
- **Identification:** Identification refers to the process of recognizing and acknowledging that an incident or problem has occurred. This includes detecting abnormal activities, anomalies, or indicators of compromise within an organization's systems, networks, or operations through various monitoring and detection mechanisms.
- **Assessment:** Assessment involves evaluating the nature, scope, and impact of the identified incident. This includes analyzing available information, gathering evidence, determining the severity and potential consequences of the incident, and assessing the risks posed to the organization's assets, operations, and stakeholders.
- **Containment:** Containment focuses on mitigating the immediate impact and spread of the incident to prevent further harm or damage. This may involve isolating affected systems or networks, blocking malicious activities, shutting down compromised services, or implementing temporary controls to limit the incident's reach while maintaining essential functions.
- **Eradication:** Eradication entails removing the root cause of the incident from the affected systems or environment. This involves thoroughly investigating the incident, identifying the underlying vulnerabilities or weaknesses exploited by attackers, and implementing permanent fixes, patches, or countermeasures to eliminate the threat and prevent recurrence.
- **Recovery:** Recovery involves restoring affected systems, data, and operations to a normal and functional state following an incident. This includes restoring backups, repairing, or replacing compromised assets, reconfiguring systems, and verifying the integrity and availability of critical resources to resume normal business operations as quickly as possible.
- **Follow-up:** Follow-up encompasses reviewing and analyzing the incident response process to identify lessons learned, strengths, weaknesses, and areas for improvement. This includes conducting post-incident reviews, documenting findings, updating policies and procedures, enhancing security controls, and implementing corrective actions to better prepare for and respond to future incidents effectively.

Information Assets: An information asset refers to any valuable piece of information or data that an organization owns, manages, or relies on to achieve its objectives and support its operations. Information assets can encompass a wide range of digital or physical data, including documents, databases, intellectual property, customer records, financial data, trade secrets, software, and proprietary algorithms.

Information Asset Owner: An Information Asset Owner (IAO) is an individual or role within an organization who holds responsibility and accountability for a specific information asset or a group of related information assets throughout their lifecycle.

Information Security Incident: An information security incident refers to any unauthorized or unexpected event that compromises the confidentiality, integrity, or availability of information assets within an organization. These incidents can involve the theft, loss, or exposure of sensitive data, as well as intentional or unintentional disruptions to information systems or networks.

IT Administrators: IT personnel who are responsible for installing and configuring hardware/software, monitoring system performance, and providing system support to the Users.

IT Assets: IT assets include:

- All IT infrastructure equipment (servers, server operating systems, etc.).
- All networking devices (switches, routers, network management systems, etc.).
- All security systems (firewalls, cameras, access control systems, security management systems, etc.).
- All client applications, software, cloud applications, and end-user computing.
- All end-user devices (desktops, docking stations, laptops, smartphones, tablets, printers, monitors, portal storage devices, and any other peripheral

IT Assets End Users: AUBH students, staff, faculty, and other associates of the University who request or hold IT Assets owned by the University.

IT Asset Owner: is AUBH

IT Asset Custodian: is the ICT Department.

Metadata: Metadata is the data providing information about one or more aspects of the data; it is used to summarize basic information about data that can make tracking and working with specific data easier.

Multi-Factor Authentication (MFA): It's a security mechanism that requires users to provide multiple forms of verification to access a system, application, or online service. MFA adds an extra layer of security beyond traditional username and password authentication by requiring additional factors to prove the user's identity.

Non-Disclosure Agreement (NDA): A legally binding contract that establishes a confidential relationship. The parties agree not to disclose information covered by the agreement. NDAs are used to protect sensitive information and trade secrets by specifying what information is confidential and cannot be shared outside the agreement.

PaaS: Platform as a Service (PaaS) is a cloud computing model that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the underlying infrastructure.

Personal Data: any information in any form concerning an identified individual, or an individual who can, directly or indirectly, be identified by reference to his or her personal identification number, or by reference to one or more factors specific to his or her physical, physiological, intellectual, cultural, economic, or social identity. In determining whether an individual is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

Precision: Precision refers to the level of detail or granularity present in the data. Highly precise data provides accurate and specific information, enabling more nuanced analysis and decision-making.

Privileged access: Privileged access refers to the level of access granted to users, accounts, or processes within a computer system, network, or application that allows them to perform actions or access resources beyond what regular users can.

Reliability: Reliability shows the trustworthiness and consistency of the data. Reliable data can be depended upon to produce consistent results and support reliable insights and decisions.

SaaS: Software as a Service (SaaS) is a cloud computing model that delivers software applications over the internet as a service. In the SaaS model, software vendors host and maintain the software application and infrastructure, making it accessible to users via a web browser or application interface, typically on a subscription basis.

Secured Software Development: The practice of incorporating security principles and measures throughout the software development lifecycle to prevent vulnerabilities and mitigate potential risks. This approach ensures that software is designed, implemented, and maintained with robust security features to protect against unauthorized access, breaches, and other cyber threats.

Secure Shell (SSH): A cryptographic network protocol that enables secure communication and data exchange over unsecured networks. SSH provides a secure channel for accessing and managing remote systems and devices, allowing users to securely log in to remote machines, execute commands, transfer files, and perform other network-related tasks.

Security Perimeter: A physical or logical boundary that is defined for a system, domain, or enclave; within which a particular security policy or security architecture is applied.

Simple Mail Transfer Protocol (SMTP): A communication protocol used for sending and receiving email messages between email servers.

Timeliness: Timeliness reflects how up to date the data is at the time of its relevance. Outdated data may lose its value or accuracy over time, particularly in dynamic environments where information changes rapidly.

Validity: Validity assesses whether the data conforms to the defined rules and constraints. Valid data adheres to predefined standards and business rules, ensuring its relevance and applicability to the intended purpose.

Virtual Private Network (VPN): A technology that establishes a secure and encrypted connection over a public network, such as the Internet, allowing users to transmit data between their device and a remote server or network as if they were directly connected to it.

4.0 ROLES AND RESPONSIBILITIES

ROLE NAME	RESPONSIBILITIES
AUBH Stakeholders	• Promptly report any IT security incidents or breaches to the ICT Department.
Data Owners	• Implement and enforce the university's data governance policies. • Classify data based on sensitivity and criticality, manage metadata, and ensure compliance with data protection standards.
Data Processors	• Process data in accordance with university policies, ensuring its integrity, confidentiality, and availability.
Data Protection Officer	• Oversee data compliance according to the PDPL and other relevant regulations. • Coordinate data protection training and awareness programs.
HR Department	• Support the conduct of mandatory information security training and manage related HR issues for IT policy breaches.
ICT Department	• Maintain IT asset registers, manage IT asset lifecycle, facilitate IT security training, and oversee the implementation of IT policies and procedures.
Information Asset Owner	• Establish and enforce security policies for information assets. • Approve access levels, manage data replication, and develop outsourcing risk strategies.
Information Security Officer	• Ensure the secure development and maintenance of software systems. • Assess and manage information security risks and oversee vendor compliance. • Review implementation of the controls as per policies relevant.
Information Asset Users	• Maintain the security and confidentiality of data within their control. • Comply with all relevant information security policies.
Incident Response Team	• Manage and respond to IT security incidents in accordance with established protocols.
IT Assets End Users	• Safeguard assigned IT Assets and comply with IT policies and acceptable use guidelines. • Ensure no unauthorized software installations and report any IT security concerns immediately.
IT Head	• Oversee the implementation of the ICT Policy across all departments. • Manage and review firewall configurations and other critical system settings to ensure security and functionality. • Lead the ICT Department in strategic planning and execution of IT initiatives.
Procurement Team	• Develop contracts that include information security clauses and oversee the procurement of IT assets in line with university policies.

Vice President of Finance and Administration (VPFA)	• Provide final approval on ICT-related financial decisions, including budgeting and expenditures. • Approve major policy changes and strategic decisions within the ICT Department. • Oversee procurement processes to ensure alignment with the university's financial and strategic objectives.

5.0 INFORMATION ASSETS CLASSIFICATION AND MANAGEMENT POLICY

5.1 Purpose

The purpose of Information Asset Classification and Management Policy is to systematically categorize and manage AUBH Information Assets based on their sensitivity, criticality, and value. This policy helps ensure that appropriate security controls and protection measures are applied to safeguard these assets effectively throughout their lifecycle. The key purposes this policy include:

- Risk Management: Asset classification enables the identification and prioritization of information assets based on the potential risks associated with their loss, unauthorized access, disclosure, or alteration.
- Data Protection: Classification helps apply appropriate levels of protection to different types of information based on their sensitivity and regulatory requirements. Assets are classified as Public, Private (internal use), and Confidential, with corresponding security controls and access restrictions applied accordingly.
- Compliance Requirements: Asset classification assists organizations in meeting regulatory compliance requirements by ensuring that sensitive information is handled and protected according to relevant laws, regulations, industry standards, and contractual obligations.
- Access Control: Classification facilitates the implementation of access controls based on the principle of least privilege, ensuring that individuals have access only to the information necessary for their roles and responsibilities.
- Incident Response: Asset classification guides incident response efforts by helping prioritize and respond effectively to security incidents based on the impact and criticality of affected assets.
- Business Continuity and Disaster Recovery: Asset classification informs business continuity and disaster recovery planning by identifying critical assets and systems essential for business operations.

5.2 Policy

5.2.1 The ICT Department must identify Information Asset Owners and ensure the maintenance of appropriate controls.

5.2.2 Responsibility for implementing and managing controls may be delegated; however, accountability must remain with the nominated Information Asset Owner.

5.2.3 Depending on the classification of Information Assets, electronic transmission, copying, or distribution shall require prior approval from identified authorities.

5.2.4 Following the classification of assets, confidential information must be stored with proper security measures.

5.2.5 Appropriate access restrictions shall be applied to prevent unauthorized personnel from accessing Information Assets.

5.2.6 A formal record of authorized recipients of data shall be maintained.

5.2.7 The distribution of data shall be based on the principles of "need to know" and "need to use."

5.2.8 Distribution lists and lists of authorized recipients shall be reviewed at regular intervals.

5.2.9 A process and procedure for recording, maintaining, and updating the inventory of all Information Assets (i.e., information asset register) owned and managed by AUBH shall be maintained.

5.2.10 The inventory shall be categorized into various types such as hardware, software, information, etc. All Information Assets should be cataloged, capturing at minimum the following details:

- Source of Information Asset
- Use of Information Asset
- Business process dependent on Information Asset
- Users/group of users of Information Asset

5.2.11 Information Asset classification shall be done based on three principles of security:

1) Confidentiality
2) Integrity
3) Availability

5.2.12 All Information Assets should be classified as public, private, or confidential following the guidance below:

- Public Information: information accessible under the Freedom of Information Law and available to any person, regardless of individual status or interest.
- Private Information: information not publicly available but can be disclosed or used by AUBH's representatives to carry out their duties if no legal prohibition to disclosure exists.
- Confidential Information: information whose disclosure would cause harm to AUBH or is protected by law or Company Authority.

5.2.13 All Information Assets and outputs from systems handling classified data should consider labeling in terms of sensitivity and include the following aspects:

- Classification of Information Assets may cease to be sensitive or critical after a certain period.
- Over-classification can lead to unnecessary additional business expenses.
- Overly complex schemes may become cumbersome and impractical.
- Care should be taken in interpreting classification labels on documents, which may have different definitions for the same or similarly named labels.

5.2.14 The Information Asset Owner shall be responsible for defining the classification, i.e., for a document, data record, data file, or data storage. The classification shall be periodically reviewed.

5.2.15 Maintenance of Information Assets:

- All Information Assets shall be properly maintained to ensure high availability and performance.
- All preventive maintenance shall be recorded and follow proper change management procedures.

5.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2022	5.9 Inventory of information and other associated assets
ISO 27001:2022	5.12 Classification of Information
ISO 27001:2022	5.13 Labelling of Information
ISO 27001:2022	5.18 Access Rights

6.0 IT ASSETS CLASSIFICATION AND MANAGEMENT POLICY

6.1 Purpose

The purpose of the IT Asset Management Policy is to provide a comprehensive framework for the effective management and utilization of AUBH IT Assets from procurement through to disposal. This policy outlines the responsibilities necessary for its implementation, ensuring:

- The maintenance of an up-to-date and accurate inventory of all IT assets procured and owned by AUBH, coupled with robust tracking of ownership, custody, and usability.
- The systematic management of the IT Asset lifecycle, including the retirement process for assets at the end of their usability lifespan, when they no longer meet the business and IT infrastructure operational requirements, or in cases of permanent damage.

This policy aims to apply appropriate security controls and protection measures to safeguard these assets effectively throughout their lifecycle. Please also refer to 8.0 Acceptable Usage Policy.

This policy applies to all IT Assets owned by AUBH, including IT Assets procured from an external vendor as well as IT Assets that are assembled or built using AUBH available resources.

6.2 Policy

6.2.1 All IT Assets purchased by the University are the property of AUBH and will be deployed and utilized in a way that is deemed most effective and objectively demonstrates value for money.

6.2.2 On behalf of the University, the ICT Department will manage a centralized IT budget. The procurement of IT Assets will follow the policies and procedures of the University related to Procurement. The ICT Department:

- Is responsible for engaging the Procurement Team for the purchase of IT Assets.
- May assist the Procurement Team in identifying potential suppliers for IT Assets.
- Will not, without adequate and suitable further justification, approve or proceed with the procurement of IT Assets that do not comply with the approved IT budget and the University's

strategic and operational plans. Exceptional approval shall be requested through the VP of Finance and Administration and be in line with the Delegation of Authority Policy.

6.2.3 The ICT Department, with the approval of the VP Finance and Administration, will establish an IT Asset standard distribution list, which outlines the type of IT Assets that can be assigned to different Employee roles.

6.2.4 For compatibility and efficiency reasons, IT Assets will be issued on a 'fit-for-purpose' basis based on predefined End User roles, IT Asset standard distribution list, and approved software list.

- Enquiries and requests for IT Assets must be submitted to the ICT Department via the IT helpdesk system.
- Requests that do not agree with the IT Asset standard distribution list require the End User's manager's approval and will be assessed and approved by the head of IT and VP of Finance & Administration and will be subject to budget availability.
- Specialized or differentiated IT Assets for IT Assets End Users with disabilities will be catered for on a case-by-case basis in a reasonable manner.
- The ICT Department will assess requests for new and replacement of IT Assets and fulfill them in accordance with the approved IT Asset standard distribution list, aiming to reissue assets held in AUBH store.
- Requests for non-standard, specialized, or non-budgeted for IT Assets will be assessed by the ICT Department and processed, with business justification provided by the End User, through the appropriate approval channels. The request will be processed if budget permits and with valid business justification; otherwise, it will be added to the ICT Department budget for the following financial year. The ICT Department may request through the VP of Finance and Administration, an overspend approval, as per the limits and authorities set in the Delegation of Authority, if the request is time-sensitive and has a valid business justification.

6.2.5 All IT Assets purchased will be registered in the IT Assets register maintained by the ICT Department. The Finance Department will maintain separate register(s) in accordance with the Finance and Accounting Policy. The IT Assets, eligible for tagging as per the Finance and Account Policy, will be tagged once they have been assessed, tested, and procured following the agreed procedures, and before being issued or put into use. The registers will contain information about the IT Assets necessary to enable them to be tracked, managed, and audited throughout their entire lifecycle.

6.2.6 All IT Assets must be assigned to individual IT Assets End Users who will be held responsible for their care and security whether they are in use, storage, or movement. Individual IT Assets End Users will be held responsible for protecting the IT Assets that have been assigned to them against physical or financial loss whether by theft, mishandling, or accidental damage and they will be held accountable for any misuse or damage to the assigned IT Assets.

6.2.7 IT Assets End Users are not allowed to install unapproved software on devices. Requests should be made to the ICT Department to have additional software that is not on the approved software list installed on a device. Any software installed must be legitimately acquired and licensed for its use.

6.2.8 All IT Assets that are no longer in use must be returned to the ICT Department for redeployment. This includes IT Assets purchased using departmental or research funds.

6.2.9 To ensure the confidentiality of information, any IT Asset that has been used to process or store personal or sensitive information will be wiped before being reissued and must go through a physical disposal and destruction process at the end of its useful life. IT Assets End Users are required to keep all organizational data safe under their AUBH account OneDrive, AUBH SharePoint site, or under the purpose fit platform approved by the ICT Department.

6.2.10 The ICT Department is accountable for the implementation of this policy and on a day-to-day basis. The ICT Department will be responsible for:

- Implementing an adequate procedure to distribute IT Assets ensuring IT Assets End Users confirm receiving and returning IT Assets in writing and update the IT Assets Register accordingly.
- Adequately administering and maintaining the IT Assets to ensure they remain fit for purpose and compliant with the licensed conditions of use during their entire lifecycle.
- Updating and maintaining the accuracy of the IT Asset register and informing the Finance Department on a monthly basis of any changes.
- Ensuring that all IT Assets are processed and tagged before they are issued to IT Assets End Users or entered into the store.
- Checking equipment is returned in the same configuration as expected and signing receipts upon collection from IT Assets End Users.
- Administrating the control and security of equipment held in stock for issuing and awaiting reissue or disposal.
- Reporting any incorrect disposal or misuse of an IT Asset to the Vice President of Finance & Administration as soon as possible.
- Conducting an annual IT Asset audit activity to support the annual fixed assets verification process and report carried out by the Finance Department.

6.2.11 IT Assets End Users issued with IT Assets will be responsible for:

- Retaining responsibility for IT Assets issued to them until they have been returned to the ICT Department for redeployment or disposal.
- Ensuring that IT Assets are not moved to another location (if fixed) or transferred to another person without the consent of the ICT Department.
- Contacting the ICT Department if they need to move, reassign, or return IT Assets.
- Reporting the loss or theft of IT Assets immediately to the ICT Department or through the University security team.
- Reporting any defects and immediately returning equipment that is not operating normally to the ICT Department.
- Returning all IT Assets to the ICT Department upon replacement, when they are no longer required for University business or when the holder leaves the University.

6.2.12 The management of IT Assets must comply with this policy.

- Breach of this policy by the IT Assets End Users may result in remotely wiping assigned devices, blocking the IT Assets End Users from the University's network, and preventing the IT Assets End Users from using University provided services and software. A breach may be considered a disciplinary offence.

- Any actual or suspected breach of this policy must be reported to the ICT Department via the most suitable channel. The Head of IT will take appropriate action and inform the relevant internal and external authorities as permitted by law.
- Failure to comply with this policy may result in disciplinary action in accordance with the relevant process. Refer to the Employee Human Resources Handbook.

6.3 Related References

None.

7.0 INFORMATION SECURITY AWARENESS AND TRAINING POLICY

7.1 Purpose

The purpose of the Information Security Awareness and Training Policy is to ensure that all AUBH Employees are aware of how to maintain security to protect the University's Information Assets from any data leakage or internal or external vulnerabilities.

The Information Security Officer shall coordinate with the HR Department to ensure that all Employees using AUBH Information Assets receive training in regulatory guidelines and laws governing customer information security, along with information security policies and procedures appropriate to their position and job responsibilities at AUBH.

7.2 Policy

7.2.1 The Information Security Officer shall ensure that training systems are in place to address:
- Initial training for new hires.
- Continuing refresher sessions for existing Employees.

7.2.2 The Information Security Awareness Program should ensure that all Employees have a basic understanding of information security matters, including general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally accepted standards of ethics and behavior.

7.2.3 The awareness program shall cover best practices in information security, controls to be implemented to avoid incidents, etc.

7.2.4 Additional training as needed should be conducted for all Employees with specific obligations towards Information Assets security that are not satisfied by basic security awareness; these Employees include security administrators and IT/network operations personnel. The training requirements shall reflect the Employees' relevant prior experience, training, and/or professional qualifications, as well as expected job needs.

7.2.5 Security awareness and training activities should commence within a week of Employee joining, for instance, through attending Information Assets security induction/orientation classes. The

awareness activities should continue regularly thereafter to ensure a reasonably consistent level of awareness.

7.2.6 All Employees shall undergo refresher training at least once a year.

7.2.7 Role-based training shall be conducted for Employees when they assume specific Information Assets security roles.

7.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2022	6.3 Information security awareness, education, and training

8.0 IT ASSETS ACCEPTABLE USAGE POLICY

8.1 Purpose

The purpose of IT Assets Acceptable Usage Policy is to specify the acceptable usage of IT Assets at AUBH, including computing devices, email, and internet. These guidelines exist to protect both the IT Assets End Users and the University. Improper usage can subject the University to various risks, such as virus attacks, compromise of network systems and services, and legal issues.

8.2 Policy

8.2.1 General

8.2.1.1 All IT Assets End Users must adhere to the IT Assets Acceptable Usage Policy, which specifically covers the acceptable usage of computing devices, email, and internet.

8.2.1.2 Devices and information systems are provided to IT Assets End Users solely for performing their official duties. They shall not be used for any personal purposes.

8.2.1.3 The IT Administrators may monitor devices and information systems provided by the University, including system usage logs and stored data for security, administration, and compliance purposes at any time without prior notice.

8.2.1.4 IT Assets End Users shall not engage in any illegal activities or activities not accepted by AUBH on devices and information systems issued to them by AUBH.

8.2.1.5 IT Assets End Users accessing AUBH's IT Assets, as outlined in their contract (employment contract, vendor contract, etc.), shall not disclose any proprietary information, trade secrets, procurement details, or any other materials classified by the organization as confidential or internal.

8.2.1.6 The IT Administrators may request IT Assets End Users to bring their devices for scheduled maintenance.

8.2.1.7 Unacceptable Use of IT Assets

- Engage in activity that is illegal under the applicable laws of the Kingdom of Bahrain.

- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to AUBH.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy, unauthorized collection, use, or disclosure of personal information.
- Access or attempt to access systems through activities the User is not authorized to perform that include port scanning, security scanning, network sniffing, keystroke logging, or other IT information-gathering techniques when not part of the User's job function.
- Reveal personal, system, or network passwords to others including, but not limited to, co-workers, family, or friends.
- Introduce any viruses or malware, or maliciously tamper with any resources.
- Engage in copyright infringement, install, or distribute unlicensed or "pirated" software or any software not approved by the Information Technology Department.

8.2.2 Usage of Computing Devices

8.2.2.1 Physical Security Control of Laptops

- The physical security of devices issued by AUBH to IT Assets End Users is a personal responsibility, and they shall adhere to the following best practices:
  - The laptop shall be kept in possession and within sight whenever possible.
  - Extra care should be taken in public areas.
  - If it is lost or stolen, the IT Administrators should be notified immediately.

8.2.2.2 Installing Software

- Administrative rights shall not be provided to Employees for their systems, except for IT Administrators and the Head of the ICT Department.
- IT Administrators shall perform all software installations centrally using SCCM.
- Policies should be regularly reviewed and pushed by IT Administrators.
- The IT Administrators shall maintain a list of approved software. If any IT Assets End User has a business purpose to install software outside the list, the IT Administrators shall perform due diligence and obtain management approval.
- Trials of licensed software shall be avoided.

8.2.2.3 Unauthorized storage of material

- IT Assets End Users shall not store or access any inappropriate materials such as pornographic, racist, defamatory, or harassing files, pictures, videos, or email messages that might cause offense or embarrassment using the devices issued by AUBH.
- IT Assets End Users shall refrain from storing personal confidential information inside the system. The ICT Department and IT Administrators shall not be responsible for any loss or misuse of such information.

8.2.2.4 Controls against unauthorized access

- Systems are provided for official use by authorized IT Assets End Users. IT Assets End Users shall not loan the system or allow it to be used by others such as family members or friends.
- All external storage media are blocked by default for students and shall be allowed after obtaining approval from the Head of the ICT Department.

8.2.2.5 Access to visitors in AUBH's network

- An isolated network for visitors or guests shall be established.
- Visitors' systems should not be allowed to connect to the internal network.
- Storage media like USBs, CDs, etc., shall be checked in systems for malware before accessing their contents.

8.2.2.6 Virus protection

- All systems shall be configured with Anti-Virus software which can automatically scan files.

8.2.2.7 Reporting Incidents

- If IT Assets End Users suspect any security incidents (such as virus attacks or ransomware) on their system, it shall be removed from the network and stop its use immediately. The system must be handed over to the IT Administrators to check the issue and minimize the damage.

8.2.2.8 Backups

- Employees must take their backups for their Desktop/Laptops to "OneDrive" to their respective folders.
- Personal files should not be placed in the backup location.

8.2.2.9 Monitoring

- IT Administrators can monitor the data inside systems issued. They will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If any inappropriate material is received by email or other means, it should be deleted immediately.

8.2.3 Usage of Email

8.2.3.1 Email account holders shall use AUBH email for legitimate purposes. IT Assets End Users shall refrain from using their email ID for non-academic communication.

8.2.3.2 All AUBH information contained within an email message or attachment is considered a University asset; thus, all information security policies apply to the same.

8.2.3.3 Email is always subject to monitoring and logging. Releasing AUBH's confidential, private, or sensitive information through email is prohibited without prior authorization.

8.2.3.4 AUBH applies resilient infrastructure practices to ensure the email service is available to all email account holders. To avoid service degradation by sending large attachments and to avoid significant delays in the delivery of corporate emails, the transmission of attachment size is limited to 50 MB by the IT Administrators.

8.2.3.5 Managing Email Accounts of Resigned Employees

- Email accounts of resigned Employees, including trainees, shall be removed before completing the HR Department's relieving process, and the mail should be archived.
- In cases where an Employee email account needs to be retained for a longer period for business purposes, it shall be done only after management approval. The IT Administrators shall change the password of such email accounts.
- The IT Administrators shall maintain a list of such email accounts, along with details of the person responsible for managing them.

8.2.3.6 Managing Email Accounts of Student Graduates

- Student email accounts shall remain active after graduation to facilitate continuous communication.

8.2.3.7 Mail Archiving and Retention

- As a policy, AUBH does not archive Employee emails. Should there be a specific need to archive an Employee's mail, the request must be submitted to the IT Administrators with management approval.

8.2.3.8 Configuring Mailboxes in Mobile Devices

- IT Assets End Users may configure their email account on their mobile device(s), while adhering to this policy.

8.2.3.9 Acceptable Use of Email

- ✓ Use the email service primarily for AUBH's business-related purposes, consistently following the University's policies and procedures with ethical conduct.
- ✓ Communicate with work colleagues to enhance work productivity and collaboration.
- ✓ Communicate with current or prospective customers and business partners of AUBH.
- ✓ Access the email service only through the authorized account owner using the electronic equipment provided by AUBH, Outlook Web Access, and mobile-configured email services.
- ✓ Sign up for newsletters, journals, and other genuine online services that are work-related and will contribute to the Employee's professional growth.

- ✓ Verify the email and names of unknown senders to ensure they are legitimate before establishing any email communication.
- ✓ Do not open attachments containing executable files, upgrades, or patches received via email.
- ✓ Avoid opening unknown links and attachments that might be malicious. If any suspicious email is received, please contact the IT Administrators immediately.
- ✓ When receiving emails from external sources, look for inconsistencies in email styles to identify spam and unwanted email communications.
- ✓ Use strong passwords and do not disclose your password or account information.
- ✓ Email messages received shall not be altered and forwarded without the original sender's permission.

8.2.3.10 Unacceptable Use of Email

- × Email that is likely to harass, insult, or discriminate based on age, sex, race, religion, national origin, sexual orientation, political beliefs, disability, or any other criteria should be avoided. IT Assets End Users need to be aware that such emails may render them and/or AUBH liable for harassment or discrimination claims, as well as defamation actions.
- × Junk or chain mail should not be distributed.
- × The distribution of information that infringes copyright laws is prohibited.
- × Email should not be used for personal business or non-business activities.
- × Email should not be used to encourage any illegal activity.
- × Email should not be used to provoke any activity involving a breach of the Employee's terms and conditions as mentioned in the employment contract.
- × Sending emails so they appear to be from another person is prohibited.
- × Distribution of confidential information to third parties without authorization is not allowed.
- × Sending or forwarding emails that are likely to contain computer viruses is prohibited.
- × Employees should not use their personal emails to share and transmit data related to AUBH and its clients or vendors.
- × Forwarding confidential mail to private email accounts or other Employees is not allowed.

8.2.4 Usage of Internet

8.2.4.1 Eligibility for Internet access

- Employees and students will have access to the internet.
- Stakeholders other than Employees and students may have access to the internet thorough the guest network or other arrangements approved by the IT Department.

8.2.4.2 Monitoring Internet Traffic

- IT Administrators shall deploy content filtering mechanisms for internet traffic to detect security breaches. The main function of these mechanisms is to monitor network traffic to and from the internet for the detection of unusual behavior and specific attack scenarios that can potentially constitute signs of security breaches. These mechanisms log certain internet traffic data (for example, destination), which is necessary for intrusion detection purposes and the investigation of security incidents.
- Only authorized personnel shall administer monitoring mechanisms and ensure that IT Assets End Users' personal data is kept confidential and protected.

8.2.4.3 Acceptable Use of the Internet

- ✓ Communicating with fellow Employees, students, business partners, and clients, within the context of an individual's assigned responsibilities.
- ✓ Using the internet for work-related purposes in support of the organization's objectives.
- ✓ Participating in educational or professional development activities.

8.2.4.4 Unacceptable Use of the Internet

- × Distributing harassing, violent, discriminating, or hateful messages and imagery using company equipment/internet.
- × Utilizing the internet and computers at the workplace to commit any illegal activity, including piracy of music, movies, and other content.
- × Distributing confidential information of AUBH.
- × Employees must not intercept, disclose, or assist in the interception and disclosure of information sent to/from the internet.
- × Sending information via the internet is not allowed for information classified as "CONFIDENTIAL," unless authorization is granted, and adequate security mechanisms are implemented. The IT Administrators monitor the flow of information to detect and record any data breaches.
- × IT Assets End Users must be extremely cautious when publishing information or questions on the internet (e.g., via mailing lists, newsgroups, social media, etc.) in order not to damage, even unintentionally, AUBH's competitiveness and/or image.
- × The internet should not be used to access movie sites like IP-TV, Netflix, etc.

8.3 Related References

Standard/ Framework	Compliance Requirement

ISO 27001:2022	5.10 Acceptable use of information and other associated assets

9.0 DATA GOVERNANCE POLICY

9.1 Purpose

The Data Governance Policy aims to establish a comprehensive framework that ensures the responsible and ethical management of data across AUBH. Recognizing the critical role that data plays in supporting the AUBH's mission of academic excellence, research, and administrative functions, this policy aims to:

- Ensure Data Confidentiality: Safeguard sensitive information from unauthorized access, disclosure, alteration, or destruction. This ensures that sensitive or private information is only accessible to authorized individuals or systems that have appropriate permissions.
- Foster Data Integrity: Maintain the accuracy, consistency, and reliability of data to support informed decision-making, academic research, and operational efficiency.
- Ensure Availability: Ensure that information and resources are accessible and usable when needed by authorized users.
- Promote Data Privacy and Security: Safeguard sensitive and personally identifiable information through the implementation of robust security measures and compliance with relevant data protection laws and regulations.
- Encourage Collaboration: Foster a culture of collaboration and communication among University stakeholders to ensure a shared understanding of data definitions, standards, and best practices.
- Comply with Regulations: Adhere to local, national, and international data governance laws and regulations, including but not limited to the PDPL Bahrain, Higher Education Council Regulations, and Ministry of Education Regulations.
- Support Institutional Decision-Making: Provide a foundation for evidence-based decision-making by ensuring that data is accurate, trustworthy, and readily available to support strategic planning, policy development, and continuous improvement.
- Optimize Data Management Processes: Establish clear roles, responsibilities, and processes for the collection, storage, and dissemination of data, promoting efficiency and reducing redundancies.
- Build Stakeholder Trust: Demonstrate the University's commitment to ethical data handling, transparency, and accountability, fostering trust among Stakeholders.
- Enable Innovation: Create an environment that encourages the responsible use of data for innovative research.

This policy covers:

(a) Data Collection and Use

(b) Meta Data Management

(c) Data Loss and Prevention

(d) Data Retention

(e) Data Sanitization

(f) Data Masking

(g) Data Backup

(h) Media Disposal

(i) Data Management in Data Warehouse

(j) Personal Data Management

(k) Data Breach Response

9.2 Policy

9.2.1 Data Collection and Use

9.2.1.1 A Data Protection Officer shall be appointed to oversee the implementation of this policy and related procedures.

9.2.1.2 Data shall only be collected for specified, explicit, and legitimate purposes, and it shall not be used for purposes that are incompatible with those original purposes.

9.2.1.3 Data Owner is responsible for maintaining confidentiality. The integrity and availability of each dataset shall be identified.

9.2.1.4 Procedure for obtaining consent from AUBH Stakeholders before collecting their data shall be established and provide information on how such consent can be withdrawn.

9.2.1.5 Proper measures shall be implemented to ensure the accuracy and integrity of data.

9.2.1.6 A comprehensive data dictionary must be upheld for all gathered personal data. This dictionary should encompass metadata, including details on the individual responsible for data collection and management, authorized personnel with access to the data, the methodologies employed for data collection and management, the systems to which the data is transmitted, and the designated retention period for the data.

9.2.1.7 Data Owners, while collecting the data, shall identify the current and potential future users (both internal and external) of the data.

9.2.1.8 Data collected shall be retained only for the specified period.

9.2.1.9 To ensure one version of the truth, proper mechanisms shall be established to avoid duplicate versions of datasets.

9.2.1.10 All data collected shall be validated to meet the following quality dimensions:

- Accuracy
- Completeness
- Consistency

- Validity
- Timeliness
- Accessibility
- Precision
- Conformity
- Reliability

9.2.2 Meta-Data Management

9.2.2.1 Metadata governance structures, standards, guidelines, roles, and responsibilities shall be established and documented to ensure consistency and interoperability across AUBH.

9.2.2.2 Metadata schemas, vocabularies, and controlled vocabularies shall be selected or developed based on industry standards and best practices. This policy is explained in the procedure for Metadata management.

9.2.2.3 Guidelines for metadata creation, including required elements, formatting conventions, and best practices, shall be provided to data creators (individuals responsible for generating or producing data).

9.2.2.4 The Data Owner shall be responsible for ensuring that metadata is defined as per the standards and guidelines and is maintained.

9.2.2.5 Metadata shall be created at the time of data creation or acquisition and updated as needed throughout its lifecycle.

9.2.2.6 Metadata containing sensitive or personal information shall be protected by University policies, data protection laws, and industry best practices.

9.2.2.7 Access controls, encryption, anonymization, and other security measures shall be implemented to safeguard metadata against unauthorized access, disclosure, or misuse.

9.2.3 Data Loss and Prevention

9.2.3.1 The Data Owner shall classify data according to its criticality and sensitivity, categorizing it as confidential, private, or public.

9.2.3.2 The Data Owner must assess the data's integrity and availability, determine appropriate access rights, and ensure that adequate data protection measures are implemented accordingly.

9.2.3.3 A risk-based approach shall be established to ensure that security controls are instituted by the risk and magnitude of the impact that could result if critical information assets are compromised. Risk treatment plans will be developed and implemented as necessary.

9.2.3.4 Employees shall follow data protection policies, report incidents, and participate in data protection training and awareness programs.

9.2.3.5 Data must be handled, stored, transmitted, and disposed of securely, by established procedures.

9.2.3.6 Access to data must be controlled through authentication, authorization, and encryption mechanisms.

9.2.3.7 Third-party vendors and partners shall be evaluated for their information security practices and adherence to data protection standards. Contracts with third parties must include data protection clauses.

9.2.3.8 Sensitive and confidential data shall be transferred outside AUBH upon proper approval and using appropriate security measures.

9.2.3.9 Proper mechanisms like encryption using industrial best practices shall be used to protect the "data at rest" and "data in motion."

9.2.4 Data Retention

9.2.4.1 The Data Owner is responsible for maintaining data and enforcing retention as per this Policy.

9.2.4.2 The Data Owner shall establish and maintain a data retention schedule that specifies the periods for which different categories of data are to be retained, considering legal, regulatory, compliance, and contractual requirements.

9.2.4.3 Information Assets holding the data must be maintained according to legal, regulatory, compliance, and contractual requirements.

9.2.4.4 Legal, regulatory, compliance, and contractual requirements for data retention must be defined as part of the data dictionary.

9.2.4.5 All archived data must be safeguarded from unauthorized access to avoid data breaches.

9.2.4.6 Backups for electronic records shall be maintained.

9.2.4.7 Data shall be reviewed annually, and any data that is no longer necessary for the purpose it was collected shall be securely disposed of.

9.2.5 Data Sanitization

9.2.5.1 A thorough assessment shall be done before the disposal of any hardware or media containing data to identify and confirm the presence of sensitive information.

9.2.5.2 Any hardware or storage media containing sensitive information should be sanitized before its transfer to another resource, sale, donation, or deemed as no longer necessary for business use.

9.2.5.3 Accurate and detailed records shall be maintained for the data sanitization process, including dates, methods used, and responsible parties.

9.2.5.4 Data sanitization requirements shall be included in contracts with third-party vendors who handle or process data on behalf of AUBH. Processes shall be established to verify that third parties adhere to the organization's data sanitization standards before returning or disposing of equipment.

9.2.5.5 Implement secure wiping procedures for electronic devices that store sensitive data to ensure the irretrievable removal of data before decommissioning or repurposing.

9.2.6 Data Masking

9.2.6.1 Data Owners should identify and classify sensitive data elements based on their sensitivity level (e.g., Confidential, Private, Public). Reference for determination of the sensitivity levels can be local privacy regulations or University norms. This classification will help determine the appropriate level of data masking.

9.2.6.2 AUBH shall use masking methods to mask sensitive data, such as substitution, shuffling, encryption, tokenization, or data truncation.

9.2.6.3 Some data elements may be exempted from masking in production or non-production environments if there is a valid business need or legal requirement. Such exceptions must be justified, approved by Data Owners, and adequately documented.

9.2.6.4 Algorithms and encryption keys used in the data masking process shall be documented properly. The keys shall be safeguarded to prevent unauthorized access and ensure that the masking process is reversible when needed.

9.2.6.5 Procedures for testing and validating the effectiveness of the data masking techniques shall be established. Regularly audit the masked data to ensure that sensitive information remains adequately protected.

9.2.7 Data Backup

9.2.7.1 The Data Owner, along with the ICT Department, shall develop the Data backup plan considering the criticality of data. The backup plan shall cover the frequency of backup, storage media, frequency of restoration and testing, etc.

9.2.7.2 Employees should ensure that the backup of critical/official data residing on their desktop/laptop is taken onto "One Drive" provided by the ICT Department. They may seek help from the ICT Department with any support required for facilitating the same.

9.2.7.3 The frequency and extent of backups must be determined by the importance of the information and the acceptable risk, as determined by the Data Owner. This shall be documented in the information asset register.

9.2.7.4 If any data is maintained on backup media, ICT Department shall periodically test the backup media to ensure that the data stored is recoverable.

9.2.7.5 The backup media shall be stored with sufficient protection from unauthorized access and proper environmental conditions in an offsite location.

9.2.7.6 Backup media must be physically destroyed securely.

9.2.8 Media Disposal

9.2.8.1 All data, whether held electronically or on paper, should be reviewed regularly to decide whether to destroy or delete any data by the designated retention period.

9.2.8.2 The Data Owner shall be responsible for identifying the data to be disposed of. The ICT Department shall be responsible for the disposal of data following this policy of disposal and relevant procedures.

9.2.8.3 The ICT Department shall maintain traceability of media disposed, to ensure the items were properly disposed of, which should, at a minimum, contain the following information: who performed the procedure, when, and what method was used.

9.2.8.4 Data deletion may be performed using secure deletion software to permanently delete information, to help ensure information cannot be recovered by using specialist recovery or forensic tools. AUBH may use services from external service providers for media disposal.

9.2.9 Data Management in Data Warehouse

9.2.9.1 When data is stored in the data warehouse, it shall be classified based on its sensitivity, criticality, and regulatory requirements.

9.2.9.2 Data handling procedures, including data entry and ETL, shall be documented, and implemented to maintain data integrity and traceability throughout its lifecycle.

9.2.9.3 Access to the data warehouse and its contents shall be restricted to authorized users with a legitimate business need. Access permissions shall be granted based on the principle of least

privilege, where users are granted only the minimum level of access required to perform their job duties.

9.2.9.4 Access Control Lists (ACLs), Role Based Access Control (RBAC), and other access control mechanisms shall be implemented to enforce segregation of duties and limit access to sensitive data.

9.2.9.5 Data stored in the data warehouse, including data in transit and at rest, shall be encrypted using strong encryption algorithms and protocols to protect confidentiality and prevent unauthorized access.

9.2.9.6 Measures shall be implemented to ensure the integrity and accuracy of data stored in the data warehouse. This includes implementing data validation checks, checksums, and data integrity controls to detect and prevent data corruption or tampering.

9.2.9.7 Logging and monitoring mechanisms shall be implemented to track user activities, system events, and security incidents within the data warehouse. Logs shall be retained for a defined period and regularly reviewed for security analysis and incident response purposes.

9.2.10 Personal Data Management

9.2.10.1 The following principles shall be followed while handling personal data by Data Owners:

- Data shall be processed in a fair, lawful, and transparent manner.
- It shall be used only for specified purposes.
- Personal data should be correct, and where relevant, kept up to date. Necessary measures for periodic reviews shall be put in place.
- It shall be protected against loss, destruction, or damage.
- Personal data that is stored for longer periods for historical, statistical, or scientific use shall only be kept in an anonymous form, by modifying the personal data into a form in which it cannot be associated with the data subject. If that is not possible, the identity of the data subjects must be encrypted.

9.2.10.2 The Data Owner shall implement proper technical and organizational measures to guarantee the protection of data against accidental or unauthorized destruction, accidental loss, as well as against alteration or disclosure of, access to, and any other unauthorized forms of processing.

9.2.10.3 The technical and organizational measures to protect personal data must be documented and accessible by all relevant parties, including the authority, the Data Owner, Data Processors, etc.

9.2.10.4 Data Owners and Data Processors shall be trained in the technical and organizational measures defined to protect personal data.

9.2.10.5 The Data Owner or Data Processors must not disclose any personal data without the data subject's consent or in the execution of a judicial order issued by a competent court, public prosecution, investigation judge, or military prosecution.

9.2.10.6 Outside Bahrain, Personal Data shall transfer only to countries or territories approved by authorities. Any transfer outside these listed countries or territories shall be made only after getting the consent of the data subject.

9.2.11 Data Breach Response

9.2.11.1 All Stakeholders must promptly report any suspected or confirmed data breaches to the ICT Department. The ICT Department shall report such incidents to the Information Security team and designated Data Owners.

9.2.11.2 The ICT Department shall manage reported incidents following the policy and procedure for Incident Management. Refer to 15.0 Incident Management Policy.

9.3 Related References

Standard/ Framework	Compliance Requirement	Mapping to policy
ISO 27001:2022	Clause 7.14: Secure disposal or re-use of equipment	2.8 Policy for Media Disposal
ISO 27001:2022	Clause:8.11: Data Masking	2.6 Policy for Data Masking
ISO 27001:2022	Clause:8.12: Data Leakage Prevention	2.3 Policy for Data Loss and Prevention
ISO 27001:2022	Clause:8.13: Information Backup	2.7 Policy for Data Backup
NIST	PR. IP-6: Data is destroyed according to policy	2.5 Policy for Data Sanitization
Personal Data Protection Law	All Relevant articles	2.10 Policy for Personal Data Management

10.0 ACCESS CONTROL AND MANAGEMENT POLICY

10.1 Purpose

The purpose of the Access Control and Management Policy is to ensure that adequate controls are in place to restrict access to systems and data and that access to systems and data is restricted to authorized users based on the principle of least privilege, safeguarding AUBH's Information Assets and maintaining the integrity of data and systems.

10.2 Policy

10.2.1 General Access Control Policies

10.2.1.1 Authentication Policies: Authentication policies, procedures, and processes must be distributed to all users as required.

10.2.1.2 Default Settings: Access control systems must be configured with a default "deny-all" setting.

10.2.1.3 Individual Accountability: Group and shared IDs shall not be used for authentication and authorization purposes.

10.2.1.4 MFA Requirements: Multi-Factor Authentication shall be enabled for accessing critical systems.

10.2.1.5 Access Revocation: User's access to systems shall be removed before their exit process is completed by HR on the last day of employment at AUBH.

10.2.1.6 Annual Access Reviews: User access to systems and data shall be reviewed at least once a year.

10.2.1.7 Record Keeping: Records of identity assignment and revocation shall be maintained, especially where an audit trail of access management is not available.

10.2.2 System-Specific Access Control

10.2.2.1 Access Configuration: Access control to system components must enforce privileges assigned to users based on job classification, function, and the need-to-know principle.

10.2.2.2 Access Authorization: Access shall be provided to users after approval from the Information Asset Owner. An Approval Matrix shall be maintained, specifying who is responsible for assigning/revoking access.

10.2.2.3 Vendor and Contractor Access: Any vendor or contractor requiring remote access must designate a person to be the Point of Contact (POC). Access should be created specifically in the name of the person and removed immediately after the support or at the time of change of person.

10.2.2.4 Special System Rights: If any users require special rights to perform specific duties on systems, such access shall be approved by the Information Asset Owner and removed once the objectives are met.

10.2.3 Data-Specific Access Control

10.2.3.1 Data Classification and Access Control: Data is classified according to its sensitivity and confidentiality, as outlined in the 5.0 Information Assets Classification and Management Policy. Access controls are applied accordingly.

10.2.3.2 Assignment of Data Access: Data access shall be assigned by Information Asset Owners based on the classification of the data and the user's role within the University. The assignment process must ensure that access is granted strictly according to the need-to-know principle and is compliant with all relevant data protection regulations.

10.2.3.3 Data Access Reviews: Access to sensitive data must be reviewed and revalidated at least annually or following risk assessment results.

10.2.3.4 Data Encryption: Sensitive data, both at rest and in transit, must be encrypted using industry-standard encryption techniques.

10.2.3.5 Audit and Monitoring of Data Access: Continuous monitoring and auditing of access to sensitive data must be implemented.

10.2.3.6 Special Data Access Rights: Temporary special access rights to sensitive data must be granted only under strict controls and require approval from the Information Asset Owner.

10.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2022	8.2 Privileged access rights

ISO 27001:2022	8.3 Information Access Restriction

11.0 NETWORK SECURITY POLICY

11.1 Purpose

The purpose of the Network Security Policy is to outline the principles and standards for AUBH's network infrastructure, data, and information systems. The goal is to protect against unauthorized access, data breaches, and other network-related security threats.

11.2 Policy

11.2.1 General

11.2.1.1 The network design shall be prepared considering the security requirements, including firewalls, intrusion detection/prevention systems, and access controls.

11.2.1.2 Access to the network shall be granted based on the principle of least privilege, ensuring that individuals have access only to the resources necessary for their roles.

11.2.1.3 Strong authentication mechanisms, such as multi-factor authentication (MFA), shall be employed where applicable.

11.2.1.4 All network devices and systems shall be kept up to date with security patches and updates.

11.2.1.5 A documented process for patch management shall be followed to minimize vulnerabilities.

11.2.1.6 Logs of network activities will be maintained, and logs will be regularly reviewed for security incidents.

11.2.1.7 The network shall be segregated based on access requirements and restrictions.

11.2.1.8 All incidents reported shall be managed by following the policy for “Incident Management”.

11.2.2 VPN Policy

11.2.2.1 VPN access must require multi-factor authentication by the user.

11.2.2.2 All traffic must be encrypted using u3.

11.2.2.3 All authentication attempts shall be logged.

11.2.2.4 It is the responsibility of the user with VPN privilege to ensure that unauthorized users are not allowed access.

11.2.2.5 VPN access shall be provided to users with an approved business case.

11.2.2.6 Users are required to install the VPN client software as directed by the AUBH team to activate their VPN access.

11.2.2.7 VPN access shall be removed at the end of the project, contract closure, employee exit, etc.

11.2.3 Firewall Policy

11.2.3.1 All firewalls and their network components shall be operated, managed, and maintained by the IT Department.

11.2.3.2 All changes to the external network connections, firewall, switches, and router configurations must be approved by the Head of IT & Information Security Officer and tested before implementing the change.

11.2.3.3 The following services/ports are necessary for business purposes and shall be allowed through the firewall. If any other protocols are to be used, justification for the same shall be documented.

- HTTPS (TCP/443)
- SSH (TCP/22)
- SMTP (TCP/25)
- VPN

11.2.3.4 Firewall configurations shall be reviewed annually.

11.2.3.5 Before a firewall rule set is created, a risk analysis should be performed to develop a list of the types of traffic needed by "AUBH" and categorize how they must be secure including which types of traffic can pass through a firewall under what circumstances.

11.2.3.6 The approach adopted to define the firewall rule set is "least privilege" in all services that are denied by default in the firewall unless expressly permitted in this policy.

11.2.3.7 When implementing firewalls, the IT Department must employ a high-availability design to ensure uninterrupted access to network resources.

11.2.3.8 Firewall rules shall be defined and implemented after the Information Security Officer's approval.

11.2.3.9 Firewall logs should be reviewed periodically to monitor any unauthorized access from external networks.

11.2.4 Network Monitoring

11.2.4.1 AUBH will identify and implement adequate mechanisms to log and monitor any violation and critical security activity and any indication of an imminent security violation. Any events will be reported immediately to the VP Finance and Administration and will be acted upon on time.

11.2.4.2 AUBH will perform external and internal network testing annually to identify and ensure that network risks are within the acceptable risk level.

11.2.5 Traffic Monitoring

11.2.5.1 Authorized IT personnel may monitor the campus backbone or specific segments for the following:

- Protocols and applications in use
- Sources and destinations - traffic patterns
- Performance metrics
- Bytes sent and received per router and switch interface.
- Errors per router and switch interface

11.2.5.2 Failure conditions

- AUBH shall consider procuring and implementing suitable tools for automating the performance of the monitoring function. Statistical records are retained for as long as they are deemed useful.
- Under exceptional circumstances, i.e., to help investigate incidents or fault conditions, specific interactions between endpoints may be monitored and recorded for analysis.

Records are retained for as long as the incident or fault is active, after which time all records will be subject to data retention policy.

11.2.6 Wireless Network Policies

11.2.6.1 Access to Wireless Networks

- AUBH shall maintain multiple wireless networks operating in the Campus to ensure segregation of access. AUBH shall segregate the users accessing the wireless services into three groups:
  - Staff
  - Students
  - Guests
- Wireless access infrastructure to the student community shall be completely segregated from the internal networks. Suitable authentication mechanisms will be implemented to ensure that the access is available to authorized students only.
- Any access to information services through the wireless network is based on appropriate authentication as defined in the security policies.
- AUBH shall ensure that the employees, contractors, and third parties must be authorized to connect to third-party wireless networks.

11.2.6.2 Wi-Fi Access Management

- Access to the Wi-Fi network at the University shall be controlled based on the following parameters:
- Limiting access to the secure areas and content to authorized individuals only.
- Third-party support services personnel shall be granted restricted access to secure areas only when required. Such access will be authorized, monitored, and revoked, when not required.
- The access to secure areas will be logged during and after normal working hours. The access log will be securely maintained, regularly reviewed, and followed up as appropriate.
- Individuals who are not registered for continuing access to IT services shall be authorized by IT and their activities shall be recorded and monitored.
- The Wi-Fi connections shall be adequately audited and monitored periodically to detect any unauthorized activity.
- At any time and without prior notice, the University reserves the right to examine and monitor any Wi-Fi connection's surfing activities.
- Wi-Fi Access rights will be reviewed at the start of every term (semester for students, term of employment for staff).
- The Wi-Fi 'staff' access will be immediately revoked for the employees leaving AUBH.

11.2.6.3 Wi-Fi Access for Staff

- The staff at AUBH shall be eligible for long-term access to the Wi-Fi.
- The staff shall be divided into categories to access the wireless internet services at defined timings to monitor and prevent AUBH infrastructure from any kind of vulnerabilities.

- To access the Wi-Fi services, the employees shall be given standard AUBH credentials at the start of each term or their time of employment to connect their devices to the internet.
- Every connected device's activity shall be constantly monitored by the IT Infrastructure & Database Administration Team and may be declined access in case of any unknown activity.
- In the case of declined access, the employee shall contact the IT Infrastructure & Database Administration Team to discuss the scenario and regain Wi-Fi access.

11.2.6.4 Wi-Fi Access for Students

- AUBH students shall be eligible for long-term access to the campus Wi-Fi.
- At the start of each semester or study year, the students shall be provided with the Wi-Fi access credentials upon registration.
- The credentials will be valid for the registered semester only. However, if a student wishes to access the campus Wi-Fi while not enrolled in a semester, he/she will contact the IT Infrastructure & Database Administration Team to prove their identity and register for using the service for a defined time by filling a specific form.

11.2.6.5 Wi-Fi Access for Guests

- Guests visiting AUBH shall be granted short-term access to the Wi-Fi service.
- A complimentary protocol shall be established within the framework to automatically accept external devices for a limited time and disconnect once the device goes out of range.
- The guest devices shall be monitored and controlled to maintain the access level, and bandwidth usage, respect the connection time limitations, and to prevent the users from accessing the restricted websites, applications, or network areas of AUBH.

11.2.6.6 Wi-Fi Access Exceptions

- In case of an event or training organized within AUBH premises, an exceptional Wi-Fi access protocol will be established similar to the guest protocol.
- The access will be granted to all devices only for the defined period within a certain physical range.

11.2.6.7 Wi-Fi Access Sanitization

- In any case of using VPNs or proxy altering hardware or software, the Wi-Fi access shall be revoked immediately by the IT Infrastructure & Database Administration Team and registered as a threat to the AUBH framework against the respective user.
- The registered threat will redirect the user case to take action for violation of AUBH security procedures.

11.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2023	8.16 Monitoring Activities

ISO 27001:2023	8.20 Network Security
ISO 27001:2023	8.21 Security of network services
ISO 27001:2023	8.22 Segregation of networks

12.0 PASSWORD POLICY

12.1 Purpose

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all Employees of AUBH using the organization's systems must take appropriate steps to ensure that they create strong, secure passwords, and keep them always safeguarded.

The purpose of Password Policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

12.2 Policy

12.2.1 Password Confidentiality

12.2.1.1 Passwords must be treated as confidential information. No employee shall give, tell, or hint their password to another person, including IT staff, administrators, superiors, other co-workers, friends, or family members, under any circumstances.

12.2.1.2 Passwords to access information assets and facilities, should not be written down or electronically stored,

12.2.1.3 Passwords should not be stored in clear text.

12.2.2 Password Construction Rule

12.2.2.1 AUBH shall institute strong password parameters for all systems which will at a minimum consider the following:

- The password must be a minimum of eight alphanumeric characters long.
- The password must have at least one lowercase letter, one uppercase letter, and one number. For systems that do not recognize upper and lower case, all characters must be treated as case insensitive.
- Use of special characters in password such as (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./) are mandatory – where possible.
- The password cannot be the same as the ID.
- The password cannot repeat the same number or letter (whether upper case or lower case) more than two times consecutively (e.g., AAA1967, Afgggh87).
- The password cannot be the same as the user's first name, last name, or mobile number.

12.2.2.2 Initial passwords will be assigned by the ICT Department; however, users must change the initial password on the first login and thereafter change it periodically.

12.2.3 Account lockout threshold.

12.2.3.1 Account shall be locked out automatically after 5 attempts of invalid logins.

12.2.4 Password age

12.2.4.1 Passwords must have a minimum age of 1 day, to prevent users from quickly cycling through the same password again.

12.2.5 Password expiry

12.2.5.1 All user-level passwords (e.g., application user, e-mail, web, desktop computer) must be changed within 90 days.

12.2.5.2 All system-level and production environment passwords (e.g., root, enable, operating system admin, application administration accounts) must be changed within 90 days.

12.2.6 Password reuse

12.2.6.1 Password history will be enforced by the systems, users must not repeat the last twelve passwords.

12.2.7 Managing privileged super system-level passwords.

12.2.7.1 All privileged super system-level passwords (e.g., domain admin, root, super admin service accounts, etc.) must be managed and always controlled. These passwords cannot be revealed, shared, and/or used unless the Disaster Recovery (DR) /Business Continuity Plan (BCP) is activated or it is deemed necessary to continue AUBH's business operation.

12.2.7.2 Users managing the system account shall maintain a password different from that of their account password.

12.2.8 Changing Password

12.2.8.1 If the user feels that their password is compromised, it must be changed immediately.

12.2.9 Multi-factor Authentication (MFA)

12.2.9.1 MFA must be enforced on all remote access, including access from the internet to third party company computing resources.

12.2.9.2 MFA must be enforced on all cloud services access, including access to cloud-based email.

12.2.10 Handling Forgotten Password

12.2.10.1 In case of forgotten passwords, users should be able to reset their password using MFA, i.e., a verification message should be sent to their mobile phone or to their personal email stored at AUBH records.

12.2.10.2 IT personnel are forbidden from resetting user passwords themselves without written user consent can be presented. Users should be always prompted to reset their own password after successfully logging in.

12.3 Related References

None.

13.0 PHYSICAL AND ENVIRONMENT SECURITY POLICY

13.1 Purpose

The purpose of the Physical and Environment Security Policy is to protect the Information Assets from physical threats. The policy:

- Covers the rules for granting control, monitoring, and removal of physical access to office premises.
- Identifies sensitive areas within the organization and defines and restricts access to the same.

13.2 Policy

13.2.1 Security perimeters should be defined and protect areas that contain information systems to prevent unauthorized physical access, damage, and interference.

13.2.2 Access rights to areas housing IT Assets shall be based on the principle of least privilege. Only individuals with a legitimate need shall be granted access.

13.2.3 AUBH shall ensure that sensitive and/or critical information processing facilities are appropriately equipped and maintained with security controls to safeguard the information contained within the facility against manmade or environmental threats.

13.2.4 Publicly accessible areas shall be appropriately isolated from information assets and information processing facilities.

13.2.5 All outgoing items, packages, and/or materials related to information security shall be registered and inspected by Security Staff. Security staff are managed by the Facilities Department.

13.2.6 Physical access to the information systems should be monitored to detect and respond to physical security incidents.

13.2.7 Cabling Security

13.2.7.1 The IT team shall also ensure that the cables are appropriately protected from unauthorized access, interception, damage, and/or interference. Access to patch panels and cabling rooms/ cabinets shall be controlled.

13.2.7.2 Cables will be clearly labeled and uniquely marked with an alphanumeric code at both ends.

13.2.7.3 Power and telecommunications cables shall be run underground and ceiling where possible.

13.2.7.4 Network cabling will be protected by conduit or suitable trunks and should not be run through public areas.

13.2.7.5 AUBH will ensure that network cabling and LAN connectivity points are not laid or installed in public access areas.

13.2.8 Alternate power sources like UPS shall be deployed to avoid disruption of service due to power failure in the server room. The specifications, policies, and procedures concerning UPS is managed by the Facilities Department.

13.2.9 Secure environments housing IT equipment will have at a minimum (server room and switch cabins):

- Dual air-conditioning
- Smoke and Fire Detectors
- Raised Flooring
- Uninterrupted Power Supply
- Suitable fire extinguishing equipment

13.2.10 Any inflammable or hazardous materials will not be allowed in or near the information processing facilities.

13.2.11 All environmental controls will be inspected periodically as per the Facilities Department policies and procedures.

13.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2023	8.17 Clock synchronization
ISO 27001:2023	Section 7.0 Physical Security which covers: a) Physical security Parameters b) Physical Entry c) Securing offices, rooms, and facilities d) Physical security monitoring e) Protecting against physical and environmental threats f) Working in secure areas g) Supporting utilities Cabling security

14.0 CLOUD SECURITY POLICY

14.1 Purpose

The purpose of a Cloud Security Policy is to establish guidelines, principles, and best practices to ensure the secure adoption, deployment, and management of cloud services within AUBH.

Key purposes of this policy include:

(a) Risk Management: Identifying, assessing, and managing the risks associated with cloud adoption and usage. This includes evaluating the security posture of cloud service providers, understanding the shared responsibility model, and implementing controls to mitigate identified risks.

(b) Compliance and Legal Requirements: Ensuring compliance with relevant laws, regulations, industry standards, and contractual obligations related to data protection, privacy, and security. This may include standards such as PDPL, ISO/IEC 27001, and others.

(c) Data Protection and Privacy: Establishing policies and procedures to safeguard sensitive data stored, processed, or transmitted through cloud services. This includes implementing encryption, access controls, data classification, and data loss prevention measures to protect confidentiality, integrity, and availability.

(d) Identity and Access Management: Defining roles, permissions, and authentication mechanisms to ensure that only authorized users and devices have access to cloud resources. This includes implementing strong authentication, Multi-Factor Authentication (MFA), identity federation, and least privilege principles.

(e) Security Configuration and Monitoring: Establishing guidelines for configuring and securing cloud environments, services, and applications. This includes defining secure baseline configurations, patch management processes, logging and monitoring requirements, and incident response procedures.

(f) Vendor Management: Establishing criteria for evaluating, selecting, and managing cloud service providers based on their security capabilities, performance, reliability, and compliance with contractual requirements. This includes conducting due diligence, performing security assessments, and establishing contractual agreements to ensure that security expectations are met.

14.2 Policy

The ICT Department shall:

14.2.1 Develop business requirements for cloud outsourcing with criteria and processes for identifying critical or important systems.

14.2.2 Identify risks associated with outsourcing each cloud service, which includes information and communication technology, information security, business continuity, legal and compliance, reputation, operations, and possible oversight limitations; and assess its impact and develop a plan to manage it.

14.2.3 Perform due diligence of potential CSPs for a service before the selection. This shall include CSP's security controls, certifications, and compliance.

14.2.4 Ensure that the CSP complies with internationally recognized information security standards and has implemented appropriate information security controls.

14.2.5 Cover the following aspects while developing a contract for cloud services:

- Location in which data is stored.
- Situations in which the client has the right to terminate the agreement.
- Dispute resolution.
- Information security.
- Data confidentiality, ownership, and control in compliance with local laws.

- Business continuity management and disaster recovery.
- Security audit.

14.2.6 Ensure that the respective rights and obligations of a licensee and the CSP are set out in a legally enforceable written agreement.

14.2.7 Ensure that information security roles and responsibilities between the licensee and the CSP, including threat detection, incident management, and patch management, are clearly defined and agreed contractually.

14.2.8 Ensure that strong authentication mechanisms and access controls are implemented to prevent unauthorized access to the licensee's data and back-end cloud resources.

14.2.9 Implement MFA for accessing sensitive cloud services, administrative interfaces, and privileged accounts.

14.2.10 During the change of CSP or termination of the services, ensure that all data is securely removed from the cloud service provider's infrastructure and that no residual data remains.

14.2.11 Implement secure baseline configurations for cloud services based on industry best practices and vendor recommendations. This shall be reviewed once every 6 months, and configurations to address security vulnerabilities and emerging threats.

14.2.12 Ensure the security posture of third-party vendors and subcontractors is monitored and assessed, especially in relation to cloud services and data.

14.2.13 Implement controls to manage third-party risks associated with cloud access, such as vendor assessments, security reviews, and contractual obligations.

14.2.14 Ensure that cloud resource ports are not publicly open; only necessary ports should be allowed, and access should be restricted to specific IP ranges.

14.2.15 Ensure that cloud resources should be accessible only through VPN; a VPN tunnel has been established between the cloud and on-premises systems.

14.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2022	5.23 Information Security for the use of cloud services

15.0 SERVICE REQUEST AND INCIDENT MANAGEMENT POLICY

15.1 Purpose

The purpose of this policy is to provide a structured approach for managing ICT service requests and incidents, ensuring timely and efficient resolution to support the operational needs of AUBH. It encompasses the management of both service requests and incidents, including cybersecurity incidents, to minimize disruptions and ensure the continuity of business operations.

15.2 Policy

15.2.1 Service Request Management

15.2.1.1 Service Request Categories

- Standard Requests: Routine tasks such as software installations, hardware setup, and access requests.
- Complex Requests: Tasks requiring significant resources, custom configurations, or multiple departments.

15.2.1.2 Request Submission

- Service Requests: Submitted via the Ross Helpdesk system or by email, including detailed information about the required service or issue.

15.2.2 Incident Management

15.2.2.1 Incident Categories

- IT Incidents: Events impacting the confidentiality, integrity, and availability of IT systems.
- Cybersecurity Incidents: Events involving unauthorized access, cyber-attacks, or data breaches.

15.2.2.2 Incident Submission

Incident Reports: Submitted via the Ross Helpdesk system or by email, including detailed information about the incident.

15.2.2.3 Incident Handling and Cybersecurity

- Detection and Documentation: All IT and cybersecurity incidents are detected as soon as possible and properly documented.
- Authorized Personnel: Incidents handled by appropriate authorized personnel.
- Root Cause Analysis: Performed to prevent recurrence, identifying and addressing weaknesses.
- Monitoring: Mechanisms in place to detect incidents, including network, infrastructure, and endpoint monitoring.

15.2.2.4 Cyber Resiliency

- The six pillars of cyber resiliency to minimize cyber risks:
    - Prepare: Employee cybersecurity awareness programs.
    - Identify: Sensitive information processes and associated threats.
    - Predict: Technologies and practices to predict cybersecurity attacks.
    - Protect: Safeguards for critical infrastructure and services.
    - Detect: Mechanisms to identify potential threats.
    - Respond: Activities to accelerate remediation and contain impact.
    - Recover: Systems and plans to restore data and services.

15.2.2.5 Incident Response Phases

- Cybersecurity incidents should be addressed through the following phases:
  - Preparation
  - Identification
  - Assessment
  - Containment
  - Eradication
  - Recovery
  - Follow-up

15.2.2.6 Evidence Preservation

- All evidence of incidents should be preserved for a minimum of 12 months.

15.2.3 Service Level Objectives (SLOs)

- Service requests and incidents are prioritized based on urgency, impact, and resource availability.
- The SLOs for helpdesk and technical support are structured based on the severity level of issues:

Severity Level	Description	Average Response Time	Average Resolution Time
Severity 1 (Critical)	System outages halting critical operations, significant operational impact on a large number of users, high financial loss, or reputational damage potential.	30 minutes	4 hours
Severity 2 (High)	Significant degradation affecting system efficiency, operations can continue with workarounds, impacting a moderate to large user base.	1 hour	8 hours
Severity 3 (Medium)	Issues that do not significantly impact overall system functionality but affect a smaller group of users.	1 hour	24 hours
Severity 4 (Low)	Minor issues, suggestions for enhancements, or non-critical concerns affecting very few users.	4 hour	72 hours

15.2.4 Communication

- Regular Updates: To users on the status of their requests and incidents.
- Documentation: Clear records of actions taken and resolutions provided.
- Follow-up: Ensuring user satisfaction and closure of requests/incidents.

15.2.5 Performance Monitoring

- Track and report on service requests and incident metrics to ensure adherence to the defined Service Level Objectives (SLOs). The following additional metrics and KPIs will be monitored:
  - User Satisfaction: Aim for a user satisfaction rating of 90% or higher based on post-resolution surveys.
  - First Call Resolution Rate: Aim to resolve 80% of service requests on the first call/contact.

- Backlog of Requests: Maintain less than 10% of service requests pending beyond the defined resolution times.
- Security Incidents: Aim to detect and respond to security incidents within 1 hour and keep the number of breaches and compliance incidents to zero.

15.2.6 Continuous Improvement

- Annual review of service request management policies and procedures.
- Implement changes based on user feedback and technological advancements.
- Training and development for ICT staff to enhance service delivery skills.

15.2.7 User Responsibilities

- Prompt Reporting: Users must report issues promptly and provide necessary information for resolution.
- Compliance: Adherence to ICT policies and procedures.

15.2.8 Escalation Procedures

- In the event of service disruptions or failure to meet SLAs, the following escalation procedures will be followed:
  - Tier 1: Helpdesk support technicians – through the helpdesk system.
  - Tier 2: ICT team leads or specialists – directly via email or on Teams.
  - Tier 3: ICT management or director – directly via email or on Teams.

15.2.9 Feedback

- Systematically gather and incorporate user feedback to continually improve ICT services.
- Feedback will be collected through surveys and regular review meetings, with quarterly reports on feedback results and actions taken.

15.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2022	5.24 Information security incident management planning and preparation
ISO 27001:2022	5.25 Assessment and decision on information security events
ISO 27001:2022	5.26 Response to Information Security incidents
ISO 27001:2022	5.27 Learning from Information Security Events
ISO 27001:2022	5.28 Collection of Evident

ISO 27001:2022	6.8 Information security event reporting
NIST	PR. IP-9 Response Plans
NIST	RS. AN – 2 The impact of the incident is understood
NIST	RS. AN – 4 Incidents are categorized consistent with response plans
NIST	RS.MI – 1 Incidents are contained
NIST	RS.MI-2: Incidents are mitigated
NIST	RS.IM-1: Response plans incorporate lessons learned.
NIST	RC.RP-1: A recovery plan is executed during or after a cybersecurity incident.
NIST	RC.IM-1: Recovery plans incorporate lessons learned.
NIST	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

16.0 SECURED SOFTWARE DEVELOPMENT POLICY

16.1 Purpose

The purpose of the Secured Software Development Policy is to define the practices to be followed during the development of software/systems (developed internally or outsourced) at AUBH, in a way that maximizes its security. Secure development will contribute to the availability, integrity, and confidentiality of the software/system and information maintained within the software/system, by ensuring that as many vulnerabilities as possible are identified, designed to handle them, and tested before the software/system is deployed in the live environment.

This policy serves several key purposes:

- Security Integration: It ensures that security considerations are integrated into every phase of the software development process, from requirements gathering and design to coding, testing, deployment, and maintenance. By embedding security from the outset, the Policy aims to minimize vulnerabilities and risks associated with the software.
- Risk Reduction: The Policy aims to mitigate security risks by implementing secure coding practices, adhering to industry-standard security protocols, and leveraging security testing techniques such as static analysis, dynamic analysis, and penetration testing. This helps identify and address security flaws and weaknesses before software is deployed.
- Compliance: The Policy ensures compliance with relevant regulatory requirements, industry standards, and contractual obligations related to software security. Compliance with standards such as ISO/IEC

27001, NIST SP 800-53, OWASP, and PDPL may be addressed within the policy to ensure that software development practices align with established security benchmarks.

- Protection of Assets: The policy aims to protect critical assets, sensitive data, intellectual property, and customer information by building secure software that guards against unauthorized access, data breaches, and cyber threats. This helps safeguard the organization's reputation, financial resources, and competitive advantage.
- Efficiency and Cost-effectiveness: Incorporating security into the SDLC from the early stages helps avoid costly rework, security patches, and remediation efforts later in the development lifecycle. This results in more efficient development processes and cost-effective maintenance over the software's lifespan.

This policy applies to all software or systems developed internally or externally for the use of AUBH.

16.2 Policy

16.2.1 General

16.2.1.1 AUBH must develop, operate, and maintain its systems following this policy.

16.2.1.2 Introducing new systems and major changes to existing systems must follow a formal process of security risk assessment that includes analysis of the impacts of the changes on the users and the environment. System rollback plans shall be in place to bring the system back to its older state.

16.2.1.3 A system development plan shall be created for each engagement. It shall address the areas of planning, gathering requirements and analysis, design, development and coding, testing, deployment, and maintenance aligned to the selected software development life cycle.

16.2.1.4 Third-party vendors must meet the policy requirements when developing systems.

16.2.1.5 Threat modeling shall be done to assess the potential threats to the system and design controls to address them.

16.2.1.6 Release of systems functionalities must be done only after successful testing and approval.

16.2.2 Secured System Development Environment

16.2.2.1 Risks associated with the development of individual systems shall be evaluated.

16.2.2.2 Secure development environments shall be established for specific system development efforts.

16.2.2.3 System source code shall be protected from all forms of unauthorized access and tampering by safeguarding the development, build, distribution, and update environments and following the least privilege principle.

16.2.2.4 All development projects must exhibit a separation between production, development, and testing environments.

16.2.2.5 Developers must not have access to production environments, if required, temporary access shall be provided after getting the appropriate approvals from the customer or system owner.

16.2.2.6 Systems accounts and access permissions must be based on the least privileges required to perform the task.

16.2.3 Software Development Lifecycle Requirement

16.2.3.1 Information security requirements must be identified using various methods such as deriving compliance requirements from policies and regulations, threat modeling, incident reviews, or the

use of vulnerability thresholds. The results of the identification should be documented and reviewed by all stakeholders.

16.2.3.2 Information security requirements and controls should reflect the business value of the information involved and the potential negative business impact, which might result from a lack of adequate security.

- Information security requirements should as a minimum consider:
- The level of confidence required towards the claimed identity of users, to derive user authentication requirements.
- Access provisioning and authorization processes, for business users as well as for privileged or technical users.
- The required protection needs of the assets involved, regarding availability, confidentiality, and integrity.
- Requirements derived from business processes, such as transaction logging and monitoring, and nonrepudiation requirements.
- Requirements mandated by other security controls, e.g., interfaces to logging and monitoring or data leakage detection systems.

16.2.3.3 Solution and infrastructure design shall be developed considering the non-functional requirements like availability, scalability, maintainability, security, performance, fault tolerance, etc.

16.2.3.4 Criteria for accepting products should be defined which cover security requirements as well.

16.2.3.5 Solution design must ensure the integrity of data within the system.

16.2.3.6 The following factors shall be considered while designing Infrastructure and solutions.

- Secure connection parameters between the user and the system resources shall be established, such as the use of HTTPS where needed such as with login forms, digital signatures, and encryption where sensitive data are in transit.
- Tested preventive measures shall be in place to protect the system from Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks.
- Proper use of authentication mechanisms such as identity management and password policies/ complexities enforcement shall be used.
- Secure session establishment and termination between the users and the resources shall be incorporated.
- Multi-factor authentication in high-risk systems shall be implemented where possible.
- Users and system activities in the systems shall be logged and monitored where possible for auditing and reference purposes.

16.2.3.7 Secured coding guidelines and techniques shall be followed throughout the SDLC.

- Ensure code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle.
- Ensure code provides predictable execution or justifiable confidence and that the software, when executed, will provide security functionality as intended.
- Coding techniques must address injection flaws, particularly SQL injection, buffer overflow vulnerabilities, cross-site scripting vulnerabilities, improper access control (insecure direct object reference, failure to restrict URL access, directory traversal, etc.,), cross-site request forgery (CSRF), broken authentication and session management.
- Data validation checks shall be applied to all sources of incoming data. The application must validate input to ensure it is well-formed and meaningful.
- Disable Error messages that return any information to the user.
- Use environment variables prudently and always check boundaries and buffers.

16.2.3.8 Testing

- A thorough test and verification should be done during the development processes. Test plans and test cases must be created to ensure test coverage and test results must be documented.
- While testing the solution, test data shall be prepared in such a way that there is no personally identifiable information or confidential information is used.
- Identifiers that will help to identify personal or any confidential information shall be sanitized.

16.2.3.9 Change Management

- Changes to information resources shall be managed and executed according to a formal change control process. The process will ensure that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
- Production release: Changes should not be implemented directly to the production information systems without an impact assessment of such changes and the approval of other authorized personnel.
- Production Deployment: Implementation must only be undertaken after appropriate testing and approval by the stakeholders.

16.2.3.10 Handling production data for reproduction of issues

- Sensitive production data should not be replicated in a testing environment without the approval of the Information Security Officer and Information Asset Owner. If data is replicated to the test environment to test and reproduce any issues, it shall be deleted as soon as an issue is identified and fixed.

16.2.3.11 Security Testing in the Production Environment

- Vulnerability Assessments such as penetration testing and web application security testing shall be conducted after approval of the Information Security Officer and top management.
- Scope of such testing should be limited to find out potential vulnerabilities and disruptive testing, Denial of Service, etc. should not be done during testing,

16.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2022	8.4 Access to Source Code
ISO 27001:2022	8.25 Secured Development Life Cycle
ISO 27001:2022	8.26 Application security requirements
ISO 27001:2022	8.27 Secure system architecture and engineering principles
ISO 27001:2022	8.28 Secured Coding
ISO 27001:2022	8.29 Security testing in development and Acceptance
ISO 27001:2022	8.31 Separation of development, test and production environments
ISO 27001:2022	8.32 Change Management
ISO 27001:2022	8.33 Test Automation
ISO 27001:2022	8.34 Protection of Information Systems during audit testing
NIST	PR.DS-7: The development and testing environment(s) are separate from the production environment
NIST	PR. IP-2: A System Development Life Cycle to manage systems is implemented

17.0 THIRD-PARTY PROVIDER MANAGEMENT POLICY

17.1 Purpose

To establish guidelines for managing relationships with ICT third-party providers (i.e., vendors and third-party suppliers), ensuring effective delivery of products and services while maintaining high standards of security, compliance, and performance. This policy aims to safeguard AUBH's sensitive information, intellectual property, systems, and assets from potential threats arising from external interactions.

17.2 Policy

17.2.1 Third-Party Provider Selection

17.2.1.1 Selection Criteria: Third-party providers will be selected based on their ability to meet AUBH's technical, security, and service requirements, including reputation, service quality, cost-effectiveness, and compliance with industry standards.

17.2.1.2 Provider List: A comprehensive list of all third-party providers providing support to ICT environments will be maintained.

17.2.2 Contract Management

17.2.2.1 All third-party provider agreements must be documented and reviewed by the ICT Department.

17.2.2.2 A Non-Disclosure Agreement must be signed before sharing information with third-party providers.

17.2.2.3 Contracts should clearly define/state, where applicable:

- Service levels
- Performance metrics
- Security and privacy obligations
- Penalties for non-compliance
- Compliance with relevant laws and regulations
- The right to audit the supplier's security controls
- Who is responsible for managing data and under what circumstances

17.2.2.4 Regular audits and reviews of third-party provider performance and compliance with contract terms should be carried out at least annually

17.2.3 Security and Compliance

17.2.3.1 Security Policies: Third-party providers must comply with AUBH's security and data handling policies and Bahrain Data Protection Law. This is required before accessing Information Assets.

17.2.3.2 Security Assessments: Comprehensive security assessments, including security audits, risk assessments, and due diligence checks, must be conducted before engaging third-party providers. Regular security assessments and audits will be conducted to ensure compliance.

17.2.3.3 Incident Reporting: Third-party providers must report any security incidents or breaches immediately.

17.2.3.4 Access Controls: Access to systems, data, and facilities must be granted to third-party providers on a need-to-know and least-privilege basis.

17.2.3.5 Information Security Measures: Information on measures taken by the third-party provider to ensure adequate information security, data security, and confidentiality must be collected and evaluated.

17.2.3.6 It must be ensured that outsourced system development adheres to the 16.0 Secured Software Development Policy.

17.2.3.7 Assess the business continuity and disaster recovery processes of service providers before engaging in managed service models (IaaS, PaaS, SaaS).

17.2.4 Performance Monitoring

17.2.4.1 Monitoring and Auditing: Conduct regular monitoring and evaluation of third-party providers' performance against agreed-upon SLAs. Annually audit third-party providers' security controls to verify compliance.

17.2.4.2 Reviews: Perform quarterly performance reviews and hold feedback sessions with third-party providers.

17.2.4.3 Improvement Plans: Develop and implement corrective actions and improvement plans for underperforming third-party providers.

17.2.4.4 KPIs: Establish key performance indicators (KPIs) and regularly evaluate these measurements to assess third-party providers' performance.

17.2.5 Communication

17.2.5.1 Channels: Establish clear communication channels and designate points of contact for third-party provider-related issues.

17.2.5.2 Updates: Conduct regular meetings and provide updates to ensure alignment with AUBH's goals and requirements.

17.2.5.3 Documentation: Maintain documentation of all communications and decisions related to third-party provider management.

17.2.6 Termination of Services

17.2.6.1 Procedures: Establish procedures for the termination of third-party provider services, including proper notice, transfer of data, and return of assets.

17.2.6.2 Continuity: Ensure continuity of services and minimal disruption during the transition to the new third-party provider.

17.2.7 Risk Management

17.2.7.1 Risk Assessment and Management: Conduct risk assessments for each third-party provider to identify potential risks and their impact on AUBH. Develop a comprehensive risk management plan for the evaluated risks, particularly those associated with outsourcing specific services.

17.2.7.2 Risk Mitigation: Develop contingency plans and risk mitigation methods for identified hazards.

17.2.8 Onboarding and Offboarding

17.2.8.1 Onboarding

- Procedure: Establish a comprehensive and systematic onboarding procedure for new third-party providers.

- Documentation: Ensure all required paperwork, including contractual requirements as specified under 17.2.2 Contract Management, are completed and signed.
- Orientation and Training: Provide orientation and necessary training to the third-party provider's team regarding AUBH's policies, procedures, security protocols, and performance expectations.
- Access to IT Assets and Information Assets: Grant access to relevant systems, data, and facilities in line with the policies set in the ICT Policy.
- Performance Metrics Setup: Define and agree upon KPIs and SLAs with the third-party provider. Establish a baseline for performance monitoring.

17.2.8.2 Offboarding

- Procedure: Establish a comprehensive and systematic offboarding procedure for the third-party provider when their services are no longer required.
- Access Revocation: Revoke all system, data, and facility access granted to the third-party provider. Ensure all credentials and access permissions are disabled promptly.
- Data Handling: Ensure secure data destruction or return of any data, documents, or digital assets held by the third-party provider. Confirm the completion of data handling processes through certification or verification.
- Asset Return: Facilitate the return of any physical assets or equipment provided to the third-party provider. Conduct an inventory check to ensure all assets are returned in good condition.
- Final Assessment: Conduct a final performance assessment to document the third-party provider's service delivery and compliance during their engagement. Identify any unresolved issues or pending deliverables.
- Documentation: Document the offboarding process, including the return of assets, data destruction verification, and access revocation. Maintain records for compliance and future reference.
- Feedback and Improvement: Gather feedback from internal stakeholders, where applicable, regarding the third-party provider's performance. Use this information to refine the onboarding and offboarding processes and improve future third-party provider engagements.

17.3 Related References

Standard/ Framework	Compliance Requirement
ISO 27001:2022	5.19 Information security in supplier relationships
ISO 27001:2022	5.20 Addressing information security within supplier agreements

18.0 RELATED DOCUMENTS AND REFERENCES

- Academic Year Preparation Process
- IT Service Level Agreement
- IT Assets Growth Plan
- Approved software list

- Finance and Accounting Policy
- Employee Human Resources Handbook
- Delegation of Authority Policy
- Asset Disposal Policy

POLICY HISTORY			
Date of Last Action	Action Taken/Changes	Authorizing Entity	Effective Date