7.c. Data Security

Subject	Health Safety and Environment	***Effective From***	Sep - 2011
Policy #	7.c.	***Latest Revision***	Dec - 2023
Title of The Policy	Data Security	***Next Review***	Dec - 2024
Responsible Entity	Information Technology Center	***Policy Pages***	4

Definitions	**User:** the person who uses the computer to do his tasks, such as; academic and administration staff, and students. **AAU:** Al Ain University **Computer:** any computerized material belongs to Al Ain University with its own software and hardware that is designed to present a computing source to accomplish a specific task. **Computer Life cycle:** the period that the user can use the computer and get all its' functionalities. **Functionality Evaluation:** a process of evaluating the computer and determine if it is still in use or it should be replaced. **Performance update:** a process of increasing the specifications and performance of the computer and update the installed softwares which will increase the computer performance. **Software:** program used to do special tasks.
Purpose	Outlines the mechanisms to secure the IT systems and infrastructure against security risks. As well as to ensure the protection of AAU's information resources from unauthorized access or damage, and to provide. This policy is applicable to all AAU students, faculty and staff and to all others granted use of AAU's information resources. • Ensures protection against the potential consequences of breaches of confidentiality, failures of integrity, or interruptions of the service availability in both campuses. • Ensures that all AAU's information assets as well as computing and network facilities are protected against damage, loss, or misuse. • Ensures that all staff, students, and faculty members of AAU are aware of, and comply with, the principles of electronic information use. • Increases awareness and understanding of information security requirements across AAU. • AAU information used in the scope of teaching, learning, research, or administration is unadulterated. AAU provides safe access to this information through up to date secure procedures and security devices and systems. • Information Technology Centre develops and publishes security controls to ensure University information is properly protected, and review and update these controls as necessary to ensure compliance with the up to date security industry. Increases awareness on the part of the users of their direct responsibilities for protecting the confidentiality and the integrity of the data they own or handle.

Scope	This policy is applied to the following categories of security within the AAU: • Computer system and application security • Physical security • Operational security • Procedural security • Network security
Statement	AAU is dependent on the availability and integrity of its computer-based IT services for many aspects of teaching, learning, research and administration. It is essential to protect IT systems and infrastructure against security risks, whether internal, external, deliberate or accidental. All members of AAU community are responsible for awareness of and compliance with mechanisms and regulations that ensure: • Information is protected against any unauthorized access. • Information confidentiality is assured. • Information integrity is maintained. • Information availability is maintained. • Legislative and regulatory requirements are met. • Business continuity plans are developed, tested, and maintained. • Information security awareness training is available for faculty members, students and staff members. • All actual or suspected information security breaches are reported to ITC for thorough investigations. • Rules exist to support this Policy and its Procedures, including internal virus control measures, passwords, and continuity plans. • Business requirements for availability of information and systems are met. • Any kind of system is not allowed on network without anti-virus program. • Update of all anti-virus software on regular basis and verify the systems. • Verification that all downloaded files via e-mail are free of viruses. • Servers are equipped with anti-virus program with high efficiency of virus protection. • All the unfixed media are inspected and scanned for viruses before use by the user. • Infected files will be isolated and kept in the Quarantine System and user will be informed. ITC will provide the appropriate solution • Users will be allowed to use a memory chip (USB) in their computers, after checking to verify that they are free of viruses before use. • All outgoing and incoming e-mails will be scanned to ensure that they are free from viruses and harmful content. • Infected emails will be isolated and kept in the Quarantine System and user will be informed. ITC will provide the appropriate solution. • User will not have any admin access to enable or disable features of Antivirus software. • Compromised user/system will be taken off the network and kept in isolation until further clearance from ITC. • Any phishing or spam email or content will not be accessed by user without instructions from ITC. • All granted types of access for AAU internet published services are secured through

updated security policies applied to security firewall. Redundant security firewalls reliable and secure 24/7 access to AAU internal resources.

- AAU has reliable and redundant network in each level which enables Faculty, administration staff and students to use information technology and to access information resources from inside and outside university.
- AAU ITC team is responsible to provide physical security to the university resources and assets. Data center is secured by finger print access and physical door lock keys and provide access only for authorized staff only. IDFs are secured by two level of physical security by locking the IDF door and locking the Rack door in order to protect to network devices.
- AAU has secured and reliable MPLS connection between Al Ain head quarter and Abu Dhabi campus to ensure that information technology resources are accessible to all users at each of the university campuses. AAU upgrades the bandwidth of this connection to match university needs and increase of the link usage.
- ITC is responsible for maintaining this Policy, and for providing support and advice during its implementation.

Procedures

Confidentiality and Privacy

All members of AAU Community are obligated to respect and to protect confidentiality of data. AAU does not monitor the content of personal web pages, e-mail, or other online communications. However, AAU reserves the right to examine computer records and monitor activities of individual computers upon approval by AAU Administration.

Access

No one in AAU is allowed to access confidential records unless specifically authorized to do so. Authorized individuals may use confidential records only for legitimate purposes. Technology assets must be kept in an appropriately secure physical location. The management team must ensure that controls are in place to avoid unauthorized intrusions into systems and networks and to detect attempts of such intrusions.

Accountability

Members of AAU community are responsible for ensuring that others do not use their system privileges. AAU authorized staff are responsible for reviewing the audit logs and identifying potential security violations. All controlled systems should maintain audit logs to track usage information up to a level appropriate for each system. If an AAU authorized staff member suspects that a security breach has occurred, he/she must immediately notify the immediate supervisor.

Authentication

Authentication for point-to-point communication is implemented for all systems that send or receive data.

Availability

Mission critical systems are expected to be available at all times. Each critical system must be redundant and should have detailed recovery procedures, and specific notification for downtime periods. Data backup procedures should be tested and well documented.

	Reporting Violations Owners of computer, network, and applications systems, and users of these systems, have the responsibility to report any apparent security violations. Guidelines for reporting violations must be available to all users and management teams. These guidelines should provide guidance on what, when, where, to whom, and within what time frame the violation should be reported. The concerned user(s) must be notified in case of a breach.
Recent Changes	