
 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Policies Manual		Policy Number	IT-06
			Effective Date	12-Aug-2018
	Subject Information Security		Most Recent Review Date	15-Apr-2018
			Due Date for Next Review	01-Sep-2021
	Responsible Office: Chief Information Officer		Page Number	1 of 2

6. Information Security

Overview

Outlines the mechanisms to secure the IT systems and infrastructure against security risks.

Scope

Applies to the following categories of security within the UAEU:



1. Computer system and application security
2. Physical security
3. Operational security
4. Procedural security
5. Network security

Objectives



1. Ensures protection against the potential consequences of breaches of confidentiality, failures of integrity, or interruptions of the service availability.
2. Ensures that all UAEU's information assets as well as computing and network facilities are protected against damage, loss, or misuse.
3. Ensures that all staff, students, and faculty members of UAEU are aware of, and comply with, the principles of electronic information use.
4. Increases awareness and understanding of information security requirements across the UAEU.
5. Increase the users' awareness of their direct responsibilities for protecting the confidentiality and the integrity of the data they own or handle.

Policy

1. UAEU 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 risk.
2. All members of UAEU community are responsible for awareness of and compliance with mechanisms and regulations that ensure:
 - a) Information is protected against any unauthorized access.
 - b) Information confidentiality is assured.
 - c) Information integrity is maintained.
 - d) Information availability is maintained.
 - e) Legislative and regulatory requirements are met.
 - f) Information security awareness training is available for faculty members, students and staff members.
 - g) All actual or suspected information security breaches are reported to DoIT for thorough investigations.

 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Policies Manual	Policy Number	IT-06
		Effective Date	12-Aug-2018
	Subject Information Security	Most Recent Review Date	15-Apr-2018
	<i>Responsible Office:</i> Chief Information Officer	Due Date for Next Review	01-Sep-2021
		Page Number	2 of 2

- h) Rules exist to support this Policy and its Procedures, including internal virus control measures, passwords, and continuity plans.
 - i) Business requirements for availability of information and systems are met.
 - j) Any kind of system is not allowed on network without anti-virus program.
 - k) Update of all system components and software on regular basis and verify the systems.
 - l) Verification that all downloaded files via e-mail are free of viruses.
 - m) Servers are equipped with anti-virus program with high efficiency of virus protection.
 - n) All the unfixed media are inspected and scanned for viruses before use by the user.
3. 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.
 4. All outgoing and incoming e-mails will be scanned to ensure that they are free from viruses and harmful contents.
 5. The mail server will be updated periodically with the latest software (service packs/patches) for anti-viruses.
 6. Infected emails will be isolated and kept in the Quarantine System and user will be informed. DoIT will provide the appropriate solution.
 7. User will not have any admin access to enable or disable features of Antivirus software.
 8. Compromised user/system will be taken off the network and kept in isolation until further clearance from DoIT.
 9. Any phishing or spam email or content will not be accessed by user without instructions from DoIT.
 10. All UAEU operated computers and servers that are compatible with Active Directory (AD) and connected to UAEU network must be a member of the UAEU's enterprise domain
 11. DoIT is responsible for maintaining this Policy, and for providing support and advice during its implementation.

 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Procedures Manual	Related Policy	IT-06
		Effective Date	12-Aug-2018
	Subject Information Security	Most Recent Review Date	15-Apr-2018
		Due Date for Next Review	01-Sep-2021
	<i>Responsible Office:</i> Chief Information Officer	Page Number	1 of 1

Procedures of Policy No. (6) - Information Security

1. Confidentiality and Privacy

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

2. Access

No one in UAEU 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.

3. Accountability

Members of UAEU community are responsible for ensuring that others do not use their system privileges. UAEU 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 a UAEU authorized staff member suspects that a security breach has occurred, he/she must immediately notify the immediate supervisor.

4. Authentication

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

5. Availability

Mission critical systems are expected to be available 99.9%. Both mission critical systems and critical systems must be redundant and should have detailed recovery procedures, and specific notification for downtime periods. Data backup procedures should be tested and well documented.

6. 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.