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 UAEU.
5. 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.

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.
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) Business continuity plans are developed, tested, and maintained.
   g) Information security awareness training is available for faculty members, students and staff members.
   h) All actual or suspected information security breaches are reported to UITS for thorough investigations.
   i) Rules exist to support this Policy and its Procedures, including internal virus control measures, passwords, and continuity plans.
   j) Business requirements for availability of information and systems are met.
   k) Any kind of system is not allowed on network without anti-virus program.
   l) Update of all anti-virus software on regular basis and verify the systems.
   m) Verification that all downloaded files via e-mail are free of viruses.

n) Servers are equipped with anti-virus program with high efficiency of virus protection.
o) 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 content.
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. UITS 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 UITS.
9. Any phishing or spam email or content will not be accessed by user without instructions from UITS.
10. UITS is responsible for maintaining this Policy, and for providing support and advice during its implementation.