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 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.

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.