

 جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	Information Technology Procedures Manual	Related Policy	IT-02
		Effective Date	01-Sep-2014
	Subject Access Control	Most Recent Review Date	01-Dec-2013
	Responsible Office: Chief Information Officer	Due Date for Next Review	01-Sep-2016
		Pages of these Procedures	1 of 5

Procedures of Policy No. (2) - Access Control

1. User Access Management

a) User Registration

- (i) The User ID Registration Procedure governs the authorization, deactivation and deletion of accounts.
- (ii) Authorized user accounts (UAEU users, third-party contractors/vendors, client representatives) shall be created/activated for a required period of time, as per the respective academic, administrative or business needs.
- (iii) User IDs should follow standard conventions relevant to User Name, Attributes, Distribution Lists, Security Groups Association, Mailbox properties, etc., as specified in the User ID Registration Procedure.
- (iv) Authorization:
User accounts are only to be created, deactivated or deleted following the approval of the correct authority. It is the responsibility of the authorized personnel who creates user accounts to confirm that the correct level of authority has been granted whenever and wherever required.
- (v) Traceability:
 - Unique User Accounts are to be created so that the identity of all users can be established at all times during their computer and related facilities usage.
 - Periodic User ID reconciliation will be performed.
 - A unique reference number will be attached to each User ID Creation Request, to enable reverse traceability.
- (vi) Accountability:
The User ID Registration Procedure contains specific responsibilities for personnel operating critical functions in the creation, discontinuation and deletion process for User IDs or other functions. These procedures ensure that there are no conflicts of interest, such as a requester being also an approver.

b) Privilege Management

- (i) Access to operating systems and applications is to be generally restricted to designated administrators and staff members who are associated with the management and maintenance of the respective platforms.
- (ii) Users are assigned specific account profiles and privileges as defined and authorized by their respective function head in accordance with their particular function or role.
- (iii) User privileges are to be reviewed on a regular and frequent basis (the interval of review is established by the agreement with data custodian or system owner) and necessary action must be taken based on the outcome of the review process. Access will be revoked where the circumstances of those who have been granted privileges no longer allowed such access.

 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Procedures Manual	Related Policy	IT-02
		Effective Date	01-Sep-2014
	Subject Access Control	Most Recent Review Date	01-Dec-2013
	Responsible Office: Chief Information Officer	Due Date for Next Review	01-Sep-2016
		Pages of these Procedures	2 of 5

c) Password Management

The assignment/use of passwords is controlled in accordance with the defined Password Policy.

d) Review User Access Management

- (i) UITS will have in place procedures by which identified teams review the occurrences of User IDs and access rights.
- (ii) Bi-annual audits will ensure that the access rights and User IDs of users who have left the Institution have been removed.
- (iii) A process shall be in place to ensure that access rights of users who have been transferred to different locations, different departments, etc. are changed in light of the change in job requirements and are modified accordingly in the system. This process is activated following HR notification.
- (iv) The users' access rights are reviewed at regular intervals.

e) Unattended User Equipment

- (i) All computers belonging to UAEU Network must be password-protected with a standard screen saver.
- (ii) Active Sessions are disconnected after a pre-defined time frame.
- (iii) Users shall be advised to terminate unattended active sessions.
- (iv) Users are responsible not to leave their computers unattended.
- (v) The general best practice for enabling automatic lockout of a screen saver is to set the timeout to 15 minutes, so that it can provide adequate security and not be inconvenient to the user.

f) Broadcast Message

- (i) Important announcements are conveyed to the UAEU community via mass email broadcast.
- (ii) The Information Technology Department under the CIO controls the access to and dissemination of message broadcasts.
- (iii) Only authorized staff members are allowed to send broadcast email messages.
- (iv) The broadcast access request is managed and controlled based on UITS Signatory Authority, which clearly sets forth the authority and approval required.

2. Network Access Controls

a) User Authentication for External Connections

- (i) VPN (Virtual Private Network) connectivity shall be provided to remote users with proper approvals.
- (ii) Encryption shall be enabled to encrypt the traffic between client and server for remote users.

b) Network Perimeter Security

- (i) Internal networks shall be protected and separated from the Internet and other organizations' networks through firewalls.
- (ii) Border routers/firewalls shall be configured to prevent IP spoofing, denial of service, and other common Internet-based attacks.

 جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	Information Technology Procedures Manual	Related Policy	IT-02
		Effective Date	01-Sep-2014
	Subject Access Control	Most Recent Review Date	01-Dec-2013
	Responsible Office: Chief Information Officer	Due Date for Next Review	01-Sep-2016
		Pages of these Procedures	3 of 5

(iii) Firewalls shall be specifically configured to deny all incoming connections except the ones that are specifically required for process or business requirements and have been formally documented and approved. Any connection from the external network must be provided through firewall with proper approvals.

c) Server Security

- (i) No server shall be exposed directly on the Internet. All servers and/or servers under UAEU UITs custody shall be placed on internal zone of the firewall.
- (ii) Servers that are accessible from the Internet shall be deployed in a DMZ (Demilitarized Zone) and IP addresses shall be NATed (Network Address Translation).
- (iii) All servers shall be hardened as per the specified Hardening Documents provided by hardware and operating systems supplier.
- (iv) Servers should be deployed in a different VLAN (Virtual Local Area Network).
- (v) All servers on UAEU network shall maintain clock synchronization to ensure that audit trails are accurate.

d) Network Equipment Security

- (i) Diagnostic/externally accessible/dial-up ports shall remain disabled on all the active network elements and systems, unless specifically opened for some particular activity such as business/client requirements, activities such as PT (Penetration Testing)/VA (Vulnerability Assessment), etc. Appropriate approval from UITs shall be obtained prior to commencing the activity.
- (ii) All network elements on the UAEU network shall maintain clock synchronization to ensure that audit trails are accurate.

e) Internal Network Security

Network devices shall be configured to ensure that user access to systems is restricted to required services and unlimited network roaming is avoided. This is to be accomplished by:

- (i) Segregating production networks from non-production networks.
- (ii) Segregating networking equipment and servers from user environment.

f) External Network Security

- (i) All connections for Internet browsing from within UAEU network shall go through defined proxy servers only.
- (ii) All external customer connections to UAEU over the Internet shall be secured through the use of VPN (Virtual Private Network).
- (iii) All external access requirements shall be subject to a risk assessment based on business requirements of access and shall be authorized only after all security controls that are required to ensure that external access architecture are secure, and have been implemented and verified.

g) Network Change Management

All changes to the network architecture or configurations on the network elements that could impact security (movement of servers, addition of new servers and network devices, etc.) shall follow the defined UITs Change Management Process.

 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Procedures Manual	Related Policy	IT-02
		Effective Date	01-Sep-2014
	Subject Access Control	Most Recent Review Date	01-Dec-2013
	Responsible Office: Chief Information Officer	Due Date for Next Review	01-Sep-2016
		Pages of these Procedures	4 of 5

3. Operating System Access Control

a) Secure Log-on Procedures

- (i) Access to information services shall be made available via a secure log-on process. The procedure for logging on to a computer system shall disclose minimum information about the system in order to prevent unauthorized users from accessing unnecessary information.
- (ii) The log-on procedure includes, but not limited to, the following characteristics:
 - All systems shall have a standard log-on banner configured, clearly stating that the system is for authorized UAEU users only and may be monitored.
 - The log-on procedure shall not detail errors during log-on.
 - Systems shall be configured to lock the user account after predefined unsuccessful attempts.
 - Unsuccessful log-on attempts for all users shall be logged.
 - All log-on attempts for critical users (viz. system administrators, DBAs (database administrators), network administrators, etc.) shall be duly logged and maintained for a predefined period.

b) User Identification and Authentication

- (i) All users (including technical support staff, such as operators, network administrators, system programmers and database administrators) shall have a unique identifier (user ID) so that activities can subsequently be traced to the responsible individual. User IDs should not give any indication of the user's privilege/organizational level, e.g. manager, supervisor.
- (ii) Shared IDs are not allowed. All authorized users on a particular system will be made part of a separate group so that an audit trail can be maintained.

c) Password Management System

A password management system helps user to select strong passwords and enforces certain password guidelines, which users should follow. The password management system in use shall have the following features, as a minimum:

- (i) The system should only allow the selection of passwords as described in the Defined Password Policy.
- (ii) The system should allow users to change their passwords.
- (iii) The system should be able to maintain password age and history as defined in the UAEU Password Policy, and prevent re-use based on the same.
- (iv) The system should not store the passwords in clear text. It should store passwords using encryption.
- (v) The system should force the users to change temporary passwords on their first log-on.
- (vi) The system should not display passwords on screen when they are being entered.
- (vii) The system should provide confirmation when passwords have been successfully changed.

d) Use of System Utilities

Most computer installations have one or more system utility programs (e.g. Editors, Compilers, NTbackup, Disk Defragmentors, etc.) that might be capable of overriding system and application controls. It is essential that their use is restricted and tightly controlled. The following should be adhered to, as a minimum:

 جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	Information Technology Procedures Manual		Related Policy	IT-02
			Effective Date	01-Sep-2014
	Subject		Most Recent Review Date	01-Dec-2013
	Access Control		Due Date for Next Review	01-Sep-2016
	Responsible Office: Chief Information Officer		Pages of these Procedures	5 of 5

- (i) All systems shall be configured with minimal access rights, and only as per the user requirements. All system installations will follow the system hardening Policies.
- (ii) No third-party utilities shall be installed on any system without prior authorization from UITs.

e) Session Time-out

Terminal time-out is required to close the connection after a defined period of inactivity. Terminal time-out for customer systems shall be configured based upon technical or security requirements specified by the customers. For UAEU systems, the following should be configured:

- (i) Telnet/SSH session: Wherever active, inactivity time-out for network devices shall be configured for a period not more than five minutes.
- (ii) Other Internal Applications (viz. Client/Server, Web-based, etc.), developed/acquired would also include session time-outs, as defined.

f) Limitation of Connection Time

- (i) The period shall be defined during which connections to computer services are allowed for high risk/critical systems.
- (ii) The duration of active sessions shall be defined.

4. Application and Information Access Control

a) Information Access Restriction

Users shall be given access to information based upon business requirements only. Role-based permissions shall be configured. Business applications at UAEU shall have the following controls:

- (i) Access shall be given to business-required menu options according to the needs of the user and as explicitly defined in the application-specific documentation.
- (ii) Access rights shall be controlled based upon the business requirement and as defined in the system-specific documentation.
- (iii) Applications shall produce defined output according to roles set out in the application-specific documentation.

b) Sensitive System Isolation

Sensitive systems may require a dedicated (isolated) computing environment. The sensitivity may indicate that the application system should run on a dedicated computer or should share resources only with trusted applications/systems. Judgments are made on a case-by-case basis under authorization and control by UITs.

5. Mobile Computing and Communications

All mobile computing devices authorized by UAEU are allowed to connect to the UAEU network. All devices must comply with UAEU mobile computing rules.