 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Network Security	Last Review date	10/05/2024
	Policy Number	ITC-24	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Overview

UoS ensures the stability of the network communication and its security. The appropriate network security can protect all information from unauthorized modification or disclosure. In addition it protect the whole system from unauthorized access and denial of service. The Network Security Policy dictates the statements on Network Security Management processes to ensure protection of the University of Sharjah's information and information assets.

Scope


This policy is applicable to all systems, and information processing facilities, personnel as well as all third-party personnel who are connected to the University of Sharjah's information assets and systems.

Purpose

The purpose of this policy is to outline and establish guidelines for managing security of the University of Sharjah's IT network infrastructure and to ensure secure IT operations of information processing facilities.

Policy

- Access to physical and logical configuration of the University of Sharjah's network shall be restricted to authorized personnel only.
- Only authorized individuals shall be allowed to access UoS's network, and shall use the systems designated for their specific usage to perform authorized activities only.
- All network related setup, configurations and modification shall follow specific documented procedures and change/release management process.
- Network administration is allowed only over secure channels (SSH, HTTPS)
- Management traffic shall only be accepted from authorized management networks.
- Remote access rights to the internal network shall not be granted unless approved by appropriate process
- Special controls (e.g., firewalls) with appropriate access control rules shall be established to safeguard systems connected to public (or shared) networks (e.g., the Internet).
- Network and security diagnostic tools and ports shall be used in a controlled manner and be closed and secured when not in use.
- There shall be a documented change management process for authorizing, activating and terminating all external network connections. Access to critical internal services shall abide same.
- Network connections associated with communication sessions shall be terminated as per the defined time period of inactivity.
- Network administrator shall implement appropriate security and operational controls for any network connections beyond the UoS's direct control based on the Change management process.


 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Network Security	Last Review date	10/05/2024
	Policy Number	ITC-24	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

- Appropriate network routing controls shall be deployed by network admin for protection of UoS network from external connections.
- Penetration tests shall be conducted on all business-critical systems at least once a year.
- The test and production facilities / environments shall be physically and logically separated in the network.
- All network and security devices shall be enabled to log security events.
- The network services function shall maintain the following details, at a minimum:
 - a. Up-to-date network diagrams
 - b. Network connectivity including details of routers, switches and links speeds
 - c. IP address details
 - d. Firewall details
 - e. Firewall rule base and descriptions
 - f. Access control lists of routers, switches and firewalls
- An operational level agreement (OLA) shall be documented to define the following:
 - a. Implemented security controls
 - b. KPIs to measure the effectiveness of the above controls
 - c. Service level targets related to availability of network services and the associated security controls
 - d. Criteria for reporting performance of network service to the management in order to identify scope for continual improvement
- University of Sharjah shall enable clock synchronization on all networking devices with agreed reference such as Universal Coordinated Time (UTC) to facilitate forensic analysis. Clock synchronization shall be continuously monitored to ensure its accuracy.

Procedures

Firewall and Intrusion Prevention System Security Policy

1. The firewalls implemented in UoS network shall have all unwanted and malicious services terminated, logs and alerts configured and access rules (required IP and ports) configured based on the security requirements.
2. Access control lists shall be documented and maintained by the network administrator. These shall be reviewed yearly.
3. All Firewall access shall be reviewed annually.
4. Remote access to firewall administration shall be restricted only to the network administrator and shall be allowed only through the use of secure access.
5. Any remote access over untrusted networks to the firewall for administration purpose must use strong 2 factor authentications.
6. Firewall logs shall be examined on a real time basis to determine if attacks have been detected. Records indicating the review of firewall logs shall be maintained.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Network Security	Last Review date	10/05/2024
	Policy Number	ITC-24	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

7. The firewall shall have enabled a “Deny all” approach and reject any kind of probing or scanning tool that is directed to it so that information is not leaked out by the firewall.
8. In case of incidents which require firewall downtime for reconfiguration, the below must be considered:
 - a. Secondary firewall shall be made operational.
 - b. After being reconfigured, the firewall must be brought back into an operational state.
 - c. Change to firewall configuration shall follow the Change Management Process.
9. Internal systems shall not be connected to the Internet without the network firewall.
10. All network and security devices and network links shall be configured in a high availability mode and shall be tested annually.
11. Intrusion prevention systems shall be deployed at critical segments in the network with appropriate policies and logs shall be reviewed on a real time basis.
12. The firewall and intrusion prevention systems configuration shall be backed up as and when changes are made to the device configuration so that in case of system failure, data and configuration files can be recovered within the acceptable period.
13. The Information Security Head, supported by internal auditor(s) shall have the right to audit the firewall and intrusions prevention systems configurations.
14. All terminations of external networks entry points must be guarded with a firewall.

Router and Switch Security Policy

1. All routers and switches shall be configured and implemented only by authorized personnel.
2. The routers and switches shall be configured to reduce risks of being compromised.
3. All network devices shall be placed in a room, free of electrostatic or magnetic interference and should have controls for temperature and humidity.
4. Any configuration changes to the router and switches shall be through change management process and should cause minimum disruption to UoS’s business.
5. All passwords used in the routers and switches should comply with the Password Policy.
6. Access control list must be configured to filter unwanted traffic from flowing in and out of UoS network.
7. All routers shall be configured as per the best practices.
8. All the routers must have a logon banner.

Reference

SI No	Standard Name	Control Reference
1	ISO 27001:2013	A.13.1, A.12.2, A.11.4, A10.6