UNIVERSITY
OF BAHRAIN

INFORMATION TECHNOLOGY

Operations Security Policy

Authority / Information technology Center

Effective: 17 March 2019

Table of Contents

POLICY TITLE

Title: Operations Security Policy

Policy Description: aims to outline the controls and measures over security operations.

Policy Scope:	☐ Academic ☒ Administrative ☐ Research ☐ Student ☐ general
Policy Status	☐ New policy ☒ Revision of existing policy
Approval Authority:	University of Bahrain Council
Authority/ Owner of Policy:	Information technology Center
Approval Date:	10 March 2019
Effective Date:	17 March 2019
Approval Date of Last Revision:	10 March 2019
Date of Next Revision:	
Related Documents:	None

Policy Stakeholders

☐ President

☒ Vice President

☐ Legal Advisor

☐ Deans

☒ Directors

☐ Faculty members

☐ Students

☒ Admin Staff

□ All University Affiliates

1 Policy Purpose

This policy aims to outline the controls and measures over security operations at the University of Bahrain (UOB).

2 Policy Scope

This policy applies to all UOB employees, students, contracted personnel, trainees, and third-party representatives who have been provided with access to any Information Technology (IT) assets and services.

3 Policy Statement

3.1 Infrastructure Management and Protection

- The configuration of servers, network security devices, firewalls, and other enterprise security technologies should be managed to provide consistent setup and document changes and ensure security requirements are maintained when the configuration changes.
- Risk assessment for all systems that receive, process, store, or transmit information periodically will improve the Security team's ability to understand and manage the risk faced by the confidentiality, integrity, and availability of these IT assets and the information that requires protection.
- All the information stored in the devices, documents, and technologies mentioned in the previous paragraph should be classified based on Law No. (16) 2014 "State Secret Law".
- Servers must be registered within the corporate enterprise management system.

- For security and maintenance purposes, only authorized personnel may monitor equipment, systems, servers, and network traffic.
- Servers should be physically located in an access-controlled environment.
- A Centralized Anti-virus server shall be deployed to check all the incoming and outgoing traffic.
- The security team shall centrally manage anti-malware activities. A central monitoring and logging console shall be deployed to monitor the status of pattern updates on all computers and log their activities.
- Anti-malware should be installed on all servers, including domain servers, file and print servers, Internet proxies, email servers, application servers, Internet gateways, and all servers in the testing environment.
- Any removable media should be scanned before use on servers.
- All servers shall be backed up in a manner that allows for complete server recovery, including the operating system and system state, as per the backup schedule.
- Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the server.
- Servers shall only host services they were designed and approved to host. For this policy, the term ‘services’ refers to specific services a server was designed to host, such as a website, file, print, DNS, DHCP, Telnet, or FTP. All services not required for system functionality are to be disabled.
- Automatic Antivirus pattern update should be configured in the Software and alert the detection in the server's central console.
- All the issues regarding access to IT infrastructure, including the areas containing it, should be by Access Control and Physical Security Policy.
- IT Center is responsible for scanning for all files, including compressed files sent as attachments in the incoming and outgoing mail (SMTP traffic), cleaning the malware detected automatically, and deleting the infected file to the quarantine folder if unable to clean it.

- All connections to networks outside the UOB premises, such as the Internet, must be protected by the IT Center with a firewall that filters incoming and outgoing network traffic against common threats.
- Isolation of sensitive systems shall be considered while designing the networks. Appropriate segmentation of the network should be considered to achieve this objective.
- Redundant provisions shall be made for critical network components to ensure the continuous availability of the network.
- UOB's Network Perimeter shall be protected using firewall and related technologies to enable:
  - Blocking unwanted traffic.
  - Directing incoming traffic to more trustworthy internal systems.
  - Hiding vulnerable systems from the external network.
  - Providing logs of traffic to and from the private network.
  - Hiding information like system names, network topology, network device types, and internal user IDs from the external network.

- To support recovery after failure or natural disaster, the IT Center shall take a backup of data and system configuration files.
- The IT Center shall back up and store the firewall configuration offsite when changes are made to it so that data and configuration files can be recovered in case of system failure.
- IT Center is responsible for ensuring that all enterprise information systems and any UOB information system hosting confidential data are protected by a network firewall and a host-based software firewall, both configured in "default deny" mode for incoming traffic and enforcing documented trust relationships for those systems.
- The IT Center should ensure that all workstations connected to the UOB's network have a host-based firewall configured appropriately for the system's security requirements and the classification of data stored therein.

- Configuration of network firewalls and host-based firewalls on enterprise information systems should be audited periodically to ensure consistency with the security requirements of the system(s) they protect.
- Once an incident has been detected, a secondary firewall should be made operational in case the firewall needs to be brought down and reconfigured.
- Internal systems shall not be connected to the Internet without a firewall. After being reconfigured, the firewall must be returned to an operational and reliable state. In case of a firewall break-in, the IT Center is responsible for reconfiguring the firewall to address any exploited vulnerability.
- The firewall software and hardware components shall be upgraded with the necessary modules to assure optimal firewall performance.
- IT Center should be aware of any hardware and software bugs and firewall software upgrades that the vendor issues.
- IT Center shall monitor the vendor's firewall mailing list or maintain contact with the vendor to be aware of all required upgrades. Before upgrading any firewall component, the firewall administrator must verify with the vendor that an upgrade is required. After an upgrade, the firewall shall be tested to verify proper operation.
- Any such upgrades to the firewall should follow the appropriate change management procedures.
- All Routers and Switches shall be configured and implemented only by IT.

3.2 Security Event Logging and Auditing

- Audit logs recording user activities, exceptions (i.e., errors or failures), and information security events should be generated corresponding with the security requirements of the system being monitored. Audit logs should be retained.
- The system administrator's activities should be audited, such as using privileged accounts.
- Audit logs should be periodically reviewed to detect information security violations.

- In arbitration, court cases, Statutory Requirements, Disciplinary Proceedings, or pending disputes, relevant Logs should be backed up in the media and kept in safe custody until the same evidence is completed.
- Logs generated from the anti-malware software will be classified.
- Clocks of systems being monitored should be synchronized regularly from an accurate time source.
- All servers & Applications shall maintain security Audit logs that include (at a minimum) the User ID, Date, Time, and Events.
- All servers shall log security Auditing events showing successful and unsuccessful events, including inappropriate access events configured as per the Minimum Baseline Security Standard (MBSS).
- Logging should be enabled for all firewalls and periodically reviewed for defective events.
- Firewall logs shall be examined weekly to determine if attacks have been detected. A record indicating the review of Firewall logs shall be maintained.
- The IT Center is responsible for assessing and reviewing information security policies periodically to ensure their continuity of effectiveness.
- Firewall capabilities for logging traffic and network events shall be enabled.
- Firewall Audit trail logs should cover errors, login/logout activity, connect time, use of system administrator privileges, inbound and outbound e-mail traffic, TCP network connect attempts, and inbound and outbound proxy traffic type.

3.3 Exceptions

All exceptions to this policy shall be explicitly reviewed by the chief of Information Technology and approved by the director of the IT Center. If exceptions exist, they shall be approved and valid for a specific period and reassessed and re-approved if necessary.

3.4 Enforcement

- Violations of this policy and supporting policies shall result in corrective action by management. Disciplinary action will be consistent with the severity of the incident as determined by an investigation and may include, but may not be limited to:
  - Loss of access privileges to information assets
  - Other actions deemed appropriate by Civil Services Bureau (CSB) rules.

4 Roles and Responsibilities

This section identifies those sharing specific policy responsibilities, such as Approval Authority and Policy owner.

- Chief of Information Technology
- Director of Information Technology Center