Insert the organization logo by clicking on the image icon

Operations Security Policy Template

Date:

**Document Control**

|  |  |
| --- | --- |
| **Document Title:** | Operations Security Policy Template |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  |
| **Publish Date:** |  |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 3](#_Toc97467464)

[2. Scope 3](#_Toc97467465)

[3. Policy 4](#_Toc97467466)

[3.1 Infrastructure Management and Protection 4](#_Toc97467467)

[3.2 Protection From Malware 4](#_Toc97467468)

[3.3 Mobile devices 5](#_Toc97467469)

[3.4 Network and Firewall Protection 5](#_Toc97467470)

[3.5 Backup and Recovery 7](#_Toc97467471)

[3.6 Security Event Logging and Auditing 7](#_Toc97467472)

[3.7 Vulnerability Assessment 8](#_Toc97467473)

[3.8 Penetration Testing 9](#_Toc97467474)

[3.9 Cloud 9](#_Toc97467475)

[4. Exceptions 10](#_Toc97467476)

[5. Policy Enforcement 10](#_Toc97467477)

Objective

This policy aims to outline the controls and measures over security operations at the <entity name>.

Scope

This policy applies to all <entity name>’s employees, contracted personnel, trainees, third party's representatives who have been provided with an access to any of Information Technology (IT) assets and services.

Policy

1. Infrastructure Management and Protection
2. The configuration of servers, network security devices, firewalls and other enterprise security technologies should be managed in a way that provides consistent setup, documents changes, and ensures security requirements are maintained when the configuration is changed.
3. Risk assessment for all the systems that receive, process, store or transmit information on a periodic basis will improve IT Security team’s ability to understand and manage the risk faced to the confidentiality, integrity and availability of these IT assets and the information that require protection.
4. IT security team is responsible for assessing and reviewing information security policies periodically assessed to ensure the continuity of effectiveness.
5. All the information stored in the devices, documents and technologies mentioned the previous paragraph should be classified based on Law No. (16) 2014 “State Secret Law”.
6. Servers must be registered within the corporate enterprise management system.
7. For security and maintenance purposes, only authorized personnel may monitor equipment, systems, servers, and network traffic.
8. Servers should be physically located in an access-controlled environment.
9. A Centralized Anti-virus server shall be deployed to check all the incoming and outgoing traffic through GDN and the Internet.
10. All the issues regarding the access to IT infrastructure including the areas containing it should be in accordance with Access control and Physical Security Policy.
11. Protection From Malware
	* 1. Anti-Malware activities shall be centrally managed by IT security team. Central monitoring and logging console shall be deployed to monitor the status of pattern updates on all the computers and to log the activities performed on them.
		2. Anti-Malware should be installed in all servers including domain servers file and print servers, Internet proxies, email servers, application servers and Internet gateways in addition to all servers in testing environment.
		3. Any removable media should be scanned prior to use on servers.
		4. IT security team is responsible for scanning for all files including compressed files sent as attachment in the incoming and outgoing mail (SMTP traffic), clean the malware detected automatically and delete the infected file to quarantine folder if unable to clean.
		5. Anti-virus mechanisms should be deployed on all systems frequently impacted by malicious software and ensure it is actively running and generating audit logs.
		6. Automatic Antivirus pattern update should be configured in the Software and alert the detection in the central console of server.
		7. IT security team should prohibit the use of unauthorized software. Please refer to Acceptable Use Policy.
		8. <entity name> must develop and preform user awareness program for malicious code countermeasures.
12. Mobile devices

Risks introduced using Mobile Devices should be managed by developing security procedures.

1. Network and Firewall Protection
2. <entity name>’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.

1. IT security team is responsible for ensuring that all enterprise information systems and any <entity name>’s information system hosting confidential data must be 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.
2. IT security team should ensure that all the workstations connected to the <entity name>’s network must have a host-based firewall configured appropriately for the security requirements of the system and the classification of data stored therein.
3. 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.
4. Once an incident has been detected and in case the firewall may need to be brought down and reconfigured, a secondary firewall should be made operational.
5. Internal systems shall not be connected to the Internet without a firewall. After being reconfigured, the firewall must be brought back into an operational and reliable state. In case of a firewall break-in, IT security team is responsible for reconfiguring the firewall to address any vulnerability that was exploited.
6. The firewall software and hardware components shall be upgraded with the necessary modules to assure optimal firewall performance.
7. IT security team should be aware of any hardware and software bugs, as well as firewall software upgrades that are issued by the vendor.
8. IT security team shall monitor the vendor's firewall mailing list or maintain contact with the vendor to be aware of all required upgrades. Before an upgrade of any of the firewall component, the firewall administrator must verify with the vendor that an upgrade is required. After any upgrade the firewall shall be tested to verify proper operation.
9. Any such upgrades to the firewall should follow the appropriate change management procedures.
10. All Routers and Switches shall be configured and implemented only by IT team.
11. All connections to networks outside the <entity name> premises, such as the Internet must be protected by IT security team with a firewall that filters both incoming and outgoing network traffic against common threats.
12. Isolation of sensitive systems shall be considered while designing the networks. Appropriate segmentation of network should be considered to achieve this objective.
13. Redundant provisions shall be made for critical network components to ensure the continuous availability of the network.
14. Servers shall only host services for which they were designed and approved to host. For this policy, the term ‘services’ refers to specific services that a server was designed to host such as a web site, file and print, DNS, DHCP, Telnet, or FTP. All services not required for system functionality are to be disabled.
15. Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the server.
16. Backup and Recovery
	* 1. All servers shall be backed up in a manner that allows for a complete server recovery, including operating system and system state as per the backup schedule.
		2. Backups and recovery process should be defined to comply with business continuity plans. And a backup policy must be agreed to collect backup copies of important data, software and preform test on them on time.
		3. IT team/<entity name> should provide documentation of backup and recovery which includes, information type to be backed up, scheduling, methods for performing, validating the information recovery, and labeling backups.
		4. The firewall configuration shall be backed up and stored offsite as well by IT security team when changes were made to the firewall configuration so that in case of system failure, data and configuration files can be recovered.
		5. To support recovery after failure or natural disaster, backup of data files as well as system configuration files shall be taken by IT security team.
17. Security Event Logging and Auditing
18. 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.
19. The activities of the system administrator should be audited, such as the use of privileged accounts.
20. Audit logs should be periodically reviewed to detect information security violations.
21. Event logs recording user activities, exceptions, faults shall be produced, stored, and regularly reviewed.
22. The Information systems should be configured to notify and alert administrative staff or IT security team by a Security Information Event Management (SIEM) solution in case of unusual or suspicious activity is noted.
23. In the event of arbitration, court case, Statutory Requirements, Disciplinary Proceedings, or disputes pending, relevant logs should be backed up in a media and kept in safe custody till the completion of the same as evidence.
24. Logs generated from the Anti Malware software will be classified.
25. Clocks of systems being monitored should be synchronized regularly from an accurate time source.
26. All servers and applications shall maintain security audit logs that include (at a minimum) the User ID, date, time, and events.
27. Multifactor authentication must be implemented for accessing sensitive logs/records.
28. Audit logs to off-site facilities must be backed up.
29. All servers shall log security Auditing events showing successful and unsuccessful events, including inappropriate access events configured as per Minimum Baseline Security Standard (MBSS).
30. Logging should be enabled for all firewalls and periodically reviewed for defective events.
31. Firewall logs shall be examined on a weekly basis to determine if attacks have been detected. Record indicating the review of Firewall logs shall be maintained.
32. Firewall capabilities for logging traffic and network events shall be enabled.
33. 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 in-bound and out-bound proxy traffic type.
34. Vulnerability Assessment
35. <entity name> should determine the required vulnerability monitoring for system components.
36. Vulnerability assessment must be conducted every three months to detect system/device’s weaknesses.
37. Monitor and scan for systems/hosted applications’ vulnerabilities and when new vulnerabilities identified and reported.
38. Vulnerability monitoring tools must be utilized to automate the vulnerability management process.
39. Vulnerability monitoring tools should be updated to ensure quick identification of potential vulnerabilities.
40. Vulnerability monitoring includes scanning for ports, protocols, patch levels, functions, inaccessible services or improper configurations and operation.
41. Vulnerability scan reports and results must be continuously analyzed.
42. Reporting channel must be established for receiving reports of <entity name> systems’ vulnerabilities.
43. Penetration Testing
44. Penetration testing must be conducted annually on systems or individual components to identify vulnerabilities.
45. Cloud
46. Cloud environment shall be separated to development, testing and production environments. For the purpose of this policy:
* Cloud development environment is the setting where applications are developed using various procedures and tools.
* Cloud testing environment is the setting where applications are tested and debugged using various procedures and tools before being deployed into production environment.
* Cloud production environment is the setting where applications are actually put into operation for their intended uses by end users.
1. Appropriate Separation between development, testing and production environments shall be implemented for all Software/application development, database and activities in the cloud infrastructure.
2. Management and control of cloud environment shall be divided as follows:
* Private environment, the part that will not have any services that need to be accessed by external users, shall be managed and controlled by the entity based on <entity name>’s requirements.
* Public environment, the part that can host some services for external users, shall be managed and controlled by <entity name> based on its requirements.
1. Information custodians must protect the public and private networks in the production environment by:
* Preventing the use of testing and development identities and credentials for production information systems.
* Preventing access to compilers, editors and other tools from production information Systems.
* Using approved change management process for promoting software/application from development/testing to production.
* Prohibiting the use of live production environment data in development, test or training.

Exceptions

All exceptions to this policy shall be explicitly reviewed by the IT security department and approved by the <entity name> management. The exceptions to this policy if any shall be approved and valid for a specific period and shall be reassessed and re-approved if necessary.

Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-