Insert the organization logo by clicking on the image icon

 Desktop Security Policy Template

Date:

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Title:** | Desktop 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](#_Toc97457111)

[2 Scope 4](#_Toc97457112)

[3 Policy 4](#_Toc97457113)

[3.1 Desktop Protection 4](#_Toc97457114)

[4 Exceptions 5](#_Toc97457115)

[5 Policy Enforcement 5](#_Toc97457116)

# Objective

The objective of the Desktop Security policy is to provide a secure computing environment where data is processed. All desktops at the <entity name> shall be configured and used as per this policy.

# Scope

This policy applies to all <entity name> desktops used by <entity name> ‘s employees, contracted personnel, trainees and third party's representatives.

# Policy

## Desktop Protection

1. All the classified information regarding desktop and the surrounding areas should be in accordance with Law No. (16) 2014 concerning state secrets law.
2. Users shall ensure all confidential information in hardcopy or electronic form is secured in their work environment at the end of the day and once they are expected to leave for an extended period.
3. Confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
4. Confidential files must be kept in closed and locked cabinet when not in use or when not attended.
5. Key used for accessing confidential files or information must not be left at an unattended desk.
6. All the issues related to the password in desktop shall be in accordance with password security policy.
7. Passwords should not be left/written on sticky notes and left on/under a computer or in an accessible location.
8. The use of removable storage shall not be allowed, and such devices shall be disabled using appropriate registry settings (Ex: floppy’s, CD drives, memory sticks etc.] unless approved explicitly for business purposes.
9. Printouts containing sensitive or confidential information must be removed immediately from the printer.
10. Disposal of sensitive or confidential document should be shredded in the official shredder bins or locked in confidential disposal bins.
11. Whiteboards containing restricted/confidential information should be erased.
12. Computer workstations and laptops must be locked when workspace is unoccupied and shut completely down at the end of the workday.
13. Portable computing devices such as laptops and tablets should be locked away.
14. Information Technology (IT) team is responsible for managing and configuring antivirus for desktops.
15. It is the user’s responsibility to report any malicious activity and virus like activity to IT team.
16. No user shall have the privilege to disable the antivirus software on his/her desktop.
17. All desktops shall be configured to generate alerts at the central antivirus server as well as the infected desktop.
18. Where infected files have not been quarantined, these files shall be cleaned manually with the help of tools provided by the vendor or reliable third parties.
19. All virus-detected incidents shall be logged as deleted, quarantined, or cleaned by IT team.
20. Secure user profile and desktop settings for users shall be configured in a professional manner to protect confidentiality of data and computing facilities while in use.
21. Users should not be able to change the Web browser security settings.
22. Users at entity shall not be provided by local administrator privileges, the local administrator account shall be managed by IT team only.
23. Adding/removing programs should be disabled for users.
24. Access to registry editing shall be prevented.
25. All nodes on the network shall be monitored for patch deployment on a regular basis.

# Exceptions

1. All exceptions to this policy shall be explicitly reviewed by IT security team and approved by the management. The exceptions to this policy if any shall be approved and valid for a specific time 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-