Anti-Malware Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

# II. Purpose

The purpose of this policy is to describe the requirements for dealing with computer virus, worm, Trojan Horse, spyware, Ransomware, and other types of malicious software.

# III. Scope

This policy applies to all Staff that use ABC Company Information Resources.

# IV. Policy

The Chief Security Officer shall ensure:

* Procedures and tools exist to guard against, detect, and report malicious software. Centrally managed anti-malware software continuously monitors and defends Information Systems.
* IT personnel are trained and proficient in the use of the security solutions used to protect against malicious software. Where possible, anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) shall be enabled in an operating system or deployed through appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
* End users are aware of the security policies enforced on their workstations.
* Anti-virus software is installed at appropriate locations within organizational Information Systems including all systems commonly affected by malicious software (particularly personal computers and servers).
* Installed anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software including Ransomware.
* Systems considered to be not commonly affected by malicious software, receive periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
* Anti-virus mechanisms are properly maintained and kept current with the scanning engine and signature database updated every 12 hours per this policy.
* Periodic scans of the Information System shall be performed and audit logs generated and retained per Data Retention Policy requirements. Real time scan of files from external sources shall be performed as files are downloaded, opened, or executed.
* Devices are configured so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
* Anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. If anti-virus mechanisms are disabled, additional security measures may need to be implemented for the period of time during which anti-virus protection is not active.

All workstations whether connected to the ABC Company network, or standalone, must use the ABC Company IT approved virus protection software and configuration.

The virus protection software must not be disabled or bypassed.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Each file server attached to the ABC Company network must utilize ABC Company IT approved virus protection software and setup to detect and clean viruses that may infect file shares.

Each E-mail gateway must utilize ABC Company IT approved e-mail virus protection software and must adhere to the rules for the setup and use of this software.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the IT Help Desk.

Mobile Code shall be authorized before its installation and use. Anti-malware software shall ensure:

* Authorized Mobile Code operates according to a clearly defined security policy.
* All unauthorized Mobile Code is prevented from executing.

Malware actions (e.g. anti-malware software updates, definition updates, malware infections, Ransomware attacks, etc.) shall be logged with logs retained for one year to allow proper investigations into malware related incidents.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all Staff that use ABC Company Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO13.07, APO14.10, BAI04.05, BAI09.04, DSS04.05, DSS04.07, DSS05.02, DSS05.07

GDPR Article 25, 32

HIPAA 164.308(a)(5)(ii)(B)

ISO 27001 A.12.2

NIST SP 800-37 3.1

NIST SP 800-53 AC-19, PL-8, SC-3, SI-2-4

NIST Cybersecurity Framework DE.CM-4-5, RS.RP-1, RC.RP-1

PCI 5.1-4