Anti-Malware Procedure

|  |  |
| --- | --- |
| 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

This procedure provides detailed steps and actions to secure Information Systems per the Anti-Malware Policy.

# II. Purpose

The purpose of this procedure is to formally document the steps, actions, and processes needed to meet the requirements specified in ABC Company's Anti-Malware Policy.

# III. Scope

This procedure applies to all ABC Company Department Heads and IT Staff who administer networks.

# IV. Procedure

On an annual basis, end users receive security related training regarding malicious software. New Staff are trained within 30 days of, being granted access to any IT resources. Staff receive regular training, reference materials, and reminders that include malware related risks. For more information see the Security Awareness and Training Plan.

When new equipment is installed and, on a quarterly basis, IT Staff review configurations to ensure that centrally managed anti-malware software continuously monitors and protects Information Systems. Such software is reviewed to ensure it is capable of detecting, removing, and protecting against all known types of malicious software including Ransomware. Mechanisms are reviewed to ensure the scanning engine and signature database are updated every 12 hours.

On an annual basis, IT Staff receive security related training that includes security solutions used to protect against malicious software. Such training includes anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) configured to apply protection to a broader set of applications and executables.

On an annual basis, Information Systems considered to be not commonly affected by malicious software, receive evaluations by IT Staff to identify and evaluate evolving malware threats to confirm whether such systems continue to not require anti-virus software.

On a weekly basis, scans of Information Systems are performed with audit logs generated and retained per Data Retention Policy requirements. Real time scan of files from external sources are performed as files are downloaded, opened, or executed.

When new equipment is installed, and on a quarterly basis, IT Staff shall:

* Review devices to ensure they are configured to automatically conduct an anti-malware scan of removable media when inserted or connected.
* Ensure approved anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by the appropriate Department Head on a case-by-case basis for a limited time period.

The appropriate Department Head authorizes mobile code before its installation and use. Anti-malware software ensures unauthorized mobile code is prevented from executing and authorized mobile code operates according to a clearly defined security policy.

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

# V. Enforcement

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

# VI. Distribution

This procedure is to be distributed to ABC Company Department Heads and IT Staff who administer networks.

**Procedure History**

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