Ransomware 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

Ransomware is a type of malicious software (malware) that can deny access to files or data. The software has different variations that may lock a computer or device or encrypt files. Typically the software demands payment using electronic currency. Controls are needed to ensure ABC Company’s Information Systems are protected against new and emerging types of malicious software.

# II. Purpose

The purpose of this policy is to describe the requirements for managing risks related to Ransomware.

# III. Scope

This policy applies to the Chief Security Officer.

# IV. Policy

The Chief Security Officer shall ensure:

* The Risk Assessment, Risk Analysis, and Risk Treatment Plan identify Ransomware related risks and controls to address such risks. See the Risk Management Policy for more information.
* Policies, procedures, and tools are developed and maintained to prevent, detect, and take corrective actions to manage Ransomware related risks. See the Anti-Malware Policy for more information.
* 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. See the Anti-Malware Policy for more information.
* Spam filters are implemented to reduce the likelihood Staff will click on e-mail links or download malware attachments to their local devices. See the E-mail Policy for more information.
* Backups are performed per the Backup Policy and Backup Plan.
* End users receive the appropriate security education and awareness training and such training address risks related to Ransomware. See the Security Awareness and Training Plan for more information.
* Social engineering security assessments evaluate the effectiveness of the Security Awareness and Training Plan. See the Audit Policy for more information.
* Malware actions (e.g. anti-malware software updates, definition updates, malware infections, Ransomware attacks, etc.) are 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 the Chief Security Officer.

**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