**Security Policy:**

**Malware And Antivirus Policy**

This policy / procedure complies with the requirements of the ISO 27001:2013 International Standard

Annex A 12.2.1, 12.6.2

[**Company Name]**

[Address]

[City, State Zip]

**1. Purpose**

The purpose of this document is to define the policy and procedure requirements governing protection of in-scope information that is accessed, processed, or stored at remote teleworking sites.

**2. Scope**

This policy applies to information assets within the scope of the Information Security Management System (ISMS).

**3. Policy (A.12.2.1, 12.6.2)**

It is the policy of [Company Name] that information processing assets used to process, store and transmit in-scope information shall be protected from malware (e.g., viruses, ransomware,..) and that pro-active measures are established to assure ongoing protection as the malware threat profile changes. (All relevant requirements of the Acceptable Use Policy regarding installation of software and circumvention of anti-virus programs shall apply.)

**4. Responsibilities**

Roles and responsibilities regarding malware protection are as follows.

* Managers / supervisors are responsible for assuring that this policy is effectively communicated to staff.
* All users of information assets are required to comply with this and other applicable policies, and to submit to compliance audits of systems, assets, and information on request.
* Deliberate circumvention of this policy constitutes a breach of security and, upon detection, should be Immediately reported in accordance with the Incident Management Policy and Procedure.

**5. Requirements**

# Senior Security Lead Actions [list other title as appropriate]

* Promote protective and preventive user behaviors through Security Awareness Training.
* Conduct periodic reviews of the software and data content of systems supporting in-scope information processing, including the presence of any unapproved files or unauthorized changes;
* Establish protocols and processes for response to, and recovery from, malware incidents that prevent disruptions in security continuity.
* Conduct formal investigations of malware incidents in accordance with the Incident Management Policy/Procedure.
* Subscribe to sources of information about evolving malware threats and asset vulnerabilities to assure that current anti-malware measures are current. Communicate evolving threats and preventive steps to the organization.

# IT / Security Operations Actions

* Implement detection/prevention of unauthorized software use.
* Implement detection/prevention of known or suspected malicious websites.
* Install malware detection and repair software on every information asset that processes or stores in-scope information.
* Malware detection and repair software will, at a minimum:
  + scan ny files received over networks or storage medium, for malware before use;
  + scan electronic mail attachments and downloads for malware before use,
  + scan web pages for malware.
* Update malware profiles at least daily.
* Run malware detection scans on every information asset at least daily.
* Remove detected malware from information assets immediately.
* Isolate infected assets or environments to minimize impact on systems and information.

# User Actions

* Download and installation of application software from unapproved sources is prohibited. [Note: see the Approved Applications List located for the current list.]
* Users must refrain from clicking on any links or opening emails from unknown sources which can lead to introduction of malware or ransomware.
* Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc. is forbidden.
* Detection of malware by any User should be immediately reported to the **Senior Security Lead.**

**6. compliance**

1. Compliance to this policy will be promoted through onboarding and Security Awareness training, and through internal audits.
2. Compliance to this policy will be measured through remote audits, including personally owned assets that are used for business purposes. All equipment may be audited for content, configuration, and usage history at any time, by authorized auditors. [Auditors are authorized by the [senior security lead].
3. Compliance to this policy will be formally assessed through the ISMS annual surveillance audits, and the Internal Audit process.
4. Exceptions to the policy require advance approval of the **Senior Security Lead.**
5. Non-Compliance to the policy will be addressed through disciplinary measures defined in the HR Security Policy and may include revocation of teleworking privileges and/or termination.

**7. Malware and antivirus records**

* Anti-malware Scanning Logs
* Security Incident Log

**8. reference documents**

* Approved Applications List
* Incident Management Policy/Procedure
* HR Security Policy
* Acceptable Use Policy