|  |  |  |
| --- | --- | --- |
| Document ID  **ITSD105** | Title  **COMPUTER MALWARE** | Print Date  **mm/dd/yyyy** |
| Revision  **0.0** | Prepared By  **Preparer’s Name / Title** | Date Prepared  **mm/dd/yyyy** |
| Effective Date  **mm/dd/yyyy** | Reviewed By  **Reviewer’s Name / Title** | Date Reviewed  **mm/dd/yyyy** |
|  | Approved By  **Final Approver’s Name / Title** | Date Approved  **mm/dd/yyyy** |

**Policy:** The Company shall protect its Information Technology assets from infection by malicious software, or malware.

**Purpose:** To prevent data loss, corruption, or misuse of Company computing resources or information that may occur when malware is introduced to the Company Information Technology network.

**Scope:** This policy applies to all Company personnel and to all computer hardware and software comprising the Company’s Information Technology network.

**Responsibilities:**

The Information Technology Security Manager is responsible for implementing malware control procedures, training LAN Administrators and other Information Systems Department personnel, training users on computer malware control, and evaluating and updating appropriate computer malware detection software.

The LAN Administrator is responsible for coordinating actions required to prevent computer malware outbreaks, coordinating all actions required to eradicate the malware, and recovering data to the greatest extent possible.

The Tech Support Manager is responsible for installing and maintaining malware protection on Information Technology assets and for cleaning malware infections from Company applications, devices, etc.

Users are responsible for following the guidelines of this policy document and for immediately notifying the Information Technology Security Manager in the event a malware attack is suspected.

**Definitions:** Malware - Short for “malicious software”, malware is designed to damage, disrupt, or abuse an individual computer or an entire network and/or steal or corrupt an organization’s most valuable and sensitive data. Viruses, worms, and Trojan horses are examples of malware.

Spam or junk email – Unsolicited commercial email sent in bulk over the Internet. Spam puts a cost and a burden on recipients by clogging up network bandwidth, consuming disk space, and wasting employees’ time. Spam is frequently a malware vector.

Subscription service – A service whereby a software vendor offers support for its product, usually for a predetermined time period. Anti-virus vendors typically include a one-year subscription (for updates, notices, etc.) with the purchase of a product license. Many vendors offer fee-based subscription services whereby subscribers automatically receive notifications, security bulletins, etc., for a set period of time.

Target – The ultimate destination for malware; that which the malware is designed to attack. Boot sectors, hard disk drives, email servers, and departmental (HR, accounting, etc.) servers are examples of malware targets.

Vector – How malware is carried to a computer, server, or system.

**Procedure:**

### 1.0 MALWARE DEFENSE PLANNING

1.1 How does malware typically work and what threats exist? Malware is commonly passed to a potential target through email. The person who receives the email opens an attachment, which unleashes the malware, which then spreads to other computers via a shared network. (Malware may attack by other means but this is a common method.) To lessen the potential for damage to the Company’s Information Technology assets by malware, the Company should develop and implement a multifaceted approach to malware prevention.

1.2 To prepare the Company’s Malware Defense Plan, The Information Technology Security Manager shall review the following items:

* ITSD101-2 IT THREAT ASSESSMENT REPORT;
* ITAM102-5 IT ASSET INVENTORY DATABASE;
* ITAM102-6 IT NETWORK MAP;
* Information Technology Industry standards and best practices;
* Anti-malware vendor web sites or portals; and
* Information Technology security alerts and bulletins (many of which are available for free and as a subscription service).

1.3 The Information Technology Security Manager shall use the preceding items (and possibly others) to develop a Malware Defense Plan. This Plan shall be submitted to Information Technology Management for review and approval.

1.4 Upon Information Technology Management’s approval of the Malware Defense Plan, the Information Technology Security Manager shall implement the Plan, assign Plan responsibilities to members of the Tech Support Manager, and train (or supervise training of) Tech Support personnel.

The Information Technology Security Manager shall communicate the Plan to all employees except the Tech Support Manager and arrange employee training through the Human Resources department.

### 2.0 MALWARE DEFENSE PLAN

2.1 The Tech Support Manager shall install firewalls on all personal computers (workstations) and on all servers, in accordance with ITAM102 IT ASSET STANDARDS.

2.2 the Tech Support Manager shall ensure that operating systems, web browsers, email programs, and related software are configured for optimum security, also in accordance with ITAM102.

2.3 The Tech Support Manager shall install an anti-virus program on every PC and server (again, in accordance with ITAM102) and all anti-virus software shall be automatically updated through the use of a subscription service (updates should be automatically logged by the software).

* Additional anti-malware programs should be installed on all PC’s and servers to protect against nuisances such as spyware and adware, which are potential malware vectors.

2.4 As vendors learn of vulnerabilities (bugs) in their software and repair them, they notify registered users, post bulletins on their web sites, and notify news media that these patches are available for download. Many vendors offer subscription services, through which the Company may be notified of security threats and related issues and obtain software patches.

The Company should subscribe to one or more notification services, in order to maintain its awareness of threats and to ensure all software is updated in a timely fashion.

2.5 The Tech Support Manager shall evaluate all software patches (for operating systems, browsers, email programs, applications, etc.) for relevance and criticality. If the patch is determined to be relevant (for example, an operating system security patch has more relevance - and is certainly more critical - than a foreign-language update of an application), the Tech Support Manager shall install the patch in a test environment and verify its effectiveness and compatibility with existing software before installing it in the production environment. Such updates shall be logged by the Tech Support Manager, if the software being patched does not automatically log activity.

2.6 All anti-malware protections shall be configured so as to prevent their being disabled by users. Only the Tech Support Manager staff, the Information Technology Security Manager, and members of the Information Technology Security staff shall be allowed to temporarily disable anti-malware measures (for example, disabling a local anti-virus program to install and configure an application locally).

* Users shall not be allowed to install software. Only the Tech Support Manager shall be allowed to install approved software, in accordance with ITAM101 IT ASSET STANDARDS.

2.7 The Company shall minimize malware risks by backing up critical information, in accordance with ITSD104 IT DISASTER RECOVERY.

2.8 All users shall be trained on the Malware Defense Plan at the outset. Users shall be retrained (updated) on the Plan at least once a year. The Human Resources Manager shall be responsible for Malware Defense Plan training.

* All users shall sign a statement at the end of training, indicating that they have received training, that they understand the Plan, and that they will conduct their business in accordance with the Plan.

### 3.0 MALWARE DEFENSE PLAN REVIEW

3.1 The Tech Support Manager shall periodically (once a week is recommended) review all anti-virus, firewall, and other relevant logs to determine if the software is up-to-date and is performing as expected. The Tech Support Manager shall report its findings to the Information Technology Security Manager for possible action.

3.2 The Information Technology Security Manager shall periodically (monthly, at a minimum) review user satisfaction data (see ITAD110-2 IT USER SATISFACTION SURVEY) and security incident information (see ITSD110-1 IT INCIDENT REPORT and ITSD101-1 IT THREAT ASSESSMENT REPORT) to determine incident trends and progress toward Company goals.

3.3 Information Technology Management shall periodically (annually, at a minimum) meet with the Information Technology Security Manager to review the Malware Defense Plan, to determine its continuing applicability and conformity to Company requirements.

3.4 A periodic (at least annual) audit of the Malware Defense Plan shall be conducted by an accredited auditor, to determine if the Plan is in use, if it is functioning as expected, and if it conforms to standards and requirements. Information Technology Management shall review the results of such audits and reviews with the Information Technology Security Manager and recommend changes to the Plan.

3.5 In the event that anti-malware measures do not prevent malware from infecting any part of the Company Information Technology network, that event shall be handled in accordance with ITSD110 IT INCIDENT HANDLING.

### 4.0 MALWARE DEFENSE PLAN UPDATE

4.1 The Information Technology Security Manager shall incorporate updates into the Malware Defense Plan and ensure communication of Plan changes to all employees.

4.2 Within a month of changes being made to the Malware Defense Plan, Information Technology Management shall conduct a review with the Information Technology Security Manager to verify that changes were implemented and the desired results are being achieved.

### Forms:

* None.

### References:

1. **ISO/IEC 27002:2013 – INFORMATION TECHNOLOGY- CODE OF PRACTICE FOR INFORMATION SECURITY CONTROL**

For more, see <http://www.iso.org/iso/catalogue_detail.htm?csnumber=54533>.

1. **NIST SPECIAL PUBLICATION 800-83, REV. 1 (JULY, 2013) GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING FOR DESKTOPS AND LAPTOPS**

This publication provides recommendations for improving an organization’s malware incident prevention measures through several layers of controls. The guide gives extensive recommendations for enhancing an organization’s existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones.

The guide also focuses on providing practical strategies for detection, containment, eradication, and recovery from malware incidents in managed and non-managed environments. The recommendations in the publication address several forms of malware, as well as various malware transmission mechanisms, including removable media and network services such as email and Web browsing.

For details, see <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>.

### Additional Resources:

1. “Microsoft Malware Defense Guide” – <http://technet.microsoft.com/library/cc162791>.
2. Search Security – <http://searchsecurity.techtarget.com/>.
3. Computer Security Institute – <http://www.gocsi.com/>.
4. Virus Bulletin – <http://www.virusbtn.com/index>.
5. Computer Security Resource Center, Computer Security Division, NIST (CSRC) – <http://csrc.nist.gov/>.
6. The SANS Institute – <http://www.sans.org>.
7. SecurityFocus.com [(http://www.securityfocus.com/](http://www.securityfocus.com/)) facilitates discussions on security related topics, creates security awareness, and provides a comprehensive database of security knowledge and resources freely available to the public.
8. Microsoft Security Compliance Manager – <http://technet.microsoft.com/library/cc677002.aspx>.

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of Changes** | **Requested By** |
| 0 | mm/dd/yyyy | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |