

IT108 - Virus and Malware Protection Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.11 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[Document Control iii](#_Toc23349323)

[Introduction 4](#_Toc23349324)

[Purpose 4](#_Toc23349325)

[Audience 4](#_Toc23349326)

[Scope 5](#_Toc23349327)

[Policy Statement 5](#_Toc23349328)

[Enforcement 9](#_Toc23349329)

[Revision History 9](#_Toc23349330)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | December 19th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

This Policy addresses protecting Signifi information, computer, network and telephony resources against damage or destruction from viruses, trojans, worms or other forms of malicious code and software also collectively referred to as malware.

All Signifi owned or leased computer equipment must be setup in a secure fashion to protect the information contained on the system from any form of malicious code.

Virus or malware can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, memory sticks, and CDs. Virus and malware are usually disguised as something else, and so its presence is not always obvious. A virus or malware infection can be very costly to Signifi in terms of potential data loss, loss of staff productivity and/or damaged reputation.

Purpose

The purpose of this policy is to prevent malicious software such as virus or malware from harming any servers and corporate computing assets that are connected to the Signifi infrastructure.

Audience

This policy applies to all Signifi employees, associates, part-time and temporary workers, trainees, contractors, and vendors.

Scope

This policy applies to all users which include but not limited to employees, associates, contractors, part-time and temporary workers, trainees, service providers, and those employed by others to perform work at hosted or outsourced sites, or who have been granted access to Signifi information or systems. This policy applies to all Signifi resources owned, leased, or supported by Signifi, or any outside entity that has signed a Vendor Access Agreement with Signifi.

Policy Statement

The following steps must be adhered to by the user and/or IT Department:

1. IT Responsibilities
   1. Implement credible and reputable anti-virus software or malware protection system that should be capable of detecting, removing and protecting against malicious software.
   2. Ensure that anti-virus mechanisms are current, actively running, capable of generating logs and not alterable by the user. Logs must be retained for a minimum of one year, with three months immediately available for analysis.
   3. It is the responsibility of the Data Center Operations and IT Service Desk teams to have current virus definitions for Signifi approved anti-virus software definitions installed on all IT managed devices that are owned or leased by Signifi. The virus patterns for the software must be updated at least bi-monthly or preferably whenever a new update is available to ensure latest viruses are recognized and detected.
   4. The Information Security team will randomly check systems to ensure that the virus software is active, and all updates have been applied.
   5. Enable the built-in firewall that is included in major operating systems and/or install a firewall application on all corporate computers and servers (as required).
   6. Anti-Virus software must be enabled for automatic updates and periodic scans.
   7. Virus-infected computers must be removed from the network immediately. The computer must not be connected to the network again, until it is confirmed clean by an appropriate IT resource.
   8. Any external data introduced into the IT systems/network through mobile devices must be first scanned with an approved virus detection mechanism prior to being utilized, stored or installed on any system.
   9. Any standalone environment (e.g. Lab) must conform to this Policy unless otherwise approved by the Director of IT.
   10. In the event of a virus or malware detection and reporting, the IT Service Desk, Customer Support and Information Security teams will determine the impact of the virus on Signifi computing environment. Analysis should be given emphasis but not limited to the following:
   * Disconnect the affected system or systems (if it hasn’t already been disconnected by the associate) from the network immediately to prevent the virus or malware from spreading.
   * Examine all machines on the local network for signs of contamination. In most case, if one host has been compromised, others on the network have also been contaminated.
   * It may be necessary for Data Center Operations or IT Service Desk teams to shut down the data network, or portions thereof.
   * Install the latest update of the Signifi approved anti-virus software on isolated system(s), if required and run a full system scan.
   * Look for unusual or hidden files or directories on the system.
   * Check system binaries to make sure they have not been changed.
   * Check system or network configuration files for unauthorized entries.
   * Restore clean backups.
   * Once sure that the system/s are clean re-connect them to the network.
   * Closely monitor the affected network segment for an appropriate amount of time for signs of recurrence.
   * An event log of reported virus outbreaks must be maintained by Information Security that defines the origin and methods of eradication.
2. User Responsibilities
   1. Scan all email attachments before opening them. Email is a method to spread malicious program via attachments and IT has implemented controls to perform this function.
   2. Anti-virus solutions deployed on systems must not be disabled by an employee at any time.
   3. Contractors, vendors, or individuals whose computer device is not owned by Signifi must have updated anti-virus installed and operating before connecting it to the Signifi environment. All external parties are required to sign the Remote Vendor Access Agreement.
   4. Never open any files attached to an email from unknown, suspicious or untrustworthy source.
   5. Be suspicious of e-mail messages containing links to unknown web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link with the intention of secretly taking control of your system. Do not click on a link sent to you if you were not expecting a specified link.
   6. Signifi employees, associates and contractors must not intentionally write, generate, copy collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of or access to any Signifi computer, network or information. Such software, as previously defined, is known as a virus, worm, trojan or malware
   7. No associate should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the appropriate IT resource. The user must disconnect their computer from the network before calling the IT Service Desk to prevent the virus or malware from spreading. After disconnecting from the network do not shutdown the computer so that evidence is preserved.
   8. The infection must be reported to IT Service Desk. Report the following information (if known): virus name, extent of infection, source of virus and potential recipients of infected material.
   9. Signifi associates are not authorized to engage in any activity that is illegal under local, provincial, federal or international law while utilizing Signifi owned resources.
   10. While Signifi’ IT department desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Signifi. Personal privacy protection is NOT provided and must not be expected.
   11. Electronic assets and the information generated should be used for business purposes only. Official business is defined as any process that is in support of Signifi operations, management and primary business engagements. This definition also extends to any authorized agent, vendor, contractor, or other support personnel.
   12. Signifi reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Enforcement

All instances of non-compliance will be reviewed by the department director. The department director, with the assistance of the Human Resources department has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Update

This policy and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2019-12-05 | First version | Darace Rose |
| 1.1 | 2019-12-17 | Update template | Razvan Anghelidi |
| 1.11 | 2020-12-03 | Annual review | Razvan Anghelidi |
| 1.12 | 2021-12-12 | Annual review | Hadeel Alzuhairi |