

IT105   
Risk Management Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.12 |
| 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 11](#_Toc23349329)

[Revision History 11](#_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

Information Security threat and risk assessments form a part of the risk management process to ensure responsible management and security of information and information resources. Information security threat and risk assessments are conducted to evaluate the security threats and risks to information, programs, systems, services and physical spaces. Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what counter measures (safeguards and controls), if any, to take in reducing risk to an acceptable level (i.e., residual risk), based on the value of the information resource to the organization.

Purpose

The purpose of the Risk Assessment Policy is to empower Signifi Information Security team to perform periodic information security threat and risk assessments, including vulnerability assessments and penetration tests on corporate computer systems for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

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 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

1. Risk Assessment

**Annual Risk Assessment**

* 1. Information Security must ensure a formalized risk assessment based upon the methodologies outlined in “ISO 27005 – Information Risk Security Risk Management” or “National Institute of Science & Technology publication 800-30 – Risk Management Guide for Information Technology Systems” is performed on annual basis in order to identify possible threats and vulnerabilities to security of Signifi information systems and assets that may contain Highly Confidential and Confidential information. The risk assessments must also be performed following any major changes to the environment.

**Review and update of Information Security Policy:**

Following the execution of a risk assessment, Information Security shall provide a report to the Executive Management Team to consider and to address or mitigate any risks identified.

**Risk versus Cost Benefit Analysis**

* 1. The assessment of counter measures must be performed through a cost-benefit analysis where controls to mitigate risks are selected to reduce to a level acceptable to management. This analysis may be based on any of the following:
  + The cost of the control compared to the benefit of minimizing the risk.
  + Management’s appetite for risk (i.e., the level of residual risk that the management is prepared to accept).

1. Vulnerability Management

**Quarterly Internal Network Vulnerability Scanning**

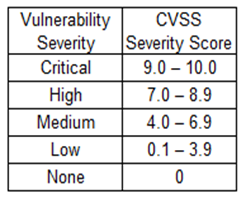
* 1. Vulnerability scans are performed by a qualified internal resource (e.g. an individual possessing formal training and appropriate information security related designation such as a CISSP). For internal vulnerability scanning, IT may instead choose to use an Approved Scanning Vendor that appears on the PCI Security Steering Committee website, or a qualified information security services organization;
  2. IDS/IPS technologies are configured to allow vulnerability scanners to successfully scan system components (e.g. adding appropriate exception rules to IDS/IPS configurations);
  3. Vulnerability scans are configured to make reasonable attempts at identifying live systems (e.g. using methods other than ICMP ping to identify ‘live’ hosts);
  4. Vulnerability scans are configured to scan all Transmission Control Protocol and User Datagram Protocol ports.
  5. Vulnerability scans are configured to perform OS and Service fingerprinting; and
  6. Vulnerability scans are configured to account for any load balancers that may be implemented.
  7. The above vulnerability scans must also be executed against all PCI in-scope systems after any changes to the components (including changes of software, configurations, application/OS patching etc.).

**Quarterly External Vulnerability Scan**

* 1. Information Security must ensure that a quarterly external vulnerability scan is performed by an Approved Scanning Vendor (ASV) that appears on the PCI Security Steering Committee website, against all public facing IP address spaces used by Signifi. This includes public facing interfaces for any remote offices that also have connectivity back to Signifi’s personal information data environment.
  2. The above vulnerability scans must also be executed against in-scope systems after any changes to the components (including changes of software, configurations, application/OS patching etc.). External scans performed after changes may be performed by qualified internal resources if desired and covered by the ASV during the next quarterly external scan.

**Identification of newly discovered vulnerabilities**

* 1. IT must establish a formalized process for identifying newly discovered vulnerabilities including but not limited to:
  + Subscribing to automated security notification feeds from operating system and application & database server vendors.
  + Subscribing to industry leading vulnerability disclosure databases (e.g. National Vulnerability Database, Qualys Vulnerability Database Notifications, Common Vulnerabilities and Exposures Database, etc.); and
  + Conducting a risk assessment of newly discovered vulnerabilities and implementing remediation procedures in alignment with the Patch Management Policy.
  1. Risk ranking of newly discovered vulnerabilities – Information Security must establish a formalized process for risk ranking newly discovered vulnerabilities based upon the following guidance:
  2. The Common Vulnerability Scoring System (CVSS 3.0) or a directly compatible alternative must be used with severity scores categorized in the table below:



|  |  |
| --- | --- |
| Vulnerability Severity | CVSS Severity Score |
| Critical | 9.0-10.0 |
| High | 7.0-8.9 |
| Medium | 4.0 – 6.9 |
| Low | 0.1 – 3.9 |
| None | 0 |

**Annual Web Application Vulnerability Assessments**

* 1. Information Security must ensure that all web applications that store, process and/or transmit Highly Confidential or Confidential information and/or public facing web applications are reviewed via manual and/or automated means on an annual basis in order to identify any vulnerabilities. At a minimum the scope of the testing must ensure web applications are assessed against industry accepted guidance (i.e. OWASP Top Ten or SANS Common Web Exposures Top 25). Alternately, IT may also implement a Web Application firewall in front of web applications in order to alleviate the requirement to perform annual web application vulnerability assessments. Remediation of identified vulnerabilities must follow the requirements specified within the Patch Management procedures.

The above testing must also be performed after any changes to application code and/or infrastructure configuration changes.

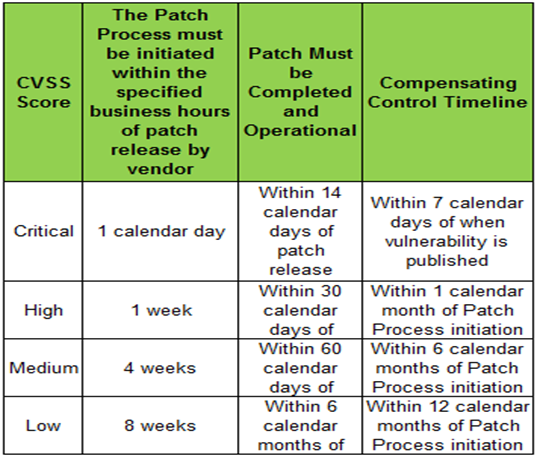
**Quarterly Wireless Access Point Review**

* 1. Information Security must perform a quarterly assessment to detect the presence of unauthorized wireless access points at Head Office locations throughout Signifi or within the personal information data environment. The following are acceptable methods to be used to detect unauthorized wireless access points:
  + Network Access Control/Wireless Intrusion Detection Systems (must be deployed across the entire environment to ensure all networked locations are covered) and must be configured to issue an immediate alert to network security personnel; and/or
  + Physical inspection using a wireless scanner at each designated physical Company location where Network Access Control/Wireless Intrusion Detection Systems are not deployed.
  + Any exceptions identified through the execution of the above testing must immediately be escalated via the established incident management procedure and protocol.

**Annual Network and Application Security Penetration Testing**

* 1. Information Security must engage a qualified security services vendor to perform against the following:
  + Company’s network perimeter.
  + All internal and external applications and system components considered part of the personal information data environment and or critical systems deemed necessary at the time of the assessment.

**Review and Remediation**

* 1. Information Security must ensure a formalized procedure for reviewing, risk assessing and formulating potential remediation options is developed and presented to designated business owners following the execution of the above noted testing and review activities. Threats or vulnerabilities that may pose a significant threat to Highly Confidential or Confidential information must immediately be escalated to the appropriate business unit.
  2. Vulnerability Management Timeline – At minimum, policies must ensure patching must be completed and operational within the timeline indicated below:  
       
     

1. File Integrity Monitoring
   1. IT must deploy file integrity monitoring tools on all systems considered part of the personal information data environment in order to detect and alert security personnel of unauthorized changes to critical files and/or system configurations. Comparisons of changed files must be performed at minimum on a weekly basis.

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 | 2020-12-01 | Annual review | Razvan Anghelidi |
| 1.12 | 2021-12-12 | Annual review | Hadeel Alzuhairi |