

IT120  
System Development and Infrastructure Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.04 |
| 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](#_Toc35542726)

[Introduction 4](#_Toc35542727)

[Purpose 4](#_Toc35542728)

[Audience 4](#_Toc35542729)

[Scope 5](#_Toc35542730)

[Policy Statement 5](#_Toc35542731)

[Enforcement 14](#_Toc35542732)

[Revision History 14](#_Toc35542733)

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 7th, 2021 |
| Shamira Jaffer | CEO | December 2nd, 2020 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Information security must be integrated into new application and systems development from their inception and throughout the development lifecycle. The details included in this policy are a minimum and must be considered in order to develop applications with enhanced security. This policy outlines Signifi requirements for securely designing, developing, testing and remediating vulnerabilities within software applications developed for, or customized by, Signifi.

Purpose

This policy articulates requirements for developing, configuring and maintaining secure applications and systems. Security best practices must be taken into consideration in all stages of the software development lifecycle; daily operations and infrastructure design.

Audience

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

Scope

This policy applies to all users which include but not limited to employees, 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. Include Information Security in all phase of the System Development Lifecycle

The Software Development Manager should ensure that information security requirements are integrated into all phases of Signifi System Development Lifecycle including but not limited to the following phases:

* Requirements specification;
* Design;
* Construction (coding and implementation);
* Integration;
* Testing and debugging (validation);
* Installation (deployment and post-implementation); and
* Maintenance.

1. Integrate security planning and requirements into the development of requirements specifications

The Software Development Manager should ensure information security requirements are identified, planned and integrated into business and technical requirements that form the initial requirements specifications for systems being developed and implemented at Signifi.

1. Architect and Design systems reflective of industry best-practices for Information Security Architecture

The Software development department manager should ensure that system-level security architectures are developed that reflect industry best-practice technical and administrative security controls designed to protect Signifi information systems and assets. These architectures should include:

* Detailed technical security design; and
* Detailed administrative security design (processes and procedures);

1. Review Security Architecture and Designs against Security Policy

The Software Development Manager must ensure that proposed and agreed security architectures are reviewed against Signifi Information Security Policy and note any gaps or deviations from the specified requirements. They should raise any threats that may not be covered by the existing Signifi Information Security Policy to the Information Security department’s review and direction.

1. Architect and Design secure systems that balance costs with risk mitigation

The Software Development Manager must ensure that a cost/benefit analysis of various proposed design options is performed in order to balance costs with appropriate risk mitigation measures while still achieving required compliance requirements.

1. Separate Development/Test and Production Environments

The Software Development Manager and QA Manager must ensure Custom Designed Software and/or Commercial Off The Shelf (COTS) Software that process Highly Confidential or Confidential data are developed in segregated development and test environment. This section is stipulated by clause 1.1 of IT104 - Signifi Access Control Policy.

1. Implement One Function Per Server

The IT Manager and Software Development Manager must implement, where possible, only one primary function (primary application) per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Where virtualization technologies are in use, implement only one primary function per virtual system component.

1. Segregation of Duties between Development, Test and Production Environments

The IT department must ensure duties between personnel assigned to access and/or support the development environments of Custom Designed Software and /or COTS that process Highly Confidential or Confidential data are logically and/or physically separated from those assigned to access and/or support the production environments. The use of segregated named IDs is required between environments with adequate monitoring controls implemented to ensure privileged user activities can be monitored and reviewed.

1. Use of live Personal Account Numbers (PANS) in development/test is prohibited

IT, Software Development Manager and QA manager MUST ENSURE Custom Designed Software and/or COTS that process, transmit or receive credit card data do not use live PANs for development or testing, and instead rely upon PANs generated specifically for development and testing only (usually provided by vendors).

1. Prevent common coding vulnerabilities

Software Development Manager must establish secure coding guidelines and training for developers and ensure secure coding techniques are used to address or mitigate common coding vulnerabilities, including:

* Common code injection flaws (including SQL, OS Command Injection, LDAP and XPath injection vulnerabilities);
* Buffer overflows;
* Insecure cryptographic storage;
* Insecure communications when transmitting Highly Confidential or Confidential data;
* Improper error handling vulnerabilities and unnecessary information disclosure;
* Cross-site scripting vulnerabilities;
* Cross-site request forgery vulnerabilities;
* Improper access control and privilege escalation vulnerabilities (e.cg. unsecured directories, unrestricted URL access, etc.); and
* Known ‘High’ risk vulnerabilities resolvable by code changes identified in the vulnerability identification process (see Information Security Risk Assessment Policy for additional details).

1. Storage of sensitive authentication data

IT and Software Development Manager must ensure Custom Design Software and/or COTS that process sensitive authentication data do not store this information (even if encrypted) once the data has been used for transaction authorization. Specifically, the following must be enforced:

Prevent storage of full contents of any track (magnetic strip on the back of a credit card) in any form;

* Prevent storage of card verification values also referred to as CVV2, CVC2, CID, or CAV2 data in any form; and
* Prevent storage of personal identification number (PIN) or encrypted PIN block in any form.

1. Mask PAN when displayed or printed

IT and Software Development Manager must ensure Custom Designed Software and/or COTS that have requirements to display PAN data (on screen or when printed) are coded to only display the first six and last four digits of the PAN.

1. Render PAN unreadable if stored

It is preference to implement tokenization solutions for all Signifi systems that are required to store, process and/or transmit cardholder and/or sensitive authentication data. Where the use of tokenization is not feasible, IT and Software Development Manager must ensure Custom Designed Software and/or COTS that have requirements to store PAN data in any location including but not limited to portable media, backups, log files etc. utilize one of the following approaches:

* One-way hash based on strong cryptography;
* Truncation; or
* Strong Cryptography with associated Key Management.

1. Use of strong cryptography when transmitting Highly Confidential or Confidential data over open, public networks

IT and Software Development Manager must ensure Custom Designed Software and/or COTS that have requirements to transmit Highly Confidential or Confidential data over open, public networks (e.g. not utilizing dedicated VPNs or MPLS connections) implement strong cryptography to secure the communication and transmission channel.

1. Sending of unprotected Highly Confidential or Confidential data via end-user messaging technologies is prohibited

IT and Software Development Manager must ensure Custom Designated Software and/or COTS do not send unprotected Highly Confidential or Confidential data via end-user messaging technologies (e.g. email, instant messaging, chat, etc.).

1. Authenticate all access to any databases containing Highly Confidential or Confidential data

IT must ensure that access to databases containing Highly Confidential or Confidential data require authentication and do not allow anonymous access.

1. Prohibition against Trap Doors to Circumvent Access Controls

Programmers and other technically oriented staff must not install trap doors that circumvent the authorized access control mechanisms found in operating systems and/or access control packages.

1. Vendor-Provided Written Integrity Statements

If outsourced vendor software is being written and/or used for Signifi applications, management must obtain a written integrity statement from the involved developer. The statement must provide assurances that the software in question does not contain undocumented features, does not contain hidden mechanisms that could be used to compromise the software’s security, and will not require the modification or abandonment of controls found in the operating systems under which it runs.

1. Auditing

Design and build the application with the ability to audit and log user access, important transactions, and changes to the application operating parameters. Code must also be commented so that any reasonably competent developer can follow the logic of the function to its completion.

* Audit logs must contain:
* All actions taken by any individual with root or administrative privileges;
* Access to all audit trails;
* Invalid logical access attempts;
* Use of identification and authentication mechanisms;
* User identification;
* Type of event;
* Date and time;
* Success or failure indication; and
* Identity or name of affected data, system component, or resource.

1. Debugging Tools

When using debugging tools, the log feature must not log Signifi sensitive data to the log file. When complete, the log files must be removed.

1. Review of custom code prior to release into production environments

Software Development Manager must ensure that all Custom Designed Software that store, process and/or transmit Highly Confidential or Confidential data undergo manual and/or automated review and reflect the following:

* Code changes are reviewed prior to release into production environments by Personnel and/or qualified third parties knowledgeable in secure coding techniques other than the originating code author;
* Documentation of independent review are created and/or maintained for auditability; and
* Code changes are reviewed and approved by Management to ensure secure coding guidelines have been adhered to.

1. Removal of test data and accounts prior to release into the production environment

IT, Software Development Manager and QA manager must ensure that all Custom Designed Software and/or COTS that store, process and/or transmit Highly Confidential data have been reviewed to ensure the removal of all test data and testing/temporary accounts prior to release into the production environment.

1. Perform adequate testing of code prior to release into production environments

Software Development Manager and QA manager must ensure appropriate test cycles are built into all development efforts. These may include:

* Unit Testing – Developers and then QA test and verify functionality of specific sections of code;
* Integration Testing – Developers and then QA test and validate interfaces between software and system components operate as designed;
* System Integration Testing – Developers and then QA test and verify that newly developed systems interact with external systems and operate to designed requirements and specifications;
* Regression Testing – Developers and then QA test the application code to ensure previous enhancements and bug fixes are not re-introduced and system operates to specifications;
* User Acceptance Testing – QA tests the system(s) with the end-users to confirm functionality meets specified requirements;
* Security Testing – IT performs vulnerability scanning and penetration testing as required and directed by PCI DSS; and
* Security testing should be performed under conditions as close to production conditions as possible.

1. Perform post-implementation reviews

Software Development Manager and QA manager must ensure systems are reviewed and accredited as being built and implemented to agreed design and functional specifications once systems are released into the production environment (and prior to go-live) or after any major changes are made to the infrastructure or code base.

1. Annual Web Application Vulnerability Assessments

IT must ensure that all public facing web applications that store, process and/or transmit Highly Confidential or Confidential data and/or public facing web applications that are logically connected to and/or physical hosted with the previously noted 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 should ensure the applications are assessed against industry accepted guidance (e.g. OWASP Top Ten or SANS Common Web Exposures Top 25).

IT may implement a Web Application Firewall (WAF) in front of web applications in order to continuously perform web application vulnerability assessments. The above testing must also be performed after any changes to application code and/or infrastructure configuration changes.

1. Quarterly Security Standards Review/Update

IT must ensure that all documents containing

public facing web applications that store, process and/or transmit Highly Confidential or Confidential data and/or public facing web applications that are logically connected to and/or physical hosted with the previously noted 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 should ensure the applications are assessed against industry accepted guidance (e.g. OWASP Top Ten or SANS Common Web Exposures Top 25).

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 | 2019-12-09 | First draft | Darace Rose |
| 1.01 | 2020-02-26 | Change Signifi occurrences | Seenan Bunni |
| 1.02 | 2020-03-18 | Adapt to Signifi specifics | Razvan Anghelidi |
| 1.03 | 2020-11-30 | Add quarterly standards review/updates | Razvan Anghelidi |
| 1.04 | 2021-12-02 | Annual review | Razvan Anghelidi |