

IT103   
Information Security Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.13 |
| 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](#_Toc26134101)

[Introduction 4](#_Toc26134102)

[Purpose 4](#_Toc26134103)

[Audience 5](#_Toc26134104)

[Scope 5](#_Toc26134105)

[Policy Statement 6](#_Toc26134106)

[Document Control 7](#_Toc26134107)

[Exceptions 8](#_Toc26134108)

[Enforcement 10](#_Toc26134109)

[Revision History 10](#_Toc26134110)

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

Computer information systems and networks are an integral part of business at Signifi and its affiliates. These systems and infrastructure provide access to financial, administrative, and confidential information. Security is critical to the physical and logical network, systems, applications, and databases with each area offering its own set of security issues and risks. The protection of information systems is essential to manage business risk at Signifi. The nature of our business requires that we ensure the confidentiality, integrity, and availability of Signifi information systems to provide high quality products and services to our members.

Information is defined as “Data associated with meaning and purpose” and information protection incorporates the following criteria:

**Confidentiality:** confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.

**Integrity:** Integrity means that data cannot be modified undetectably.

**Availability:** Availability means that information must be available when it is needed.

Purpose

The purpose of the Signifi’s Information Security Policy is to provide all users which include but not limited to employees, associates, part-time and temporary workers, trainees, contractors and vendors with access to Signifi systems the guiding principles to ensure confidentiality, integrity and availability of information and to understand individual responsibilities. The policy has been established to protect all computers, mobile devices, networks and information assets owned, leased or otherwise held, controlled and/or used by users in performing their duties. This includes but is not limited to all corporate information systems facilities, telephone network components and their supporting systems, communications networks, and the information stored on, transmitted by and/or processed in these facilities.

Audience

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

Scope

To Whom this Policy and all Supporting Policies and Standards Applies

This policy and all supporting policy framework documents apply to all users which includes 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 and all supporting policy framework documents apply to all Signifi resources owned, leased, or supported by Signifi and/or any outside entity that has signed a Vendor Access Agreement with Signifi.

The supporting Policy framework documents include, but are not limited to the following:

* Data Classification Policy
* Hiring Policy
* Misconduct Policy
* Password Policy
* Record Checks Policy
* Security obligations for all Vendors
* Acceptable Use Policy
* Access Control Policy
* Asset Care Policy
* Business Continuity Policy
* Data Backup and Retention Policy
* Encryption Policy
* Hardware Decommissioning Policy
* Incident Management Policy
* Logging Monitoring and Audit Policy
* Physical Security Policy
* Privacy Policy and Operating Practices Manual
* Risk Management Policy
* Security Awareness Policy
* System Development and Infrastructure Policy
* Vendor Access Policy
* Virus and Malware Protection Policy
* Wireless Access Policy
* Change Management Policy

Individuals whose system is connected to the Signifi network are subject to this policy and all supporting policy framework documents and required to abide by them.

Policy Statement

Through this Information Security policy, Signifi Inc shall ensure that:

* Confidentiality, Integrity and Availability of all information assets and data shall be maintained and available on a need-to-know basis.
* Information will be protected against any and all unauthorized access.
* The Local Area Network and Wide Area Network of Signifi will be secured, by implementing controls to safeguard the network from all possible attack vectors either intentional or unintentional.
* Disaster Recovery plans must be maintained, reviewed, and tested as far as practical.
* Information Security Awareness training will be imparted to all relevant Associates to have continual improvements in the ways of data security.
* Legislative, regulatory, and contractual requirements will be met; and
* All actual or suspected information security breaches will be reported to the appropriate entities and will be thoroughly investigated.
* The Chief Executive Officer and Chief Information Officer have approved and support the overarching Information Security policy and all supporting policy framework documents. To that end, the following operational support is stipulated:
* Standards and Procedures will support the policies, including virus control measures, password requirements, DR plans, etc.
* The Information Security Team is responsible for maintaining the policies, providing support and advice during their implementation.
* All associates are responsible for adhering to these policies and ensuring compliance in their respective areas.
* Compliance with the overarching Information Security Policy and all supporting policy framework documents is mandatory which will be monitored and audited periodically.

Document Control

This overarching Information Security Policy and all supporting policy framework documents 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.

The revisiting of this policy will also take into account the results of management reviews. The following information will be presented for the review and update:

* Changes that could affect the organization’s approach to managing security.
* Process performance and information security policy compliance.
* Feedback from interested parties and relevant authorities.
* Trends related to threats, vulnerabilities, and incidents.
* Status of preventive and corrective actions; and
* Results of previous management reviews.

In response to the presented information, the review will action issues related to:

* Improvement of the organization’s approach to managing information security and its processes; and Improvement of control objectives and allocation of resources and/or responsibilities.

Exceptions

It is recognized that there are specific, unanticipated situations in which compliance to information security policies and standards might not be possible due to operational and/or other adaptive business reasons.

In such cases, it is necessary for the business unit to complete a formal, written exception process as described below before proceeding with any action. In all such cases, the business unit and executive approver assumes responsibility for the risk on behalf of the business unit for all risks related to the exception.

Exceptions to this policy must be made in writing by the designated head of the business unit that will be out of compliance with this policy and received by Information Security and approved by the IT executive.

* The request for an exception must clearly identify the following:
* The specific circumstances under which the exception is being sought
* The rationale/justification for the exception.
* Risk assessment.
* Compensating controls to mitigate the risks.
* The alternatives that have been considered.
* The duration of the exception; and
* Approvals and concurrences.

Exceptions are granted for a maximum period of one year. If an exception is required for a longer period, it must be renewed upon its expiry. When an exception expires, the privileges approved through the exception will be revoked with written notice.

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 (YYYY-MM-DD) | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2013-06-11 | First version | Razvan Anghelidi |
| 1.1 | 2019-12-04 | Updated version | Darace Rose |
| 1.11 | 2019-12-09 | Change template | Razvan Anghelidi |
| 1.12 | 2020-12-02 | Annual review | Razvan Anghelidi |
| 1.13 | 2021-12-13 | Annual review | Hadeel Alzuhairi |