

IT112  
Vendor Security Obligations

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.02 |
| 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 ii](#_Toc33427970)

[Introduction 3](#_Toc33427971)

[Purpose 3](#_Toc33427972)

[Scope 5](#_Toc33427973)

[Statement 5](#_Toc33427974)

[Revision History 9](#_Toc33427975)

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 (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 | February 25th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

A” Vendor” is an external individual organization or service provider that performs any task, operation, job or process that could be performed by associates within Signifi, but is instead contracted to a non-employee. In addition, the functions that are performed by the Vendor require access to Signifi information systems and can be performed on-site or off-site.

A “Subservice Organization” is a vendor whose controls, in combination with Signifi’s controls, are necessary to achieve Signifi’s service commitments and system requirements and to fulfill certain SOC 2 trust services criteria. Subsequently, in this document, “Vendor” includes “Subservice Organization”.

Vendor access to Signifi can play an important role in support operations, and of hardware and software management. Setting limits on what can be accessed, modified, and copied by a vendor will reduce the risk of liability, loss of trust, and ultimately damage to our corporate reputation and business.

Applicable data protection laws may impose restrictions and/or requirements on vendor access in cases where the Vendor may access personal data stored at Signifi “Personal data” means any information about an identifiable individual, which includes, without limitation, information relating to identity, nationality, credit card, age, gender, address, telephone number, e-mail address, date of birth, picture, marital status, education as well as certain personal opinions or views.

Signifi requires that its Vendors adhere to strict security guidelines to protect Signifi’s data.

Purpose

This document is intended to provide a summary of the security requirements and best practices to all Signifi Vendors before connecting to the Signifi systems and network.

Scope

This applies to the Vendor’s Security Officer (i.e. person in charge of Computer Security) and all staff participating in the contractual agreement with Signifi.

The Vendor must ensure that ALL Vendor employees participating in the contractual agreement with Signifi complete their internal Privacy and Security training; this will allow them to understand their requirements and help their organization become compliant.

Statement

Behavioral Requirements

The Vendor should ensure that:

* All vendor employees participating in the contractual agreement with Signifi must always use assigned credentials.
* All vendor employees participating in the contractual agreement must never allow another person to use their credentials.
* All vendor employees participating in the contractual agreement are accountable for any actions performed with their ID.
* All vendor employees participating in the contractual agreement with Signifi must never disable, override or willfully bypass any information security control.
* All vendor employees participating in the contractual agreement with Signifi must never attempt to exploit any suspected security weakness on Signifi network, systems and assets, even to explore that such a weakness may exist, unless it is part of their assigned job duties or responsibilities and they are explicitly authorized to do so.
* All vendor employees participating in the contractual agreement with Signifi must lock their computing devices when leaving their device unattended while logged on to Signifi’s network.
* All vendor employees participating in the contractual agreement with Signifi must use approved tools and processes to access Signifi’s network and assets.
* All vendor employees participating in the contractual agreement with Signifi must never take a picture of data displayed on Signifi’s systems/assets.
* All vendor employees participating in the contractual agreement with Signifi must encrypt emails that contain confidential information, use a secure file transfer solution or use a secure e-mail system approved by their organization before communicating sensitive/confidential information.
* All vendor employees participating in the contractual agreement with Signifi must never use external email accounts (e.g., Hotmail, or Gmail) to send confidential information to or receive confidential from Signifi.
* All vendor employees participating in the contractual agreement with Signifi must always create passwords used that are at least twelve (12) characters, with a maximum not less than 64 characters long, and include all four of the following conditions of complexity:
  + One number
  + One uppercase letter
  + One lowercase letter
  + One special character

**Technical Requirements**

The Vendor should ensure that:

* Only Organizational approved tools are used to connect to Signifi’s Network.
* All devices accessing Signifi’s network remotely have encryption applied to the Hard Disk.
* Passwords applied to approved tools used to access Signifi’s network must be at least ten characters long and include at least three of the following:
  + One number
  + One uppercase letter
  + One lowercase letter
  + One special character
* Ensure that browsers and operating systems are kept up-to date.
* When communicating confidential information to Signifi, ensure that the information is encrypted by using features in products such as Microsoft Office, etc.
* Implement an antivirus product and ensure it is kept up to date.
* If you offer guest Wi-Fi, ensure the guest network is segmented from your Office network.
* Vendor must restrict access to security logs to authorized individual only and protect logs from unauthorized access.
* Ensure network and system hardening is performed at least once every sis (6) months.
* Monitor firewall at the perimeter and internally, as necessary.
* Subservice organizations should provide Signifi yearly with a SOC 2 report.

**Administrative Requirements**

The Vendor should ensure that:

* Vendor should establish, implement and maintain reasonable policies and a program of organization, operational, administrative, physical and technical and organizational security.
* Vendor must take reasonable steps to prevent unauthorized physical or electronic access to or loss of Signifi’s confidential and services, systems, devices or media containing this information.
* Vendor must employ risk assessment processes and procedures to regularly assess systems used to provide services or products to Signifi.
* Vendor must limit and monitor physical access to its facilities.
* Vendor must have a clean desk policy for employees to follow.
* Maintain documentation for approving, testing and documenting all network connections and changes to firewall and router configurations.
* Have a documented process and controls in place to detect and handle unauthorized attempts to access Signifi’s information.
* Have a documented incident management process and related process and staff such process and procedures with specialized resources.

Vendor Name:

Vendor Employee Name:

Vendor Employee Signature:

Date:

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 | January 7th, 2020 | First Version | Razvan Anghelidi |
| 1.01 | 2020-12-02 | Annual review | Razvan Anghelidi |
| 1.02 | 2021-12-12 | Annual review | Hadeel Alzuhairi |