

IT111  
Vendor Access 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 ii](#_Toc33423949)

[Introduction 3](#_Toc33423950)

[Purpose 3](#_Toc33423951)

[Scope 4](#_Toc33423952)

[Policy Statement 4](#_Toc33423953)

[Enforcement 7](#_Toc33423954)

[Revision History 7](#_Toc33423955)

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 07th, 2020 |
| Shamira Jaffer | CEO | February 24th, 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.

Purpose

The purpose of this policy is to establish the rules for access to the Signifi information, information systems or data centers by vendors which include consultants, contractors and other service providers. This policy is designed to minimize the potential exposure to Signifi facilities and information from risks associated with vendor access.

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. Vendor Agreements

The following general terms must be included in all agreements with vendors that are granted access:

* Signifi CEO, or a designated delegate, approval needed before Club member information and other repositories are stored or processed with a third party (i.e. vendors, business partners, hosted services, “cloud‟ services, non-Club data centers).
* Agreement to permit Signifi to perform reasonable inquiry and if desired on-site audits of the Vendor to ensure compliance with above noted requirements.
* Vendor is responsible for immediately informing Signifi of any known or suspected violations of the Signifi security policies.
* Acknowledgement that the Service Providers will not share or disclose Signifi information to any other parties without prior written consent; Vendors are required to sign non-disclosure agreements and Vendor access agreements with wording to ensure they are legally bound to comply with Signifi security policies.
* All software developed by vendors on behalf of Signifi is the property of Signifi and cannot be otherwise distributed without written consent by the Executive Management team.
* The vendor must have business continuity provisions in place in the event of a major disruption, disaster, or failure to minimize Signifi impact during a disaster or disruption.
* Where engagement with a vendor involves access to credit card information of Signifi customers, the Vendor must acknowledge that they will achieve and maintain PCI Compliance.
* Agreement to provide Signifi with evidence of PCI Compliant status upon request.
* Acknowledgement that vendors are responsible for the security of cardholder data they may possess.
* Agreement to immediately notify Signifi of any control failures that threaten the Service Provider’s PCI Compliant status, and/or may have resulted in the unauthorized disclosure of Cardholder and/or Highly Confidential data; and
* Agreement to immediately notify Signifi of any suspected breaches or incidents that may have threatened the security of the Vendor’s information systems and assets.

Any vendor agreements and contracts must specify:

* The work that is to be accomplished and the time frame.
* The Signifi information that the vendor will have access to.
* The minimum-security requirements that the vendor must meet (i.e. method for remote access);
* How Signifi information is to be guarded by the vendor. Signing of a non-disclosure agreement is required where Highly Confidential, Confidential or Internal information is shared with the Vendor as referenced within the Information Data Classification Policy.
* Strict use of Signifi information and information resources for the purpose of the business agreement by the Vendor. Any other Signifi information acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes or divulged to others.
* Feasible methods for the destruction, disposal, or return of Signifi information at the end of the contract as applicable; and
* The return of company property such as a laptop, PDA, access cards or cell phone after the completion or termination of the agreement.

1. Computer Room

The following must be adhered to when vendors require access to Computer Rooms:

* When Vendors are scheduled to have access to the computer room, the IT staff must be notified in advance of the date, time, and type of work to be performed. The authorized Signifi resource will be kept informed of the status of the work, as well as the notification that the work is completed.
* All Vendor access to the computer / server room must be logged in a visitor logbook; and
* All Vendor access to the computer and telecom rooms must be accompanied by a point person from IT.

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 | 2020-01-07 | First Version | Darace Rose |
| 1.1 | 2020-02-20 | Added clauses | Razvan Anghelidi |
| 1.11 | 2020-12-04 | Annual review | Razvan Anghelidi |
| 1.12 | 2021-12-12 | Annual review | Hadeel Alzuhairi |