

IT104   
Access Control Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.11 |
| 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](#_Toc23870960)

[Introduction 4](#_Toc23870961)

[Purpose 4](#_Toc23870962)

[Audience 5](#_Toc23870963)

[Scope 5](#_Toc23870964)

[Policy Statement 5](#_Toc23870965)

[Enforcement 10](#_Toc23870966)

[Revision History 10](#_Toc23870967)

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 13th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Access to Signifi information and systems is granted in a manner that balances restrictions to prevent unauthorized access versus the need to meet business requirements.

Purpose

The purpose of this policy is to provide access control requirements for the access to Signifi information systems or information by employees, associates and contractors to protect the:

* Confidentiality.
* Integrity; and
* Availability of information

These controls must:

* Define the information security responsibilities of all persons who have access to Signifi systems.
* Ensure that only authorized persons are granted access to Signifi systems and that personal accountability is assured.
* Ensure that only authorized information systems are granted access to Signifi environment.
* Provide authorized persons or information systems with only the least amount of privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

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 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 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. Access Control
   1. All employees using Signifi Information Technology resources must be authorized. Access is governed by this policy and supporting procedures. The elements involved in controlling and monitoring access include identification, authorization and authentication.
   2. Identification - All associates are assigned a unique ID to use in accessing the Signifi systems and applications. User IDs are not to be shared. Associates are responsible for maintaining the security of their IDs and all activity occurring under those IDs.
   3. Authorization - Only those associates who have valid reasons for accessing the Signifi systems and information are granted the least access privileges appropriate to their business requirements.
   4. Process to verify job application information for all users who will have access to Signifi systems. Verification methods may include:
   * Character or employment references
   * Criminal record checks where possible taking into consideration employment arrangements of the organization and unions.
   * Verification of prior experience, academic record, and professional qualifications, and
   * Verification of identity from government issued identification.
   1. Authentication - Authentication ensures an identity. Each ID requires a technique, usually a password, for validating identity. Under certain conditions, vendors who support hardware or software may be granted system access. Such connections should also comply with appropriate identification, authorization, and authentication. Vendors should only be provided access for the duration required for the support request. All vendors must complete and sign the Remote Vendor Access Agreement.
   2. Limit access to system components containing Highly Confidential information, such as personal information data, to only those individuals whose job requires such access. Access limitations must include the following:
   * Adhere to the concept of least privilege necessary
   * Assignment of privileges is based on individual personnel’s role and function
   * Documented approval from authorized parties specifying the required privileges
   * Consent must be attained from the user or Human Resourced department prior to any IT personnel accessing a user’s computer
   1. Implementation of an automated access control system:
      1. The purpose and level of access to be granted to a user shall be determined by the respective Data Owner and the access will be granted / implemented by IT. In some cases where the Data Owner is IT, both functions shall be performed by IT.
      2. The level of access granted to an employee for access to information systems must support but not exceed what is necessary to perform his/her functional responsibilities and duties. Assignment of access rights must be based on an individual’s job function and responsibilities.
      3. Employees shall be advised that access to any system and/or any transaction performed using their Signifi provided account may be logged, monitored or audited and that the associate shall be uniquely accountable for all transactions executed using their account by the associate.
      4. The actions performed by IT Administrators who have access to Highly Confidential or Confidential information must be sent to a centralized logging solution that is not alterable by the IT Administrator who performed the activity. This is intended to maintain the integrity of the logs and to preserve the actions taken for troubleshooting, audit and compliance purposes.
      5. When some associate leaves Signifi, all system privileges and access to data must be immediately disabled or removed.
      6. Signifi Information Systems shall display an approved system banner message before access is granted.
      7. Business areas must periodically review access rights and privileges of their respective systems and notify Identity Management of any changes. In the event of unauthorized access to a system, the user admin shall immediately disable any accounts or permissions as it deems necessary and take other measures as may be appropriate to protect the information and systems.
   2. Maintain a list of all individuals that have access to Signifi systems. The list must include the following:
   * The ID, and
   * Person or information system’s details: Full name, department, and location, and contact information (email and telephone number (where available).
2. Separate development, test, and production environments
   1. Without adequate separations between environments, it may be possible for the production environment to be compromised due to vulnerabilities in a test or development environment if logical and/or physical separation has not been instituted. Signifi must maintain separate development, test and production environments.
   2. Production data such as live Primary Account Number (PANs) must not be used for testing or development purposes.
   3. Always remove test data and change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
3. Separation of duties between development, test, and production environments
   1. Development and test functions will be kept separate from production functions. For example, a developer may use an administrator-level account for use in the development environment and have either no access or a separate account with user-level access to the production environment.
4. Remote Access
   1. Approved Signifi employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs. When using these services, the user is responsible for establishing a connection to the Internet before establishing the VPN session.
   2. It is the responsibility of all Signifi employees with VPN privileges to not share their VPN credentials (username/password or Secure Token) with anyone.
   3. All individuals and machines, while using Signifi’s VPN technology, are a de facto extension of the Signifi network, and as such are subject to all Signifi policies and expectations.
   4. All vendor access must comply with requirements of Vendor Access Policy and sign off on the Vendor Access Agreement.
   5. Accounts used by vendors for remote access, maintenance or support must be enabled only during the time period needed.
   6. IT shall log and monitor remote vendor access regularly.
   7. For Signifi employees, only corporate computers provisioned by the IT department are permitted to establish a VPN connection and must have a properly configured, up-to-date operating system, enabled with anti-virus software and a software firewall.
   8. Remote Access VPN connection shall be established using “Two Factor Authentication” such as tokens or certificates and strong encryption.
   9. Dual homing or split tunnelling is NOT permitted; only one network connection is allowed.
   10. VPN users will be automatically disconnected from Signifi’s network after eight (8) hours of inactivity. The user must then login again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
   11. When an employee leaves Signifi, all existing remote access services will be terminated or disabled immediately.
   12. Remote access is considered a privilege and may be revoked at any time without reason.
   13. Support will be accomplished by the associate bringing or shipping the assigned Signifi computing asset to a serviceable Signifi facility.

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 | 2019-12-13 | Update template | Razvan Anghelidi |
| 1.11 | 2020-12-01 | Annual review | Razvan Anghelidi |
| 1.12 | 2021-12-12 | Annual review | Hadeel Alzuhairi |