

IT100   
IT Acceptable Use 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 ii](#_Toc23869891)

[Introduction 3](#_Toc23869892)

[Purpose 3](#_Toc23869893)

[Audience 3](#_Toc23869894)

[Scope 4](#_Toc23869895)

[Policy Statement 4](#_Toc23869896)

[Enforcement 9](#_Toc23869897)

[Revision History 9](#_Toc23869898)

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 22nd, 2022 | |
| Shamira Jaffer | CEO | | December 23rd, 2021 | |
| Shamira Jaffer | CEO | | December 7th, 2020 | |
| Shamira Jaffer | CEO | | December 13th, 2019 | |
|  | |  | |
|  |  | |  | |

## Document Sensitivity Level

Confidential

Introduction

Overview

All users that have access to organizational computer systems must adhere to the IT Acceptable Use Policy in order to protect the security of the network, protect data integrity, computer systems and all organizational assets.

We depend heavily on our computer systems to provide complete and accurate business information when and where it is needed. The impacts of unauthorized access or modification of important business data far outweighs the cost of the equipment itself.

Laptop computers are an essential business tool but their very portability makes them particularly vulnerable to physical damage or theft. Computer systems and organizational assets taken off premises are subject to special information security risks; their likelihood of loss or theft increases leading to higher exposure of unauthorized access or tampering.

Purpose

The purpose of this policy is to ensure that Signifi Information Technology (IT) assets such as desktop and laptop computers, servers, monitors, software and all other technology assets will be distributed and tracked to verify that Signifi has control over and knowledge of all technology assets in use.

This policy is also designed to establish rules and controls necessary to minimize information security risks affecting Signifi computing devices, as well as outline the proper use of computing devices, to prevent loss or theft of the devices and to protect Signifi data that may reside on such devices from unauthorized access or modification.

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. Assets
   1. IT must maintain an inventory of all Signifi computing assets.
   2. Signifi will provide software on the specific role of the associate. For a list of authorized software please consult IT Service Desk at [it@signifi.com](mailto:it@signifi.com)
   3. Each IT asset purchase and/or use, hardware or software, needs to be first approved first by IT. IT will check:

* If any PII (Personally Identifiable Information) will be stored in that asset
* If Signifi or Signifi clients data will be stored in that asset
* If the vendor or supplier is certified to the level required by Signifi’s agreements with its clients

Failure to engage the IT department before purchasing or using any IT asset, hardware or software, will make the user and their manager responsible for any consequences of this non-compliance, including lawsuits from clients or former clients and possible financial losses.

* 1. All users issued a workstation or other company assets are responsible for its physical safekeeping. Users must ensure that mobile assets (e.g. laptops, blackberries) are taken home on a daily basis or in a locked cabinet
  2. All assets distributed to staff will be assigned a unique identifier and will be recorded and tracked.
  3. Employees will be required to acknowledge the assets they have been given and that acknowledgement will be stored for future reference
  4. IT will maintain the computer assets throughout the Assets Lifecycle. An asset must be returned to IT without exception if the asset is deemed obsolete or device failure occurs
  5. Personal devices must not be used for corporate use.
  6. Hardware IT assets must be returned to Signifi in a usable state, with normal wear and tear. Any physical damage (cracked screen, keys missing or not functioning, signs of liquid spills, cracks, scratches, damaged hinges and so on), as well as not returning the device at all, will determine that the replacement device will be paid by the employee.

1. Physical Security
   1. Only assets issued by Signifi IT shall connect to Signifi LAN
   2. Devices shall be kept in the associate’s physical presence whenever possible
   3. Whenever a device is being stored, it shall be stored in a secure place, preferably out of sight
   4. Employees must not leave their workstation unattended without first logging-out or turning on a password-protected screen lock for any length of time
   5. System administrators must not leave servers or workstations unattended for any period of time without first logging-out, locking the server or workstation, or turning on a password-protected screen lock
   6. All employees must power off their PCs before leaving for the day, unless otherwise instructed
   7. All workstations must have a cable lock or be stored in a locked cabinet when not in use or when left unattended, where appropriate
   8. Special care must be taken when using computing devices in public places, meeting rooms, and other unprotected areas inside and outside of the Signifi premises to avoid the risk of exposure to unauthorized persons
   9. Laptops must not be left visible in your car or left overnight in a vehicle even if stored in the trunk
   10. Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage
   11. Users must report to IT if a computing device is lost or stolen and indicate if the missing device contains or is suspected to contain Highly Confidential or Confidential data
   12. The user may be required to provide a copy of any filed police report associated with a Signifi stolen device(s)
   13. When an associate leaves the company, all IT assets must be gathered by the associate’s manager and returned to IT. This includes associate departures due to resignations, terminations, and long-term disability.
2. Access Security
   1. Whenever possible, all computing devices must be password protected.
   2. Employees must not grant access to their computing devices to non-Signifi employees;
   3. All computing devices should enable screen locking and screen timeout functions;
   4. Highly Confidential or Confidential data stored on Signifi computing devices should be kept for the minimum time required for its effective business use to minimize the risks and impacts should a breach occur;
   5. As applicable, Highly Confidential or Confidential data, if stored on a computing device must be encrypted;
   6. All computing devices must be configured to validate access credentials, at a minimum username and password, before allowing access to system resources; and
   7. The guest account(s) must be disabled on all computers.
3. Application Configuration  
   1. The IT Service Desk shall maintain a software inventory list for different lines of business;
   2. All software installed on computing devices must be licensed and approved;
   3. Applications must be carefully tested for compatibility and security settings before deploying them on computing devices; and
   4. IT must keep all computing devices current with critical security patches as per the patch management schedule.
4. Installation, Patching and Logical Security  
   1. IT will inform all employees with access to the Personal Information data environment that copying, moving and storage of Personal Information data onto local storage and/or removable media is prohibited.
   2. IT must ensure that network configurations for computing devices and more specifically, devices that may access Personal Information data are deployed in the following manner:
   3. Direct public access between the Internet and the device is prohibited (e.g. do not allow the pass through of traffic from the Internet directly to services running on an end-point device); and
   4. Do not allow any direct connections inbound or outbound for traffic between the Internet and the device (i.e. require the use of a proxy server implemented at the network perimeter)
   5. Operating System installation must be performed by Signifi approved personnel
   6. All unneeded network services and protocols must be disabled;
   7. System configuration attributes must be defined, reviewed, and approved prior to being applied to desktops
   8. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers
   9. IT must configure system security parameters to prevent misuse
   10. Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH v2, TLS 1.2 and above, or IPsec v2 to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.
   11. Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release unless a compensating control is in place to mitigate the risk.
   12. Further to the above point Signifi IT may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (public facing devices and systems, databases) higher than less critical internal devices, to ensure high priority systems and devices are addresses within one month, and addressing less critical devices within three months
   13. Where applicable, patches must be tested prior to rolling them out on production servers and workstations and must follow the Signifi Change Management Policy.
5. Disposal of Computing Devices   
   1. Highly Confidential or Confidential information held on any computing device should be securely deleted before the device is exchanged, disposed, or reassigned to another associate or for another purpose.
6. Termination of Employee  
   1. When an employee leaves the company, all IT assets must be gathered by the employee’s manager and returned to IT. This includes mobile devices from employee departures due to resignations, terminations, and long-term disability.

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 | 2019-12-07 | First version | Darace Rose |
| 1.01 | 2019-12-10 | Update names | Razvan Anghelidi |
| 1.02 | 2020-11-30 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |
| 1.04 | 2022-12-15 | Annual review | Razvan Anghelidi |