

IT119  
Physical Security Policy

|  |  |
| --- | --- |
| 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 iii](#_Toc35540065)

[Introduction 4](#_Toc35540066)

[Purpose 4](#_Toc35540067)

[Audience 4](#_Toc35540068)

[Scope 5](#_Toc35540069)

[Policy Statement 5](#_Toc35540070)

[Enforcement 20](#_Toc35540071)

[Revision History 20](#_Toc35540072)

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 | | Feb 28th, 2019 |
|  |  |
|  |  | |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Physical security measures are steps taken by Signifi for securing, controlling and monitoring physical access to the company premises, information systems and assets including those considered part of the personal information data environment as defined under the PIPEDA Act.

Purpose

The purpose of the Signifi Physical Security policy is to establish physical security measures and rules for granting/removing, controlling, monitoring physical access to Signifi facilities. It is also intended to provide direction as to how to mitigate risks of inappropriate physical access to systems, buildings, assets or corporate offices.

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. Physical Security Requirements

**Offices and Server Rooms**

* 1. Physical security of office premises is the responsibility of the Corporate Facilities department who shall manage day to day administrative activities. Administrative activities include such things as managing access cards, reviewing daily logs, reviewing feeds from video cameras and investigating breaches.
  2. Physically accessible network ports such as in the lobby when not in use must be disabled or protected by alternate means all the time.
  3. Physical security of server rooms (any area that contains servers with Highly Confidential or Confidential information) is the responsibility of the Corporate Facilities department whose department shall manage day to day administrative activities.
  4. Card and/or key access rights must be removed from individuals that change roles within Signifi or are separated from their relationship with Signifi. Lost or stolen access cards and/or keys must be reported to Corporate Facilities as soon as possible. Corporate Facilities must disable lost or stolen access cards immediately.
  5. Access cards and/or keys must not be shared or loaned to others. Access cards and/or keys that are no longer required must be returned to Corporate Facilities. Cards must not be reallocated to another individual, bypassing the return process.
  6. Physical security of the datacenter is the responsibility of the Data Centre Operations department who shall manage day to day administrative activities.

**Access Control System**

* 1. Electronic card access controls for all facilities will be the responsibility of the Corporate Facilities department. This includes day-to-day administration and 24 hour a day monitoring.

**Office Security**

* 1. Unauthorized physical access to Signifi premises is prohibited. Physical access to all Signifi premises will be limited to authorized personnel.
  2. Procedures will be developed and used to ensure all personnel can easily distinguish between employees and visitors. Employees will be encouraged to challenge any person not known to them as a Signifi employee and not showing a visible identification badge.
  3. All visitors will be escorted by a Signifi employee at all times while on Signifi premises.
  4. Staff will not permit tailgating when entering or leaving the premises. No unidentified person will be allowed entry to Signifi premises.
  5. A card access control facility will be used to limit and monitor physical access to office premises and must be used at all times. The system will be managed by the Corporate Facilities department.
  6. Card access control logs will be retained for a period of at least three months. Logs will be reviewed on a regular basis by the Corporate Facilities department staff for any anomalies and all follow-up will be documented and retained for a period of three months or longer.
  7. Cameras will be used to monitor any entry point not staffed by a receptionist or other person. (For example, each floor of an office tower used by Signifi.) Cameras will be monitored continuously by the Corporate Facilities department and will record all activity. Recordings covering any sensitive area will be maintained for at least a three-month time period. All other recordings are to be maintained for at least one month.
  8. Alarm systems will be continuously monitored by the Corporate Facilities department. If no alarm is available, cameras will be placed to enable Facilities staff to monitor the facilities.
  9. Employees will operate under clean-desk principle. No Highly Confidential or Confidential information will be left on desktops unattended. Desktops will be cleared of papers prior to leaving for the day and all materials will be placed in locked cabinets or files.
  10. Laptops will be physically locked to the desk or placed in a locked cabinet while unattended, reducing the risk of theft.
  11. Computers accessing Highly Confidential or Confidential information must not have monitors set to allow viewing from outside. They must face away from any windows or blinds must always be drawn closed.
  12. Wireless access points, gateways, and routers and other sensitive network machines will be kept in locked locations with access restricted to technical support staff.
  13. Appropriate fire extinguishers will be placed according to local fire code throughout the premises. Fire extinguishers will be maintained on a regular basis according to local fire codes.
  14. Staff will be instructed in safety and evacuation procedures on an annual basis.
  15. Fire drills will be held on a random basis and all staff will participate.
  16. A fire warden will be assigned for each floor of a building and instructed in safety and evacuation procedures.
  17. All external walls will extend from concrete ceiling to concrete floor with no gaps and must consist of standard building materials. In shared premises, those walls connecting other enterprises will be monitored continuously by the Corporate Facilities department using cameras or motion detectors.
  18. Delivery and loading areas are to be controlled and isolated from office facilities by card access-controlled doors.
  19. Access to a holding or loading area from outside of the building will be restricted to identified and authorized personnel.
  20. The holding or loading area will be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building.

**Server Room Security**

* 1. A card-based entry control system will be used to limit and monitor physical access to the server room, separate from any other door access.
  2. Access to server rooms will be managed by the Corporate Facilities department.
  3. All visitors will be required to sign a visitor log prior to being permitted entry to any server room. The log will include entry and exit date, time of day and visitor’s signature. The logs will be retained for at least three months.
  4. Visitors requiring access to server rooms will always be escorted. At no time will a visitor be left unattended.
  5. No smoking, eating or drinking will be permitted within the server room.
  6. Staff will be trained on how to deal with unauthorized personnel who request or attempt access to the server room.
  7. All equipment will be located on racks or tables. No equipment will reside on the floor.
  8. Cables are not to lay across the floor and will be neatly wrapped or bundled and labeled for easy reference.
  9. All server room equipment will be connected to a UPS or generator providing at least 30 minutes of power and automatic shutdown capability in case of power shortages.
  10. Media back-ups will be stored in a secure facility, which may be a fire-proof cabinet or safe, while residing in the server room.
  11. No paper and electronic media (e.g., electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain personal information will be left in the open while unattended.
  12. Strict control over all media distribution containing personal information will be maintained at all times.
  13. Sending physical media outside the company is discouraged. If it must be sent out, it will be via a secured courier or a delivery mechanism that can be accurately tracked.
  14. Management approves all media that is moved from a secured area.
  15. All physical media that leaves the premises must be encrypted to render it secure from loss or theft.
  16. Personal information should not be stored on physical media, but if it ever needs to be, maintain strict control over the storage and accessibility of that media.
  17. Maintain and check inventories of all Highly Confidential and Confidential media.
  18. Conduct regular assessments of confidential media to ensure it is always securely stored.
  19. All materials containing customer data or Signifi Highly Confidential or Confidential information must be disposed by cross-cutting shredding, incinerating, or pulping.
  20. Electronic media must be purged, degaussed, shredded, or otherwise destroyed when it is no longer needed for business or legal reasons so that personal information data cannot be reconstructed.
  21. Locked containers will be made available for storing Signifi confidential or customer information prior to it being destroyed. Procedures for managing such containers will be written and followed. The Corporate Facilities department will be responsible for managing destruction of confidential material.
  22. All server room walls will rise from concrete floor to concrete ceiling. If raised floors or dropped ceilings are in use, special restrictions such as wire mesh are to be used to block those areas.
  23. Server room walls, floors and ceilings will be built to community standards for office fire codes using flame resistant materials.
  24. There will be no windows in the room. If there are windows, they are to be protected from casual breakage by wire mesh glass.
  25. No server room will exist where a boundary wall is shared with other tenants. If unable to comply with this standard, the room is to be equipped with motion detectors set to automatically turn on after regular business hours remotely connected to the Corporate Facilities department for monitoring.
  26. Server rooms will be not be located in areas where there is a risk of water or other liquid leaking from above. For example, there should be no restaurant, washroom, cafeteria or other such area located above a server room.
  27. Any holes in the concrete ceiling of server rooms are to be sealed to prevent the spread of water in the event of a leak on the floor above.
  28. Server rooms located in areas with water-based sprinkler system overhead are to have those sprinklers moved. If this is not possible, they will have plastic sheeting available to cover equipment along with clearly defined procedures for their use in case of overhead flooding.
  29. A temperature and humidity device will be located within each server room and monitored regularly for abnormal conditions. Ideally, these will be connected to a central alarm system for constant surveillance by the Corporate Facilities department personnel.
  30. Clearly labeled Class C fire extinguishers will reside in each server room and will be checked annually or according to local fire codes.
  31. Adequate fire, smoke and water-detection devices will be located in all server rooms including locations under any sub-flooring. The devices will be connected to a monitoring system within the Corporate Facilities department.
  32. Flammable materials will not be stored in server rooms. Paper boxes, large reports, cleaning materials etc. will always be stored separately from the server room.
  33. An intercom or telephone will be available within each server room for emergencies.
  34. All equipment (servers, workstations, printers etc.) will be inventoried and identified with a tag. Inventory verification checks will be performed periodically by the Information Technology team.
  35. It is not permitted to take pictures or video while in the Server Room at 1705 Tech Ave Unit 3, Mississauga, ON, L4W 0A2.

**Datacenter security**

* 1. Access to Datacenters will be managed by Data Centre Operations department.
  2. No smoking, eating or drinking will be permitted within the Datacenter.
  3. The card access system will require the same card for in-bound access. No exit will be permitted without card access with the exception of fire doors. All access will be logged, and logs will be retained for at least 1 year.
  4. Access to the computer room will be strictly limited to those staff requiring access on a regular basis. All temporary or irregular access will be provided access on an as needed basis and such access will be removed immediately following the specified need.
  5. Visitors will be issued temporary Visitor Passes which are to be worn in a visible location at all times.
  6. Visitors requiring access to Datacenters will always be escorted. At no time will a visitor be left unescorted.
  7. Visitors must surrender the Visitor Pass before leaving the facility. Those visitors issued a pass for multiple days will surrender the pass and sign for it each day.
  8. Datacenters will be positioned properly geographically away from fire, electromagnetic, water or other hazards.
  9. Datacenters will not exist in areas where there is a high risk of water or other liquid leaking from above.
  10. No Datacenter will exist where a boundary wall exists on premises shared with other tenants except where that Datacenter is part of an outsourced firm providing Datacenter services and abiding by all these controls. Where such associations exist, motion detectors and video cameras will be used to monitor any areas sharing a boundary wall.
  11. No Datacenter will have a boundary wall residing on a laneway or anywhere that vehicle traffic exists where that wall forms part of the critical computer processing areas of the Datacenter (the computer or media room).
  12. Exterior walls, doors, windows or other openings will be strong enough to resist all but extreme forms of accidental or intentional damage.
  13. All fire doors on a security perimeter will be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards; they will also operate in accordance with local fire code in a failsafe manner.
  14. To prevent or reduce the potential for vehicle impacts, steel posts will be designed and used in front of building corners or other locations where there is vehicle traffic.
  15. Datacenter walls, floors and ceilings will be built using fire resistant materials such as concrete.
  16. All Datacenter walls will rise from concrete floor to concrete ceiling. Raised floors or dropped ceilings should be used only within a room that is concrete floor to concrete ceiling.
  17. Any holes in the concrete ceiling of Datacenters are to be sealed to prevent the spread of water in the event of a leak on the floor above.
  18. There will be no windows in the computer or media rooms. If there are windows, they are to be protected from casual breakage by wire mesh glass.
  19. Doors will be built using metal-cored fire-resistant doors with concealed hinges fixed and locked into strong frames. Door frames will be securely fixed and resistant to breakage, with anti-burst locking pins and strong locks.
  20. Delivery and loading areas are to be controlled and isolated from the remainder of the building by card access-controlled doors.
  21. Office and administration areas are to be controlled and isolated from the primary computing areas of the building by card access-controlled doors.
  22. Municipal power shall be redundantly supplied through multiple grids where possible.
  23. All primary computing equipment will be connected to a generator that will automatically provide ongoing power should main power be lost and will be tested at least annually. Testing should be based upon a well-defined Disaster Recovery plan.
  24. Power conditioning will be used throughout the Datacenter but especially for all power related to primary computing. The potential noise and frequency of serious spikes requires conditioning to protect the equipment.
  25. The Datacenter will have an Emergency Power off (EPO) button clearly visible, with a cover to protect it from accidental use.
  26. A temperature and humidity device will be located within each Datacenter and monitored regularly for abnormal conditions.
  27. Heating, Ventilation and Air Conditioning (HVAC) will be monitored continuously using a central monitoring system connected to the Corporate Facilities department.
  28. Datacenters will use an appropriate Halon alternative such as FM200 for extinguishing fires within all areas with critical computing components. AC units will be set to automatically shut down when FM200 is released.
  29. Clearly labeled Class C fire extinguishers will reside in each area housing computers or other electronic equipment and will be checked annually or according to local fire codes.
  30. Clearly labeled Class A, B and D extinguishers will be placed as required by need and local fire codes throughout the Datacenter premises.
  31. Air conditioning and security systems must also be automatically protected by generator.
  32. Flammable materials will not be stored in primary computing areas. Paper boxes, large reports, cleaning materials etc. will be stored separately from all primary electronic equipment.
  33. No paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain personal information will be left in the open while unattended.
  34. Sending of any physical media to another location will be done via secured courier or a delivery mechanism that can be accurately tracked.

**Video Surveillance**

* 1. Video surveillance standards for Signifi premises are the responsibility of the Corporate Facilities department.
  2. Surveillance equipment, monitoring activities and administration are the responsibility of the Corporate Facilities department.
  3. Video surveillance will not be undertaken in any area where employees or the public reasonably expect privacy such as in restrooms or change rooms.
  4. Employees must be notified they are under video surveillance in a public area. Notices must be in official language(s) for the jurisdiction in which the public area is located. In Canada, notices are required in both English and French. In areas where another language is predominant, notices may also be in that language.
  5. Notices will contain the following wording, or the equivalent in other languages:
  6. “These premises are under video surveillance”
  7. “Nos locaux font l’objet d’une surveillance video”
  8. Notices must be conspicuously placed and easily read from a distance and must be placed at all public entry points where surveillance occurs. Where not prohibited by law, undisclosed video surveillance may occur in public and non-public areas excluding restrooms and change rooms in relation to an active investigation conducted with assistance from the Corporate Facilities department if circumstances warrant. Undisclosed video surveillance must be approved by an executive responsible for the Signifi business unit, in conjunction with the Corporate Facilities department.
  9. Where local laws impose higher standards or restrictions Signifi will adhere to them in addition to the standards within this document.
  10. Equipment used for video surveillance in a public area must not record sound except in circumstances where there is written consent of the persons being recorded, the Signifi Solutions business unit in question is acting under a court order requiring or permitting the use of sound, or in other situations, determined on a case-by-case basis, provided the Corporate Facilities department has been consulted and have approved the recording in writing.
  11. Clearly written procedures will be implemented to ensure no unauthorized access to, or use or disclosure of, recorded material occurs. Signifi must maintain procedures that conform to these standards for implementing a video surveillance system, monitoring the video surveillance system so implemented, use and disclosure of recorded material, access to recorded material, and preservation of the integrity of recorded material.
  12. Signifi procedures for operating a video surveillance system must include frequency of review, allocation of responsibilities for each aspect of the operation, nature of the review (e.g. random review or review of all material recorded), timetable and detailed log of such operation reviews. The Signifi business unit must adhere to the video surveillance procedures established.
  13. Senior management of Signifi will, in conjunction with the Corporate Facilities department, ensure new and existing procedures are reviewed and revised if necessary, to ensure the requirements of these standards are met.
  14. The Corporate Facilities department must review the experience and skills of any person given responsibility for the video surveillance system, including reception equipment and storage devices, and along with senior management of the Signifi business unit, approve the delegation of responsibility for video surveillance systems to any such person.
  15. The quality of recorded material produced by the video surveillance system must be sufficient to produce clear images to assist in the identification of persons and events.
  16. Video surveillance systems must be maintained to Signifi standards as communicated by the following:
  17. Recorded material is intended for use only in the detection and investigation of criminal, civil and administrative offenses and violations of our code of conduct, and to support Signifi in the defense of legal proceedings, disputes or regulatory investigations. Unauthorized use or disclosure of recorded material is a violation of this policy.
  18. Video surveillance recordings will be considered Signifi Confidential information and will be subject to all Signifi standards relating to confidential information.
  19. Only authorized persons will have access to see, view, hear, and have access to, maintain or maintain possession of, video surveillance recordings. Authorization is the responsibility of the Corporate Facilities department.
  20. Logs will be maintained of all requests to access and use recordings. These logs will contain the name of the requestor, time and date, reason for the request and name of person authorizing the access.
  21. Surveillance records will be kept for all recorded material using the following minimum information:
* A description of the operation of the video surveillance equipment and its coverage
* A description of the maintenance and retention of video surveillance material
* Any failure of the equipment during the time period covered by the recording and whether that failure at any time affected the integrity of the recorded material
* The testing process and testing history of the recording system, including any modifications made to the system
  1. Recordings will not be removed from secure Signifi premises without written authorization from the Corporate Facilities department.
  2. Except where authorized by a court order of required by law, prior to removal by or release to any person not a Signifi employee, a signed and dated Release and Indemnity form will be completed and retained by the Corporate Facilities department.
  3. When removed, a log will be maintained indicating the reason for removal, date and time period of the information being removed, name of person removing the material, remover’s signature and date and time of removal.
  4. Recordings will be kept for a minimum of 90 days and no more than 365 days unless required for evidentiary purposes.
  5. Recordings used for evidentiary purposes must be retained as per any legal retention requirement, court or tribunal order, or while the persons, activities or transactions remain under investigation or legal dispute.
  6. Where a request is made to review recorded material and the video surveillance material contains relevant information, but it is not established it is needed for evidentiary purposes it must be retained for 7 years after which it can be securely destroyed.
  7. Recordings will be protected from unauthorized access or alteration while persons, activities or transactions recorded with the systems are the subject of ongoing dispute, legal proceedings, regulatory investigations or legal retention orders to protect against any criminal offense under Canadian law.

1. Offices and Server Rooms

**Visitor Sign In**

* 1. Personnel authorized to permit visitors and/or short-term contractors (collectively referred to as “Visitors”), must validate the identity of the visitors they are permitting to access Signifi premises. Visitors permitted access must sign the designated visitor log located at designated visitor control areas.
  2. Visitor Identification Badge – Upon receiving approval to access the Designated Area, visitors must be provided with a security badge, that:
* indicates their status as a visitor; and
* is clearly marked.
  1. Visitors should be instructed to clearly display the visitor badge, and ensure it is worn at all times while on Signifi premises.

**Visitor Log**

* 1. Visitor logs maintained at each Designated Area must include the following information at a minimum:
* Date and time of sign-in;
* Visitor’s first and last name;
* Name of Company being represented;
* Signature of Visitor;
* Temporary Badge Number (if applicable);
* Name and department of Personnel authorizing visit

**Visitor Log Maintenance**

* 1. Visitor logs detailing visitor access to Signifi premises must be maintained by designated custodians for a minimum of 3 months.
  2. Visitors are not permitted to take photographs inside of Signifi premises unless discussed specifically with sponsoring Employees. If Employees have any questions about the suitability of photographs, they should consult the Human Resources department.

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 | 2019-12-09 | First draft | Darace Rose |
| 1.01 | 2020-02-26 | Adaptations to specific Signifi conditions | Seenan Bunni |
| 1.02 | 2020-11-30 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |