b

IT204   
Signifi Solutions System Description

|  |  |
| --- | --- |
| 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.*

[Audience 5](#_Toc62632508)

[Scope 5](#_Toc62632509)

[Update 20](#_Toc62632510)

[Revision History 20](#_Toc62632511)

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 | August 3rd, 2021 |
| Shamira Jaffer | CEO | January 22nd, 2021 |
|  |  |  |

## Document Sensitivity Level

Confidential

Audience

This document is targeted towards all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, representatives, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as staff in this policy).

It also targets Signifi's clients/customers.

Scope

This document describes the services provided, along with the supporting processes, policies, procedures, personnel, and operational activities that constitute Signifi's core activities.

**OVERVIEW OF THE SYSTEM**

Company Overview and Background

Signifi Solutions was founded in 2005 with the mission to provide life-changing, timesaving, robotics-based dispensing solutions that enable industry-leading business to business and business to consumer brands to support on the go populations receiving merchandise they want when they need it most.

Description of Solutions Provided

Signifi Solutions currently offers a portfolio of two primary solutions: one for Automated Retail and one for Asset Management.

For Automated Retail, we provide a continuum for hardware smart kiosks and lockers for vending merchandise and click and collect products where consumers buy online and pick up in-store and loss prevention.

For Asset Management, we offer modular smart locker hardware to enable employees to pick up and drop off assets, such as laptops and cell phones.

Depending on a customer's unique requirements, we also offer various authentication and scanning options, such as readers (e.g. RFID, barcode, QR code, badge), interactive digital touch screens and other periphery devices as needed.

As part of our holistic solutions, Signifi also offers an enterprise software platform to manage our units/devices and operational data collected, API integration to our customer's systems as needed, configurable workflows through our User Interface and end to end services ranging from design and assembly to logistics and installation to support and maintenance.

These components are packaged together into one comprehensive dispensing solution, with the software hosted in a cloud-based, Software as a Service model

Overview of Relevant Infrastructure

The Signifi system includes the following components:

**Infrastructure** – the physical and virtual IT structures.

|  |  |  |  |
| --- | --- | --- | --- |
| **Primary Infrastructure** | | | |
| **Production System** | **Type** | **Purpose** | **Physical Location** |
| **Signifi Private Cloud at Aptum Canada** | VMWare Managed Private Cloud (ESXI cluster, SAN, hardware firewall) | Host dedicated and multi-tenant application and database servers | Toronto, ON, Canada |
| **Microsoft Azure DR servers Canada** | Public cloud servers | DR (Disaster Recovery) for Aptum system | Azure Canada East, Quebec City, QC, Canada |
| **Signifi Private Cloud at Aptum USA** | VMWare Managed Private Cloud (ESXI cluster, SAN, hardware firewall) | Host dedicated and multi-tenant application and database servers | Atlanta, GA, USA |
| **Microsoft Azure DR servers USA** | Public cloud servers | DR (Disaster Recovery) for Aptum system | Azure West US 2, WA, USA |
| **Signifi Private Cloud at OVH France** | VMWare Private Cloud (ESXI cluster, SAN) | Host dedicated and multi-tenant application and database servers for clients that need GDPR compliance | Roubaix, France |
| **Signifi Backup Server at Contabo Germany** | Dedicated server | Backup for the Signifi Private Cloud OVH France | Munich, Germany |
| **Signifi Private Cloud at OVH Canada** | VMWare Private Cloud (ESXI cluster, SAN) | Host dedicated and multi-tenant application and database servers for clients that do not need GDPR | Montreal, QC, Canada |
| **Signifi HQ** | VMWare Private Cloud (ESXI, XCP-ng NAS) | Backup for the Signifi Private Cloud OVH Canada | Toronto, ON, Canada |

**Software** – the application programs and IT system software that supports the Signifi operations.

|  |  |
| --- | --- |
| **Primary Software** | |
| **Software** | **Purpose** |
| **Signifi Vision** | The Signifi main application. Manages the kiosks and their operational data, including transactions, users, products, orders. Signifi proprietary. |
| **FreshDesk** | Customer service management, third party |
| **TeamWork** | Project Management, third party |
| **ConnectWise Control/ScreenConnect** | Remote control application for access to Signifi kiosks, third party |
| **ManageEngine Desktop Central** | Remote management and monitoring, and endpoint security for desktops, servers, and mobile devices, third party |
| **Inflow** | Inventory management, third party |
| **BitDefender** | Antivirus, installed on workstations and Windows servers |

**People** – the personnel involved in the governance, operation, and use of the system

The following functional groups/teams are used to support the Signifi service delivery:

* **Support/Customer Service** provides tier1, 2 and 3 support to Signifi clients, formed of three teams:

1. Phone and remote access support team (in-house)
2. Phone and remote access 24/7 support team
3. On-site support team (in-house)

* **Operations and QA** provide deployment services, software and hardware testing and escalation support for Customer Service
* **Software Development** provides the custom Signifi applications and escalation support for Operations
* **IT** maintains and monitors the hardware and software infrastructure and manages security and compliance
* **Hardware Engineering** designs and tests the Signifi manufactured devices
* **Manufacturing** provides assembly services for the Signifi devices

For a full list of departments, see “Signifi Departmental Organizational Chart”.

**Procedures and Policies** – the automated and manual procedures and processes, and the collection of policies they are based on.

Signifi develops, maintains, and communicates to the employees and associates a set of procedures and processes to support the operation of and control over the systems:

1. Access Control, Authentication and Authorization

Documented information security policies are in place to govern acceptable use of information systems and to guide personnel in safeguarding the infrastructure, information assets and data. Information sensitivity classifications and associate's guidelines are established to handle and analyze information based on sensitivity, value, and criticality.

Access to all information systems, and in particular to Signifi Vision, the system that hosts customer data, is protected by strong passwords and password policies, access is group-based, and two/multiple-factor authentication is used (where supported). This includes production and internal servers, file stores, databases, networks, and cloud infrastructure.

All associates (employees, contractors, representatives) of Signifi use named accounts with rights derived from their role. All IT resource access is performed over encrypted connections.

2. Access Requests and Revocation

The IT department provisions, administers, and revokes user access and privileges for the network, servers, workstations, and other underlying infrastructure.

An access request is presented to IT by the HR department and the manager of the person who will be onboarded. IT grants access based on the person's role and reviews the role access rights.

If a person changes positions, a new access request is sent to IT, and the process is repeated.

Group policies (GPOs) are used to govern user access and machine settings.

Regular and ad-hoc reviews and audits are in place to check user rights and user access.

3. System monitoring

For the servers in the managed cloud, the provider performs system monitoring and informs Signifi of any exception. It uses a dedicated appliance paired with a cloud-based solution for SIEM (Security Information and Event Management) and security (antivirus, intrusion detection/protection, firewall).

For the rest of the servers and workstations, the IT department manages monitoring, security and SIEM with many tools. These applications also send email alerts.

4. Backup and Disaster Recovery

Signifi uses VM level backup tools, and all backups are stored in a location at least 200 km away from the primary data centre. Some VMs are backed up in multiple locations. The backup system sends an email after each backup job is completed with the result of that operation, and IT personnel is reviewing the emails daily. All backups are encrypted.

Disaster Recovery is performed differently depending on the hosting provider, and as such the RPO/RTO differ based on which cloud is used for that specific server. On the Aptum managed cloud, DR is automatically triggered when the primary servers become unavailable.

5. Change management

Documented processes and policies are in place to guide personnel in change management activities regarding the IT infrastructure and service delivery, from changing settings in the system, to provisioning a new server, or tracking customer requests and software improvements.

All change requests have to be approved by the manager of the initiator and by IT. The change requests contain the change description, the system affected, priority and importance of the change, time spent, prerequisites required before the work is done and risk analysis. The change is performed by authorized users only.

6. Incident response

In case of incidents, the IT and operations personnel are guided by incident response process documentation, including alert, monitoring the situation, escalating, and remedy while managing time and communication with internal and external stakeholders.

Each incident handling is then analyzed, and lessons learned are drawn and incorporated into the process.

7. Physical security

All production servers are located in facilities certified under SOC 2 or ISO 27001.

Signifi physical facilities are protected by access control systems, 24/7 video surveillance, video interphones, and alarm systems. Besides technical measures, policies and procedures are in place for granting physical access to the facilities, for both employees and visitors.

**Data** – files, databases, tables, and output used or processed by the system.

Data is defined as:

* Client data – information uploaded by our clients or that results from processing it (e.g. user information, transactions, product information). Signifi is a data processor and not a data controller. Signifi does not mine data, or otherwise analyze data except for the purpose it was contracted. Signifi does not store credit card information.
* Signifi data – information related to internal processes, users/associates, projects, and all other data that is not client data

All sensitive data is stored in encrypted databases and data transfer is always encrypted. Access to data is controlled by role and each user receives the minimum rights required to perform their duties.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

**Control Environment**

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal controls, providing discipline and structure. Aspects of Signifi's control environment that affect the services provided and/or the system of controls are identified in this section.

**Integrity and Ethical Values**

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them.

Integrity and ethical values are essential elements of Signifi's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behaviour are the product of Signifi's ethical and behavioural standards, how they are communicated, and how they are reinforced in practice.

They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, unethical, or illegal acts. Management communicates entity values and behavioural standards to personnel through policy statements and codes of conduct.

Specific control activities that the service organization has implemented in this area are described below.

• Management maintains an employee handbook that communicates Signifi's values and behavioural standards.

• Employees sign an acknowledgement form indicating they read and understand administrative policies, including those found in the employee handbook.

• Employees sign a proprietary information agreement agreeing not to disclose proprietary or third-party confidential information, including customer information, to unauthorized parties.

• Management actively monitors and reports on employees' electronic communication

**Commitment to Competence**

Signifi’s management defines competence as the skills and knowledge required to accomplish tasks that define employees’ roles and responsibilities. Management’s commitment to competence includes consideration of the competence levels for particular jobs and how those levels translate into the necessary skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

• Management has considered the requirements and responsibilities for each job

• Pre-hire screening procedures are utilized to include the following:  
- review of candidate’s resume  
- interviews  
- skills testing, where applicable  
- reference checks and  
- background screening including education and employment verification

• Documented human resources policies are maintained to guide HR personnel during hiring and termination processes. Procedures are in place to help ensure that specific elements of the hiring and terminations processes are consistently executed

• Personnel are provided with orientation, hands-on training and supervision to the extent deemed necessary by management

• Personnel are also required to complete a new hire security awareness training and annual security awareness training thereafter, to understand their obligations and responsibilities and be able to comply with the company and departmental security policies

• Performance evaluations are conducted for employees on an annual basis, conducted to help ensure employees are meeting their goals and objectives as defined during the review process

**Senior Leadership Oversight**

Signifi recognizes that effective information security management is critical to its business and clients and strives to continually deliver high-quality service that includes protecting both Signifi and client data from internal and external threats.

The Signifi board of directors and senior management team are dedicated to creating and executing appropriate security policies company wide. To ensure its information security management program is fully integrated and supports the business requirements, Signifi’s Chief Information Security Officer has been appointed by the board of directors and senior leadership to define and implement specific security-related policies, which are annually reviewed and endorsed by the senior management team.

Signifi’s senior management team also commits to the following oversight activities:

• Setting policy objectives focused on reducing risk, identifying acceptable information security risk levels, and establishing overarching company policy relating to information management, hardware, networks, and software.

• Implementation of a systematic approach to risk assessment and methods for minimizing the risks of damage to company assets and suited to compliance and regulatory requirements.

• Promoting company-wide compliance with the security policy requirements and ensuring Signifi associates and computer systems do not infringe on any copyright or licensing laws.

• All Signifi managers, employees, representatives, and contractors are trained and responsible for complying with company policies.

**Organizational Structure and Assignment of Authority and Responsibility**

Signifi’s organizational structure provides the framework within which its activities for achieving company-wide objectives are planned, executed, controlled, and monitored.

Management believes that establishing a relevant organizational structure includes considering critical areas of authority and responsibility. Signifi has developed an organizational structure suited to its needs. This structure is based, in part, on the size and nature of its activities. Signifi’s assignment of authority and responsibility activities includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established.

This includes policies relating to business processes, key personnel's experience, and resources provided for carrying out duties. Specific control activities that the service organization has implemented in this area are:

• An organizational chart is in place to communicate key areas of authority, responsibility, and lines of reporting

• Management has considered the reporting structure and accountability for business functions and segregated responsibilities by functional areas

• Communication to employees of the organizational chart and appropriate lines of reporting

**Risk Assessment**

Signifi’s process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying essential decision factors. The Operations department oversees risk management ownership and accountability. Operations management from different operational areas is involved in the risk identification process.

**Risk Identification**

Management identifies business risk elements, including threats, vulnerabilities, safeguards, and the likelihood of a threat, to determine the actions to be taken. A risk assessment review is performed regularly to ensure that key inputs are factored in consistently across Signifi’s operations. In addition to the scheduled annual assessments, Signifi has identified the following as reasons for prompting an ad hoc risk assessment to be performed:

• Significant changes to the business affecting information security.

• A new contract involving vendors with access to Signifi or client data; and

• After an information security incident.

Signifi has also considered risks that could affect the organization's ability to provide reliable service to both internal and external user entities. Management considers risks that could affect customers based on the services they receive from Signifi.

The Signifi risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying essential decision factors.

**Risk Factors**

Management considers risks that can arise from both external and internal factors, including the following:

**External Factors:**

• Changing customer needs or expectations

• Technological developments that affect the market Signifi operates into

• Competition that could alter marketing or service activities

• New legislation or regulation that could force changes in policies and strategies

• Disasters and other factors that could lead to changes in operations or information systems

• Economic changes that could have an impact on management decisions

**Internal Factors**

• Significant changes in policies, processes, or personnel

• Fraud opportunities and fraud incentives and pressures for employees

• A disruption in information systems processing

• The quality of personnel

• Changes in management responsibilities

**Risk Analysis**

Annually, or as the organization goes through significant changes that affect risks, the management team reviews the risk assessments and plans appropriate mitigating action plans. Risk assessments at a minimum address the following:

• Unauthorized access.

• Malicious or unintended use of access control credentials.

• Unauthorized disclosure.

• Loss of or Disruption of services; and

• Modification or destruction of the information system.

**Monitoring**

Signifi management established controls to determine whether they are operating as intended and that the controls are modified for changes in conditions. Management performs monitoring activities to continuously assess the quality of internal control over time continuously. Management is responsible for directing and controlling operations and establishing, communicating, and monitoring control activities and procedures. Management places emphasis on maintaining sound internal controls, as well as ensuring integrity and ethical values to Signifi personnel.

Signifi uses an enterprise monitoring application to monitor the computing and networking resources used in production. The application monitors the hardware environment, such as the network and host and virtual servers' availability. The enterprise monitoring application is configured to send email alerts to IT personnel when predefined thresholds are exceeded on monitored systems and provides statistical reports to monitoring personnel.

A ticketing system is in place to manage system incidents, response, and resolution.

Signifi also has installed a SIEM (Security Information and Event Management) application, which provides real-time analysis of security alerts on production equipment. Email alerts are sent to Signifi personnel when certain activities are detected.

**Monitoring activities**

Signifi management established controls to determine whether they are operating as intended and that the controls are modified for changes in conditions. Management performs monitoring activities to continuously assess the quality of internal control over time Management is responsible for directing and controlling operations and establishing, communicating, and monitoring control activities and procedures. Management places emphasis on maintaining sound internal controls, as well as ensuring integrity and ethical values to Signifi personnel.

**Evaluating and Communicating Deficiencies**

Customer complaints are tracked in an automated ticketing system and reviewed for consideration on how to improve control activities.

The deficiencies identified by the Signifi employees and associated are logged in the IT tracking system. This system allows assigning ownership of the issue, tracking progress and reporting completions as needed to maintain the highest level of performance. Corrective changes to existing documents or procedures are announced to affected personnel.

Comments and feedback are incorporated and reviewed by senior management at the conclusion of any audit or auditable actions.

Trust Services Criteria and Related Control Activities

**Integration with Risk Assessment**

Along with assessing risks, Signifi management has identified and executed actions needed to address those risks. To address risks, control activities have been placed into operation to help ensure that the actions are carried out correctly and efficiently. Control activities serve as mechanisms for managing the achievement of security and availability.

**Selection and Development of Control Activities**

Signifi utilizes the risk assessments results to prioritize the information security risks and take the appropriate actions for implementing controls selected to mitigate risks. Risk analysis is an essential process for the entity's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the risk level. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk.

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 | 2020-12-07 | First version | Razvan Anghelidi |
| 1.01 | 2020-12-08 | Proofing | Jamie McDowell |
| 1.02 | 2021-01-21 | Formatting changes | Razvan Anghelidi |
| 1.03 | 2021-07-29 | Added Aptum USA hosting | Razvan Anghelidi |
| 1.04 | 2021-12-12 | Annual review | Hadeel Alzuhairi |