

IT205   
IT Security Incident Response Plan

|  |  |
| --- | --- |
| Status | Final |
| Version | 2.11 |
| 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](#_Toc26134101)

[Introduction 4](#_Toc26134102)

[Purpose 4](#_Toc26134103)

[Audience 5](#_Toc26134104)

[Scope 5](#_Toc26134105)

[Policy Statement 6](#_Toc26134106)

[Document Control 7](#_Toc26134107)

[Exceptions 8](#_Toc26134108)

[Enforcement 10](#_Toc26134109)

[Revision History 10](#_Toc26134110)

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 20th, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | December 19th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Computer information systems and networks are an integral part of business at Signifi and its affiliates. These systems and infrastructure provide access to financial, administrative and confidential information. Security is critical to the physical and logical network, systems, applications and databases with each area offering its own set of security issues and risks. The protection of information systems is essential to manage business risk at Signifi. The nature of our business requires that we ensure the confidentiality, integrity and availability of Signifi information systems to provide high quality products and services to our members.

Purpose

To maintain the trust of Signifi’s employees, customers, and partners and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a cyberattack. The better prepared we are to respond to a potential attack, the faster we can eradicate any threat and reduce the impact on the business.

This document describes the plan for responding to information security incidents at Signifi. It will explain how to detect and react to cybersecurity incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders.

Effective incident response involves every part of our organization, including IT team, technical support, operations/QA, development, legal, human resources, and corporate communications. It is important that the roles are well understood, as well as the ways of coordination with others.

This plan will be updated annually to reflect organizational changes, new technologies and new compliance requirements that concern our cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

Roles, Responsibilities, Contact Information

This Incident Response Plan must be followed by all personnel, including all associates, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of Signifi. All personnel are referred to as ‘staff’ within this plan.

Below are details about the roles and responsibilities of each member of Signifi to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

Incident Response Team Responsibilities

The **Incident Response Lead** is responsible for:

• Making sure that the IT Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.

• Making sure that the Incident Response Plan is current, reviewed and tested at least once each year.

• Making sure that staff with Incident Response Plan responsibilities are properly trained at least once each year.

• Leading the investigation of a suspected breach or reported security incident and initiating the Incident Response Plan when needed.

• Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.

• Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

**Security Incident Response Team (SIRT)** members are responsible for:

• Making sure that all staff understand how to identify and report a suspected or actual security incident.

• Advising the Incident Response Lead of an incident when they receive a security incident report from staff.

• Investigating and documenting each reported incident.

• Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.

• Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.

• Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.

• Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.

• Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.

• Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All **staff members** are responsible for:

• Making sure they understand how to identify and report a suspected or actual security incident.

• Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).

• Reporting any security related issues or concerns to line management, or to a member of the SIRT.

• Complying with the security policies and procedures of Signifi.

Roles and Contacts

|  |  |  |
| --- | --- | --- |
| ROLE | RESPONSIBILITY | CONTACT DETAILS |
| **INFORMATION SECURITY** | | |
| **CISO** | Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan.  Authorizes when and how incident details are reported.  Main point of contact for executive team and Board of Directors. | Name: John Martin, VP, Technology  Phone: +1-416-432-2506  Email: jmartin@signifi.com  Name: Razvan Anghelidi, Director of IT  Phone: +1-647-708-3941  Email: ranghelidi@signifi.com |
| **Incident Response Team Lead and Team Members** | Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident.  Maintains incident response plan, documentation, and catalog of incidents.  Responsible for identifying, confirming, and evaluating extent of incidents.  Conducts random security checks to ensure readiness to respond to a cyberattack. | Name: Britt Swann, VP Customer Success  Phone: +1-480-662-8825  Email: bswann@signifi.com  Name: Stefano Tomio, Senior Service Delivery Manager  Phone: +1-647-381-9276  Email: stomio@signifi.com  Name: Dave Smith, Director, Support Services  Phone: +1-905-601-5522  Email: dsmith@signifi.com  Name: Joey Fleming, VP, Product Development  Phone: +1-416-993-1029  Email: jfleming@signifi.com  Name: Vahidin Sehic, Director, Quality Assurance  Phone: +1-647-833-7973  Email: vsehic@signifi.com |
| **Identity and Access Team Lead and Team Members** | Responsible for privilege management, enterprise password protection and role-based access control.  Discovers, audits, and reports on all privilege usage.  Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are.  Monitors privileged account uses and proactively checks for indicators of compromise, such as excessive logins, or other unusual behavior.  Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks.  Takes action to prevent the spread of a breach by updating privileges. | Name: John Sutton, IT Administrator  Phone: +1-416-606-6241  Email: jsutton@signifi.com  Name: Albi Dhamo, IT Administrator  Phone: +355-676-059-664  Email: adhamo@signifi.com  Name: Saimir Sako, IT Administrator  Phone: +355-676-034-534  Email: ssako@signifi.com |
| **IT Operations and Support** (internal) | Manages access to systems and applications for internal staff and partners.  Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack. | Name: John Sutton, IT Administrator  Phone: see above  Email: jsutton@signifi.com  Name: Albi Dhamo, IT Administrator  Phone: see above  Email: adhamo@signifi.com  Name: Saimir Sako, IT Administrator  Phone: see above  Email: ssako@signifi.com  Name: Hadeel AlZuhairi, IT Administrator  Phone: +1-647-677-0009  Email: halzuhairi@signifi.com |
| **Technical Partners**  (ISP, MSP, Hosting, Testing Partners, etc.)  **Third Party External Incident Response Teams** | Manages security controls to limit the progression of a cyberattack across third-party systems and organizations.  Coordinates with Internal Response Team to manage risks. Professional Incident response teams help ensure a solid Incident Response process is followed. It is highly recommended that the company identify and prepare an External Response Team that can be available in an emergency IR situation and provide any requested information prior to an emergency to help them become familiar with your environment. | Name: Razvan Anghelidi, Director of IT  Phone: 905-602-7707  Email: ranghelidi@signifi.com  Name: Oppos Inc. (consulting)  Phone: +1-416-953-0802 (Darace Rose)  Email: darace.rose@getoppos.com |
| **COMPLIANCE** | | |
| **Legal Counsel** | Confirms requirements for informing employees, customers, and the public about cyber breaches.  Responsible for checking in with local law enforcement.  Ensures IT team has legal authority for privilege account monitoring. | Name: Kevin Andrade, Legal Advisor  Phone:  Email: kevin@inhauslegal.com |
| **Audit & Compliance** | Communicates with regulatory bodies, following mandated reporting requirements. | Name: Razvan Anghelidi, Director of IT  Phone: +1-647-708-3941  Email: ranghelidi@signifi.com |
| **Human Resources** | Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees. | Name: Caroline Martin, VP, Talent Acquisition  Phone: +1-416-406-0001  Email: cmartin@signifi.com |
| **Regulatory Contacts** | Receives information about a breach according to timeline and format mandated by regulatory requirements. | Name: Kevin Andrade, Legal Advisor  Phone:  Email: kevin@inhauslegal.com |
| **COMMUNICATIONS** | | |
| **Marketing & Public Relations Lead** | Communicates externally with customers, partners, and the media.  Coordinates all communications and request for interviews with internal subject matter experts and security team.  Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach. | Name: Jamie McDowell, VP, Marketing  Phone: +1-416-707-1396  Email: jmcdowell@signifi.com |
| **Web & Social Media Lead** | Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users.  Sets up monitoring across social media channels to ensure we receive feedback or questions sent by customers through social media. | Name: Melissa Dsouza, Digital Marketing Manager  Phone: +1-437-983-6212  Email: mdsouza@signifi.com |
| **Technical Support Lead** (Internal) | Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes. | Name: Razvan Anghelidi, Director of IT  Phone: see above  Email: ranghelidi@signifi.com |
| **Technical Support Lead** (External) | Provides security bulletins and technical guidance to external users in case of a breach. | Name: Dave Smith, Director, Support Services  Phone: see above  Email: dsmith@signifi.com |

Testing and Updates

Annual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually.

2. The Incident Response Plan Testing will test Signifi’s response to potential incident scenarios to identify process gaps and improvement areas.

3. The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.

4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

Incident Response Process Overview

Below is the structured 6-step process followed in this document as defined by the SANS Institute in their Incident Handler’s Handbook. The six steps outlined are:

1. Preparation—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).

2. Identification - monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

3. Containment - perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.

4. Eradication - remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

5. Recovery - bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.

6. Lessons learned - no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

Incident Response Checklist

To demonstrate and improve the effectiveness of Signifi’s incident response team and security tools, the process requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

Also use the ‘Signifi – Incident Report (Security).xlsx’ template to record information.

|  |  |  |  |
| --- | --- | --- | --- |
| PHASE OF CYBER INCIDENT | ACTION | TEAM MEMBER/ SYSTEM | DAY/TIME  ACTION TAKEN |
| **Incident Discovery and Confirmation** | Describe how the team first learned of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.). |  |  |
|  | Note the system or systems affected (internal or production server) |  |  |
| Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm attack has occurred. Check the alerts and the SIEM systems. |  |  |
| Describe potential attacker, including known or expected capabilities, behaviors, and motivations. |  |  |
| Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party. |  |  |
| Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response. |  |  |
| Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites. |  |  |
| Evaluate extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed. (See Appendix A for more information on Threat Classification). |  |  |
| Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered. (See Appendix A for more information on Threat Classification). |  |  |
| Diagram the path of the incident/attack to provide an “at-a-glance” view from the initial breach to escalation and movement tracked across the network. |  |  |
| Collect meeting notes in a central repository to use in preparing communications with stakeholders. |  |  |
| Inform employees regarding discovery. |  |  |
| Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools. |  |  |
| Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements. |  |  |
| **Containment and Continuity** | Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems. |  |  |
| Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media. Perform a Veeam or XCP-ng backup of the affected server. |  |  |
| Force multi-factor authentication or peer review to ensure privileges are being used appropriately. |  |  |
| Change passwords for all users, service, application, and network accounts. |  |  |
| Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker. |  |  |
|  | Remove systems from production or take systems offline if needed. |  |  |
| Inform employees regarding breach containment. |  |  |
| Analyze, record, and confirm any instances of potential data exfiltration occurrences across the network. |  |  |
| Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Eradication** | Close firewall ports and network connections. |  |  |
| Test devices and applications to be sure any malicious code is removed. |  |  |
| Compare data before and after the incident to ensure systems are reset properly. |  |  |
| Inform employees regarding eradication. |  |  |
| Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Recovery** | Download and apply security patches. |  |  |
| Close network access and reset passwords. |  |  |
| Conduct vulnerability analysis. |  |  |
| Return any systems that were taken offline to production. |  |  |
| Inform employees regarding recovery. |  |  |
| Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Lessons Learned** | Review forensic evidence collected. |  |  |
| Assess incident cost. |  |  |
| Write an Executive Summary of the incident. |  |  |
| Report to executive team and auditors if necessary. |  |  |
| Implement additional training for everyone involved in incident response and all employees. |  |  |
| Update incident response plan. |  |  |
| Inform employees regarding lessons learned, additional training, etc. |  |  |
|  | Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |

Responsibilities At-a-Glance

| **Activity** | **Role** |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **CSIRT Incident Lead** | **IT Contact** | **Legal Representative** | **Communications Officer** | **Management** |
| Initial Assessment | Owner | Advises | None | None | None |
| Initial Response | Owner | Implements | Updates | Updates | Updates |
| Collects Forensic Evidence | Implements | Advises | Owner | None | None |
| Implements Temporary Fix | Owner | Implements | Updates | Updates | Advises |
| Sends Communication | Advises | Advises | Advises | Implements | Owner |
| Check with Local Law Enforcement | Updates | Updates | Implements | Updates | Owner |
| Implements Permanent Fix | Owner | Implements | Updates | Updates | Updates |
| Determines Financial Impact on Business | Updates | Updates | Advises | Updates | Owner |

Update

This document 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 (YYYY-MM-DD) | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2013-06-11 | First version | Razvan Anghelidi |
| 1.1 | 2016-05-06 | Contact updates | Razvan Anghelidi |
| 1.2 | 2019-05-06 | Updated version, contact updates | Darace Rose |
| 2.0 | 2019-12-09 | Template change, contact updates | Razvan Anghelidi |
| 2.1 | 2020-12-02 | Annual review, contact updates | Razvan Anghelidi |
| 2.11 | 2021-12-16 | Annual review, contact updates | Razvan Anghelidi |