

IT101   
Incident Management Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.03 |
| 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](#_Toc26133061)

[Introduction 3](#_Toc26133062)

[Purpose 3](#_Toc26133063)

[Audience 3](#_Toc26133064)

[Scope 4](#_Toc26133065)

[Policy Statement 4](#_Toc26133066)

[Enforcement 11](#_Toc26133067)

[Revision History 11](#_Toc26133068)

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 19th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Security incidents may cause disruption to Signifi operations, compromise security and could impact the business. An incident response plan must be in place to enable repeatable, structured and effective response to security incidents that may affect IT services and infrastructure. This policy acknowledges that a quick, effective, practiced, and orderly response is a critical determinant of a security incident's outcome. The underlying motivation for this policy is to help assure that Signifi information systems continue to be trustworthy, available, and reliable.

Purpose

The purpose of the Signifi Security Incident Management Policy is to describe the requirements for dealing with computer security incidents. A security incident is any activity that harms or represents a serious threat to the whole or part of Signifi, including but not limited to computer theft/loss; unauthorized use of computer accounts and computer systems; data compromise (virus, worm, hacking, Trojans, etc.), and other network-based resource issues – including absence of service; unauthorized changes to hardware, firmware, software or data; and unauthorized exposure of information.

Audience

This policy applies to all Signifi associates, part-time and temporary workers, trainees, contractors, and vendors.

Scope

This policy is to set the criteria for the creation of strong passwords, the protection of those passwords, and the frequency of change. The combination of a User ID and Password provides authenticated access to Signifi systems and services. In some cases, additional authentication factors, such as RSA Tokens, are also used but are beyond the scope for this policy.

Policy Statement

1. General
   1. The organization and management of an incident response capability should be coordinated or centralized with the establishment of key roles and responsibilities. A computer security incident response team (CSIRT) should be formulated with clear lines of reporting and responsibilities. This team should comprise

* Chief Information Office – Incident Commander
* Manager, Information Security – chairs the CSIRT
* CSIRT Members (Information Security, Data Center Operations, Service Desk, Application Design, and other areas in IT relevant to the Incident)
* Business unit leader liaisons (legal, communications, public relations etc.)
  1. Signifi’s incident response team should be able to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications.
  2. The incident response team’s mission is to prevent further material loss, loss of public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems or networks.
  3. The incident response team should be authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to the Executive Management Team and the appropriate authorities as necessary. A detailed Signifi Incident Response plan will be followed during an incident, regardless if the incident is real or only suspected.

1. Documentation of an Incident Response Plan
   1. Information Security must document a formal Incident Response Plan which addresses the following considerations:
   2. Roles, responsibilities, and communication strategies in the event of a compromise
   3. Coverage and responses for all critical system components
   4. Notification, at a minimum, of card brands and acquirers
   5. Strategy for business continuity post compromise
   6. Reference or inclusion of incident response procedures from card brands
   7. Analysis of legal requirements for reporting compromises in affected jurisdictions.
2. Annual Incident Management Plan Review and Testing
   1. Information Security must ensure the Incident Response Plan is reviewed and updated based on lessons learned on an annual basis. Information Security must also ensure simulated testing of the Incident Response Plan is completed and documented on at least an annual basis by the CSIRT.
   2. The Incident Commander is the ultimate owner of any information security incidents that occur and is responsible for coordinating analysis, containment, eradication, restoration, and communication activities of the CSIRT. Candidates that for any reason do not meet the requirements for employment shall remain classified as applicants and may re-apply once each month for reconsideration.
3. Annual Incident Management Plan Review and Testing

* Information Security should appoint an “Incident Commander” who will function as the authoritative point of contact. He shall appoint a delegate to coordinate management of all information security incidents (on-call rotation schedules for the Incident Commander may be used to manage Personnel workloads).
* The Incident Commander is the ultimate owner of any information security incidents that occur and is responsible for coordinating analysis, containment, eradication, restoration, and communication activities of the CSIRT.

1. Computer Security Incident Response Team Structure (CSIRT”)
   1. Information Security should establish a formal team trained to detect, analyze, contain, eradicate, recover from, and manage information security related impacts caused by an adverse incident. This team should be comprised of senior level IT staff that represent a cross-section of roles including but not limited to the following:  
      * Network Administrators
      * Firewall Administrators
      * Security Analysts
      * Core Infrastructure Administrators
      * Application Administrators
   2. Individuals selected to participate on the CSIRT should exhibit the following qualities and characteristics:  
      * Be available to respond to incidents on a 24/7 basis (on-call rotation schedules may be used to manage Personnel workloads)
      * Must perform calmly and effectively under pressure and in high stress situations
      * Must have the necessary technical, analytical and communication skills necessary to remediate, analyze, mitigate and communicate status to team members and the Incident Commander
      * Must have the ability to work effectively with vendors and partners (e.g. Managed Security Services Provider) to quickly diagnose and address incidents

1. CSIRT Incident Response
   1. Information Security CSIRT Chair shall proactively respond to information security incidents within the following guidelines:
      * Contain and clear threats that have caused harm or have the potential to cause harm to Signifi’ systems and assets
      * Where deemed necessary perform forensic preservation of evidence using trained staff or external service providers
      * Treat all incidents and related information as confidential and report/escalate incidents involving unauthorized access and/or hacking to the Chief Executive Officer or Chief Information Officer or Legal Counsel.
   2. The CSIRT should not perform any of the following without prior written authorization from the Chief Executive Officer or Chief Information Officer:
      * Perform counter-measures or attacks against potential attackers, computer systems or networks that are not owned by the Signifi; and
      * Communicate with law enforcement, media, or other external parties.
   3. In instances where physical or electronic asset(s) of Signifi are stolen off-premises, associates are required to report the incident to Law Enforcement and the Information Security team or Corporate Facilities immediately.
   4. The CSIRT Chair in consultation with Chief Information Officer (or their delegate) will decide upon the severity of the incident. This rating will be used to determine the appropriate priority and response to contain, eradicate, and recover from an incident. During the course of an incident, the CSIRT Chair in consultation with Chief Information Officer may increase or decrease the severity rating of an incident based on additional factors such as elapsed time, or progress in containing damage or harm.

**Incident Severity**

* 1. CSIRT should use the following severity levels to categorize the impact of information security incidents on Signifi’ electronic information systems and assets. The severity rating should be used to guide the appropriate response, communication (internally and externally), and remediation strategy.

|  |  |
| --- | --- |
| Severity Rating | Description |
| HIGH | Incident may affect the integrity or confidentiality of data, which may result in irreversible loss of company resources (e.g. loss of personal information data or financial information in electronic or physical formats), direct loss of revenue, financial or legal risks and/or negatively impact reputation. |
| MEDIUM | Incidents may affect the availability of systems and services but does not impact integrity or confidentiality of data. |
| LOW | Incident has a limited impact on company resources such as intermittent availability of systems and services. |
| INSIGNIFICNANT | Incident has negligible impact on company resources. |

1. Preparation for Security Incident Response
   1. Information Security should ensure the CSIRT has adequately prepared in advance for responding to incidents. Preparations should include the following at a minimum in addition to documented procedures:
      * Communications & Facilities information
      * Incident Analysis Hardware and Software
      * Incident Analysis Resources

**Incident Reporting**

* 1. Personnel must immediately notify their Manager; the IT Service Desk or Information Security of any information security events (“Adverse Events”). Examples of Adverse Events are system crashes, the observation of persons (internal or external) to Signifi having unauthorized use of system privileges or access to sensitive data and/or the execution of malicious code that may destroy data. Based on the analysis of Adverse Events, CSIRT will follow the predefined Incident Handling procedures.

**Incident Communications – Credit Card Brands**

* 1. Information Security should document procedures to follow when the Credit Card Brands require notification due a suspected and/or confirmed breach.

**Incident Communications – Affected External Parties & Vendors**

* 1. In situations where a suspected and/or confirmed breach has occurred, certain IT applications and services may become unavailable to external parties. In these situations, the Chief Executive Officer or Chief Information Officer after consulting with the Legal Department should notify the affected external parties or vendors as applicable and communicate interim business continuity measures (if required).
  2. Communications with external parties and vendors should be limited to only the minimum necessary details and core information required to communicate the service outage and/or business process changes. All external communications will be handled by the Communications and external PR team.

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 | 2019-12-16 | First version | Darace Rose |
| 1.01 | 2019-12-17 | Minor edits | Razvan Anghelidi |
| 1.02 | 2020-12-01 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |