

IT116 -  
Logging, Monitoring and Audit 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](#_Toc26135329)

[Introduction 4](#_Toc26135330)

[Purpose 4](#_Toc26135331)

[Audience 5](#_Toc26135332)

[Scope 5](#_Toc26135333)

[Policy Statement 5](#_Toc26135334)

[Enforcement 9](#_Toc26135335)

[Revision History 9](#_Toc26135336)

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 25th, 2019 |
|  |  |  |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Logging and monitoring mechanisms and the ability to track user activities are critical in preventing, detecting or minimizing the impact of a data compromise. The presence of logs allows for tracking, alerting and analysis when an incident occurs. Determining the cause of a compromise is very difficult without system activity logs.

Logs are composed of entries containing information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by various systems such as antivirus software, firewalls, intrusion detection/prevention systems, servers, workstations, networking equipment and applications.

In order to utilize logs, and reconstruct or review activities, audit logs of system and application processes must be maintained. Audit records often contain security event information, such as invalid authentication attempts, file accesses, policy changes, account changes and use of privileges. In conjunction with appropriate tools and procedures, audit logs can help IT staff detect security violations, system performance problems, and flaws in business applications.

Purpose

The purpose of this policy is to ensure audit logging is enabled on all network devices, systems and applications critical to the Signifi information systems and assets. Audit logging is mandatory on all components that are considered mission critical including but not limited to the following:

* Network Devices (e.g. Routers, firewalls, switches, intrusion detection/prevention systems, wireless access points, etc.);
* Operating Systems.
* Database Management Systems.
* Core infrastructure Servers (e.g. Active Directory, DNS, Mail, etc.);
* Application Servers; and
* Applications.

Audit logs must be reviewed by IT on a regular basis to analyze the captured events generated by Signifi systems to identify wrong-doing, system failures or for troubleshooting purposes. It is also the intent of this policy to ensure the confidentiality, integrity, and availability of logs for analysis.

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

Log files that contain sensitive information must be appropriately classified and protected.

A known, stable version of Network Time Protocol (NTP) or similar technology must be implemented and kept current for time synchronization on all production systems.

During logging, information may be examined, recorded, copied and used for authorized purposes. Use of Signifi Information Technology resources constitutes consent by employees to logging and monitoring of their actions on those systems.

1. Configuration of audit logging

IT must ensure audit trails are maintained for the following types of events:

* Access to sensitive information—Audit logging is configured to log all individual access to sensitive information. Specifically, all access to bulk production data and the production infrastructure must be logged.
* Privileged account activity monitoring – Audit logging is configured to log all system activities performed by “root”, “administrator” and/or accounts with administrative level privileges.
* Anti-Virus audit logging – Anti-virus mechanisms on all applicable components are configured to generate audit logs.
* Access Control System logging – Access control systems (i.e. card swipe) are configured to generate audit logs, and that these logs are stored for a minimum of 3 months;
* Date/Time configuration logging – All attempts to change the date and/or time on applicable components are logged.
* Initialization of audit logs – Initialization of audit logs is logged.
* Access to audit logs and event sources – All access to audit logs and event sources are logged in order to detect attempts at modifying audit trail information (e.g. hackers trying to cover their tracks);
* Failed login attempts – All invalid logical attempts to access on applicable system components are logged.
* Authentication mechanism – Methods used to authenticate a user are logged (e.g. access via SSH, RDP, web login, etc.);
* Creation and deletion of critical files and system level objects; and

Event elements to be logged – Audit log entries must include the following:

* Identity of the user who generated the audit log event.
* Type of event generated (e.g. logon, log-off, restart, etc.);
* Event timestamp.
* Indication of Success or Failure.
* Source of the event (e.g. system or component where event occurred);
* Identity of component that generated the event; and
* Access to audit files.

1. Review of system component log files

IT should ensure that procedures to review audit logs (including requirements to maintain evidence of review) for all system components on a daily basis are established. Procedures should also include requirements for following up with/investigation of exceptions. Note: The use of automated monitoring tools configured to generate alerts on suspicious activity may be used to assist in daily reviews.

1. Protection of Audit Logs

IT should ensure that audit logs are protected from alteration by ensuring the following:

* Limit access to audit logs – Access to audit logs should be restricted to only those with a job-related requirement to access audit log information;
* Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation;
* Protect logs from alteration - Audit logs should be protected from alteration (e.g. through the use of strong encryption, signing and/or hashing); and
* Backup audit logs - Audit logs should be moved to a centralized log server and/or written to media that is difficult to alter promptly after being generated.

1. External or DMZ log sources

IT must ensure audit logs for external facing technologies (e.g. firewall, DNS, mail, web, etc.) are moved to a log server or location located in a secured area on the internal Local Area Network.

1. Monitoring of log files for changes

IT must ensure audit logs are monitored using File Integrity Monitoring software configured to alert on unauthorized attempts to change the logs.

1. Storage of Audit Logs

IT must ensure audit logs are retained for a minimum of 1 year, with a minimum of 3 months immediately available for analysis (i.e. maintained ‘live’ on-line or restored from backup media).

At any time and without prior notice, Signifi management reserves the right to examine electronic messages, fax records, voicemail, web browser cache files and bookmarks, files on personal computers and other information stored on or passing through Signifi electronic communications.

Such management access assures compliance with internal policies, assists with internal investigations, operational, maintenance, auditing, security and quality assurance. Signifi IT on as need basis monitors internet traffic, web sites visited, files downloaded, instant messaging sessions, time spent on the Internet, and related information. Department managers are contacted if inappropriate or excessive use for their department’s business activities is discovered.

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 | 2020-02-25 | Minor edits | Seenan Bunni |
| 1.02 | 2020-12-04 | Annual review | Razvan Anghelidi |
| 1.03 | 2021-12-12 | Annual review | Hadeel Alzuhairi |