Log Review & Monitoring Procedure

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Procedure Statements 4

2.1 Log Review and Monitoring - Functional Responsibility 4

2.2 Event Escalation 4

3. Procedure Compliance & Enforcement 5

3.1 Compliance Measures 5

3.2 Enforcement 5

4. Glossary / Acronyms 6

4.1 Glossary / Acronyms 6

5. Document Management 7

5.1 Document Revision Log 7

5.2 Document Ownership 7

5.3 Document Coordinator 7

5.4 Document Approvers 7

5.5 Distribution 7

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Objective

The objective of this procedure is to define a step by step process for monitoring logs on the XXXX’s systems and network

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-STD-ALL-016 - Logging & Monitoring Standard*

# Procedure Statements

## Log Review and Monitoring - Functional Responsibility

This procedure is been handled by the SOC team in line with XXXX-STD-ALL-016 - Logging & Monitoring Standard. The third party carries out threat intelligence analysis for the XXXX based on logs collected and send mail alerts for issues the XXXX should decide on.

## Event Escalation

The mail alerts are sent to [helpdesk@XXXX.com](mailto:helpdesk@XXXX.com) for response, and escalations are reviewed by Head IT and ISO and decision taken on them*.*And if the alert is a P1 alert or critical, SOC would call the Head IT or ISO.

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| ISO | Information Security Officer |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
| July 10, 2020 | Michael Oyerinde | r1.0 | Creation of new Procedure |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the Security Committee.

## Document Coordinator

This Procedure is coordinated by the Head IT.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
| Security Committee |  | July 10, 2020 |
|  |  |  |

## Distribution

* *IT*
* *ISO*