1. Overview

1.1 Logging from critical systems, application and services can provide key information and potential indicators of compromise. Although logging information may not be viewed daily, it is critical to have from a forensics standpoint.

2. Purpose

2.1 The purpose of this document is to identify specific requirements that information systems must meet to generate appropriate audit logs and integrate with an enterprise's log management function.

2.2 The intention is that this language can easily be adapted for use in enterprise I.T. security policies and standards, and in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new I.T. systems, whether developed in-house or procured, support necessary audit logging and log management functions.

3. Scope

3.1 This policy applies to all production systems on Kinyo's Network.

4. Standard

4.1 General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity, including where or on what system the activity was performed from (subject)?
3. What the activity was performed on (object)?
4. When was the activity performed?
5. What tool(s) was the activity was performed with?
6. What was the status (such as success vs. failure), outcome, or result of the activity?

4.2 Activities to be Logged.

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords.

2. Create, update, or delete information not covered in #1.

3. Initiate a network connection.

4. Accept a network connection.

5. User authentication and authorization for activities covered in #1 or #2 such as user login and logout.

6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permission, changing firewall rules, and user password changes.

7. System, network, or service configuration changes, including installation of software patches and updates, or other installed software changes.

8. Application process startup, shutdown, or restart.

9. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and

10. Detection of suspicious/malicious activity such as from an Intrusion Detection of Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3 Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection.

2. Subsystem performing the action – examples include process or transaction name, process, or transaction identifier.

3. Identifiers (as many as available) for the subject requesting the action – examples include username, computer name, IP address, and MAC address. Note that such identifiers should be standardized to facilitate log correlation.

4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized to facilitate log correlation.

5. Before and after values when action involves updating a data element, if feasible.

6. Date and time the action was performed, including relevant time-zone information, if not in Coordinated Universal Time.

7. Whether the action was allowed or denied by access-control mechanisms.

8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4 Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. ***Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document.***

Mechanisms known to support these goals include but not limited to the following:

1. Microsoft Windows Event Logs collected by a centralized log management system.

2. Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system.

3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and

4. Other open logging mechanism supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

5. Policy Compliance

5.1 Compliance Measurement

The team members of the I.T. Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the I.T. Department.

5.2 Exceptions

Any exception to the policy must be approved by the I.T. Department in advance.