Log Management Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

	Ncell	Classification: Internal
	Log Management Procedure	Owner: CIO/Head of IT
		Effective Date: 30-05-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Procedure Name DOCID: PR-IT-IS-08

Document Control

i. Document Identification

Document Title and Version:	**PR-IT-IS-08 Log Management Procedure**
Effective Date:	30-05-2019
Document Author:	Information Security Team
Owner:	Information Security Team

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor’s (If Required)

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO	CIO/Head Of IT

v. Revision History

Rev	Date	Author	Description	Approved By	Date
0	30-05-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	13-12-2019
1	01-09-2019	Information Security Team	Revised – Formatting Changes	Andy Chong	17-12-2019
2	20-10-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
3	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
4	10-10-2023	Information Security Team	Review and Updating – Period changed from annual to once every two years. Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
5	27-12-2023	Tarani Prasad Chaudhary	Review-Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
6	30-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

Table of Contents

1. Purpose

The purpose of the Log Management Procedure is to mandate the requirements for monitoring and logging events from information systems and seeks to ensure proper configuration, collection and analysis of required event logs. It states the minimum set of directives that must be complied with for an effective and controlled set of log management and monitoring practices.

2. Review and Updating

This procedure shall be reviewed once in every two years or whenever significant changes occur in the organization.

3. Scope

This standard shall be applicable to all employees of Ncell as well as Third party vendors and contractors who are associated with Ncell and accessing and connecting with Ncell network. The standard will cover all the critical devices (Crown jewels) including but not limited to Ncell managed applications, devices, systems and databases.

4. Roles and Responsibilities

4.1 Information Security Team

The Information Security Team shall:

i. Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity,
ii. Ensure that the actions of individual system users can be uniquely traced to the users so they can be held accountable,
iii. Assist respective teams to identify the audit logging functions and ensure that all critical auditable security events are logged and retained, consistent with the policies, and
iv. Assist in review of identified incident logs and support in analysis of incidents wherever applicable.

4.2 Services Owners/ Unit Heads & Above

The Service Owners shall:

i. Ensure that all applications are designed and developed with relevant audit logging enabled,
ii. Create, manage and retain the application and database logs for monitoring and analysis,
iii. Analyze the application, database and OS audit logs for anomalies and alert the Information Security Officer and function head for any incident encountered, and
iv. Ensure to get in lined and work with NOC team for resolution of the events / incidents identified and record the root cause, corrective and preventive actions wherever applicable.

4.3 System/OS Administrators

i. Ensure that all the critical servers are configured to have audit logging enabled,
ii. Ensure that all the operating system data is logged for pre-defined events,
iii. Review the servers to assess their log generation, retention and log capacity, and
iv. Monitor the server logs, analyze for anomalies and alert the Information Security Officer of any incident encountered.

4.4 GSOC (Global Security Operations Centre)

i. Shall ensure the integrity and confidentiality of the Ncell systems integrated logs are maintained,
ii. Assist the Ncell team in ensuring the connectivity and integration of the critical system logs with GSOC.
iii. Help Ncell Security team to ensure the regular reporting of the events / incidents as applicable.
iv. Coordinate with NOC / Ncell Incident management team as and when needed.

5. Logging and Monitoring

5.1 Audit Event Logging

An event is any observable occurrence in an organizational information system. NCell system owners in coordination with security team shall identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs.

i. Audit events should include, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV (Personal Identity Verification) credential usage, or third-party credential usage.
ii. While defining the auditable events, system owners should consider the auditing appropriate for each of the security controls to be implemented.
iii. System owners should also define the subset of auditable events that are to be audited at a given point in time.
iv. System owners should include auditable events that are required by applicable policies and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network.
v. System / Service owners and admins should use the following in identifying and defining the audit events.
vi. The events which may be identified within server audit logs:
    a. Server startup and shutdown
    b. Loading and unloading of services
    c. Installation and removal of software
    d. System alerts and error messages
    e. User logon and logoff
    f. System administration activities
    g. Accesses to sensitive information, files, and systems
    h. Account creation, modification, or deletion
    i. Modifications of privileges and access controls
    j. Additional security-related events, as required by the System Owner or to support the nature of the supported business and applications
vii. The events which may be identified within application and database audit logs:
    a. Modifications to the application
    b. Application alerts and error messages
    c. User logon and logoff
    d. System administration activities
    e. Accesses to information and files
    f. Account creation, modification, or deletion
    g. Modifications of privileges and access controls
viii. The events which may be identified within network device (e.g., router, firewall, switch, wireless access point) audit logs:
    a. Device startup and shutdown
    b. Administrator logon and logoff
    c. Configuration changes
    d. Account creation, modification, or deletion
    e. Modifications of privileges and access controls
    f. System alerts and error messages

5.2 Content of Audit Records

The information system produces audit records containing information that, at a minimum, establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. At a minimum, the following elements should be identified within each audit record:

i. Date and time when the event occurred,
ii. The software or hardware component of the information system where the event occurred,
iii. Source of the event (e.g., network address, console),
iv. Type of event that occurred,
v. Subject identity (e.g., user, device, process context),
vi. The outcome (i.e., success or failure) of the event, and
vii. Security-relevant actions associated with processing.

5.3 Log Processing, Retention and Protection

i. Applications, databases, network components and operating systems shall be configured in such a way that log files are not over-written or deleted. Log files shall be backed up as part of the daily/weekly/monthly backup schedules,
ii. Logs shall be retained for 180 days so as to provide support for post-incident investigations,
iii. It shall be appropriate to reduce the logs by filtering out log entries and further archive the logs because of the volume and the space required to store the logs, and
iv. The information processing facilities and also the information flowing in and out shall be protected, against breaches of confidentiality and integrity. Logs that are improperly secured are highly susceptible to intentional or unintentional alteration and destruction.

5.4 Administrator Logs and Operator Logs

i. Operator and administrator logs shall be subjected to regular, independent checks against operating procedures.
ii. Activities of administrators shall be logged. Administrative Logs shall include the following: -
   a. Monitoring of account usage,
   b. Remote access,
   c. Wireless connectivity,
   d. Mobile device connection,

5.5 Audit Log Review, Analysis and Reporting

iii. Audit review, analysis, and reporting covers information security-related auditing performed by organizations.
iv. Findings should be reported to organizational entities (e.g., incident response team, help desk, information security group/department). Information security-related auditing may include the following:
   e. Monitoring of account usage,
   f. Remote access,
   g. Wireless connectivity,
   h. Mobile device connection,
   i. Configuration settings,
   j. System component inventory,
   k. Use of maintenance tools and nonlocal maintenance,
   l. Physical access,
   m. Temperature and humidity,
   n. Equipment delivery and removal,
   o. Communications at the information system boundaries,
   p. Use of mobile code,
   q. Logs on critical systems, firewalls, routers, network devices and access server logs, and
   r. Logs for logons, logoffs, and accesses to system.
v. Regular dashboards and reports shall be published by incident management team on regular basis as per incident management process.

5.6 Audit Log Reduction and Report Generation

i. Audit reduction organizes collected audit information in a summary format that is more meaningful to analysts.
ii. The report generation capability provided by the information system can generate customizable reports.
iii. Information system should be configured to provide an audit reduction and report generation capability which:
   a. Support on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.
   b. Should not alter the original content or time ordering of audit records.

iv. Ncell may employ automated tools to review audit records or should have provisioned to integrate with Global Security Operation Center (GSOC). The following audit analysis tools may be used:

    a. Audit analysis tools based on attack signature, variance techniques, and audit reduction methodologies to detect intrusion.
    b. Data reduction audit tools to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data.
    c. Query applications that have the ability to query an audit log by username, location, application name, date, and time, or other applicable parameters; and have the ability to execute reports with the results of the query.

v. Information systems should be configured to provide audit record generation capability for the list of auditable events as defined in above sections.
vi. At a minimum, audit record generation capability should be configured on the following information system components:
    a. Desktop and laptop computers (end-user environment)
    b. Servers (e.g., file and print, web, firewalls, terminal)
    c. Network components (e.g., switches, routers wireless).

5.7 Monitoring for Information Disclosure

i. Ncell security team should monitor open-source information and/or information sites for evidence of unauthorized disclosure of organizational information.
ii. Team may use tools to monitor new posts on selected websites, and commercial services providing notifications and alerts to organizations.
iii. Team may receive the information and notification from security newsletters, professional networking sites, security and technology forums etc.
iv. Only authorized users should have access to utilities that reconfigure logging mechanisms, turn the utilities on and off, and write to, modify, and read log data. Log files should be collected and archived so that an intruder cannot alter or access them to remove signs of an intrusion or add erroneous information.
v. Security incident management standard should be followed to disclose and publish the organization security incidents information to the media, public forums or Cert post management authorization.

6. Governance and Compliance

i. Exception management process shall be followed to raise the exception for this procedure.
ii. Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

7. Associated Documents

i. Organization Information Security Policy
ii. Incident Management Procedure.