BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

SECURITY LOGGING & MONITORING POLICY

Reference No.: BESSEGGEN/I&CSF/SLMP

Version: 1.2

30th May 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/SLMP		
Document Name	**BESSEGGEN – Security Logging & Monitoring Policy**		
Version No.	1.2		
Document Status	Definitive		
Issue Date	30th May 2025		
Compliance Status	Mandatory		
Review Period	One year from the date of release or earlier if required		
Security Classification	Internal Use Only		
Distribution	Part of BESSEGGEN I&CSF		
	Name	**Role**	**Signature**
Authored by	BESSEGGEN INFOTECH LLP		
Reviewed by	Prince Kumar	Developer	
Approved by	Vibhu Garg	CISO	
Released by	BESSEGGEN INFOTECH LLP		

Document Revision History		
Version	**Release Date**	**Change Description**
1.0	08th Aug 2022	Added
1.1	13th May 2024	Reviewed
1.2	30th May 2025	Reviewed

Table of Contents

1. Overview

This Policy provides management direction for the log management activities and clearly defines mandatory requirements for log generation, analysis, retention, monitoring and storage of security related events and logs. This policy of BESSEGGEN INFOTECH LLP (henceforth named as "BESSEGGEN") outlines the necessary process as well to comply with regulatory requirements related to security event logging and retention.

2. Objectives

BESSEGGEN Information System's assets (servers, workstations, firewalls, routers, switches, communications equipment, etc.) shall be monitored and logged to:

- Manage, administer, and troubleshoot systems
- Protect against unauthorized access
- Verify system and operational security
- Detect and prevent criminal or illegal activities

3. Scope:

This policy applies to all the employees of BESSEGGEN, third party vendors and clients. Responsibility and implementation of this policy resides and is managed through BESSEGGEN as mandated by Regulatory agencies CERT-IN, SEBI and ISO 27001:2013

4. Policy Statement:

This policy covers the regular and systematic review of all relevant security monitoring systems belonging to or managed by the organization to ensure that specific and adequate levels of logs are implemented and enabled in BESSEGGEN systems, applications and databases.

Refer: APPENDIX-A Logging and Monitoring Controls as per ISO 27001:2013

5. Terms used and Definition:

SN	Terms	Definitions
1	**Guidelines**	To identify how physical and logical security will be provided for hardware and software assets (locks, passwords, virus protection, etc.).
2	**Licensing**	To keep track of asset licensing, ensuring compliance with all relevant agreements, laws and regulations.
3	**Asset Management**	Asset Management is which employs predictive modeling, risk management and optimized decision-making techniques to establish asset lifecycle treatment options and related long term cash flow predictions.
4	**Risk**	A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence

5	Criticality	Criticality is the quality, state, or degree of being of the highest importance
6	Risk Analysis	A systematic use of information to identify sources and to estimate risk.
7	Risk Assessment	The overall process of risk analysis and risk evaluation, where risk analysis is defined as the systematic approach to identify an organization's exposure to uncertainty and to estimate the risk.
8	Threat	A potential to cause an unwanted incident which may result in harm to a system such as unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin
9	Non-Disclosure Agreements (NDA)	A legally binding document which protects the confidentiality of ideas, Designs, plans, concepts, or other commercial material.
10	Remote Access	Ability to get access to a computer or a network from a remote Distance.
11	Network	A configuration of communication equipment and communication links by network cabling or satellite, which enables computers and their terminals to be geographically separated, while still connected to Each other.
12	Information Security	A process of safe-guarding information assets from unauthorized access, modification, use, disruption, and destruction to ensure confidentiality, integrity, availability, and non-repudiation of information.
13	Information Security Event	An event that is caused due to any action on an Information Asset. For example, deleting a key file from a critical business system.
14	Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
15	Intrusion	An uninvited and unwelcome entry into a system by an unauthorized source.

6. Roles and Responsibilities:

SN	Roles	Responsibilities
1	CISO	To establish policy so that it protects people, assets, infrastructure and technology.
2	IST Ambassador	Coordinate the activities not only within organization as well with external bodies for information security standards and guidelines related updates.
3	Manager Compliance	Coordinate with regulatory and government agencies for information security standards, guidelines compliance and audit processes. Identifying and measuring compliance risk. Report potential frauds, waste and abuse to concerned compliance/ law agencies. Seek advice from legal counsel if needed.
4	Manager Security Operations	Information security managers are responsible for ensuring that all security programs, tools, and technologies are working correctly, as well as providing the necessary protections to the company's networks, digital communications, and databases

5	**Manager ISPP**	Conduct regular audits of policies, procedures and controls to make sure they are being adhered to standards as per regulatory authorities.
6	**IT Head**	Lead, manage, and govern the information assets are adequately protected, safely guarded and disposed-off as per data security guidelines and regulatory requirements.
7	**Head Finance**	Creating forecasting models, assessing risk in investments and ensuring all accounting activities comply with regulations.
8	**HR Head**	For leading and ensuring assets are returned back after the exit of an employee, termination, or transfer to different business units in the organization.
9	**BU Head**	Lead, manage, and govern the acquisition and application of assets within the business unit of the organization.
10	**BU SPOC**	Works closely with teams to harvest potentially reusable assets and to integrate existing assets into their work. May also develop, evolve, support, and retire assets.

7. Logging and Monitoring Guidelines:

Objective: To record events and generate evidence.

7.1 Event Logging

- Individual user access
- All security logs shall be encrypted in as per BESSEGGEN Cryptography and Encryption Policy
- All security logs shall be backed-up and archived in accordance with the BESSEGGEN Back-up Policy
- Administrators shall take appropriate precautions to prevent security logging from being deactivated, modified or deleted
- All actions taken by accounts with root or administrative privileges. (All network/ system administrator commands while logged on as system/ network administrator)
- Use of and changes to identification and authentication mechanisms—including but not limited to creation, modification, enabling, disabling, and removal of accounts and modifications of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.
- Setting/modifying firewall rules, system configurations and parameters.
- All password changes.
- Creation or modification of super-user groups.
- Packet-screening denials originating from untrusted or trusted networks

Log Review

Review the following using automated methods, where technically possible, at least daily. A report should also be generated and reviewed on quarterly basis:

- All security events.
- Logs of all systems that store, process, or transmit data.
- Logs of all critical system components

- Logs of all systems that perform security functions including but not limited to Routers, firewalls, intrusion detection systems/intrusion prevention systems, and authentication servers

Content of Log Records

- User identification.
- Type of event.
- Timestamp using internal system clocks that can be mapped to Indian Standard Time (IST).
- Success or failure indication.
- Identity or name of affected data, file, system component or resource.
- Program or command used to initiate the event.
- Source and destination addresses.

Centralized Log Management Service

An authorized central log server must be in place that:

- Collects/receives log data from systems that store, process, or transmit data.
- Collects/receives log data from networks/systems/software that perform security functions including but not limited to Routers, Switches, WLC's, AP's, firewalls, intrusion detection systems/intrusion prevention systems, authentication servers, and anti-malware software.
- Collects/receives log data in as near real time as is appropriate for the log source.
- Monitors the availability of log sources.
- Alerts authorized security personnel of inappropriate or unusual activities.
- Compiles audit records into a system-wide, time-correlated audit trail.
- Alerts authorized security personnel when log storage volume is nearing max. storage capacity

Monitoring

- Systems must be monitored for system resource utilization and overall system availability to ensure the system meets business availability and performance requirements.
- Active intrusion detection and or prevention systems shall be defined and implemented to monitor suspicious activity on network perimeter devices
- Communications both internal and external of the corporate systems shall be monitored to uphold corporate policies and standards, such monitoring includes but is not limited to:
    - Removable media devices
    - Monitoring of Email
    - Internet usage

7.2 Protection of Logs

BESSEGGEN shall ensure the existing controls are aimed to prevent logging facilities from unauthorized changes and operational problems. These controls shall include, but not be limited to:

- Log files being edited or deleted.
- Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events

- Limiting access to those with a job-related need.
- Protecting log files from unauthorized modification or deletion.
- Requiring log configuration changes to be approved by authorized security personnel.
- Only allowing defined personnel or roles to set or change which events are to be logged by specific systems

7.3 Administrator and Operator Logs

BESSEGGEN shall ensure:

- System administrator and operator logs are reviewed on a regular basis.
- All system administrators and operators do not have permission to modify or de-activate logs of their own activities

7.4 Clock Synchronization

- Synchronize all system clocks at least hourly to a designated internal time source that is accurate to the approved industry-accepted authoritative time source. Time data must be protected from unauthorized modification.
- Date and Time stamp of the audit trails for all systems, servers and network components are synchronized to facilitate the tracking of user's identity and activities
- To ensure accuracy of security log file data, all systems, servers and network devices clocks shall be synchronized using the internationally accepted Network Time Protocol (NTP)

8. Exception Management

Exceptions to the guiding principles in this policy must be documented and formally approved by the CISO/Management and exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Evidence of approval by the CISO/Management

APPENDIX-A: Logging and Monitoring Control ISO 27001:2013:

A.12.4 Logging and monitoring		
Objective: To record events and generate evidence.		
A.12.4.1	Event logging	*Control* Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
A.12.4.2	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.
A.12.4.3	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
A.12.4.4	Clock synchronization	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.