BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

INCIDENT MANAGEMENT POLICY & PROCEDURES

Reference No.: BESSEGGEN/I&CSF/IM

Version: 1.2

2nd Jun 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/IM		
Document Name	**BESSEGGEN – Incident Management Policy**		
Version No.	1.2		
Document Status	Definitive		
Issue Date	2nd Jun 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	Ankit Pruthi	Partner	
Approved by	Vibhu Garg	CISO	
Released by	BESSEGGEN INFOTECH LLP		

Document Revision History		
Version	**Release Date**	**Change Description**
1.0	08th Aug 2023	Issued
1.1	14th Nov 2024	Reviewed
1.2	2nd Jun 2025	Reviewed

Table of Contents

1. Overview

The Incident Management Policy and Procedures of BESSEGGEN INFOTECH LLP (henceforth named as "BESSEGGEN") is designed to provide guidance to employees and stakeholders on the process for reporting, responding to, and resolving security incidents & technical glitches in a timely and effective manner.

2. Objectives

The policy aims to minimize the impact of incidents on the organization's operations and reputation by defining roles, responsibilities, and procedures to ensure a consistent and coordinated response to all security incidents.

- To establish a structured approach for identifying, assessing, and responding to security incidents
- Aims to ensure that incidents are resolved in a timely manner, with minimal impact on business operations and information assets
- Incidents are properly prioritized and handled in an appropriate sequence.

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

BESSEGGEN shall prepare and implement requirements and procedures to provide direction so that the BESSEGGEN network remains secure and not vulnerable to threats.

Refer Information Security Incident Management Controls guidelines stated as per Appendix-A Information Security Incident Management Controls ISO 27001:2013

5. Terms and Definitions

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	Incident Response / Incident Management	Process for detecting, reporting, assessing, responding to, dealing with, and learning from Security Incidents.
3	Data Breach	A Security Incident that directly impacts Personal Data, Sensitive Personal Information or Personally Identifiable Information
4	Personally Identifiable Information (PII)	Means any information about a Data Subject, whether in paper, electronic, or other form, which can be used to distinguish or trace an individual's identity, such as name, email address, or telephone number.
6	Virtual Private Network (VPN)	Allow individual users to connect to the organizations private network (e.g. LAN, WAN) from a remote location using a laptop, desktop computer, or mobile device connected to the internet. VPN creates a tunnel and encrypts all transmission data between an organization's network and the remote user. Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network.
7	System	An equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, control, display, switching, interchange, transmission or reception of data and that includes computer software, firmware and hardware.
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 for protecting people, assets, infrastructure and technology.
2	IST Ambassador	Coordinate the activities not only within organization as well with external bodies for information's security standards and guidelines related updates.
3	Manager Compliance	Coordinate with regulatory and government agencies for information security standard, guidelines compliance and audit processes.
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 employee, termination, or transfer to different business unit 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. Information Security Incident Management and Improvements

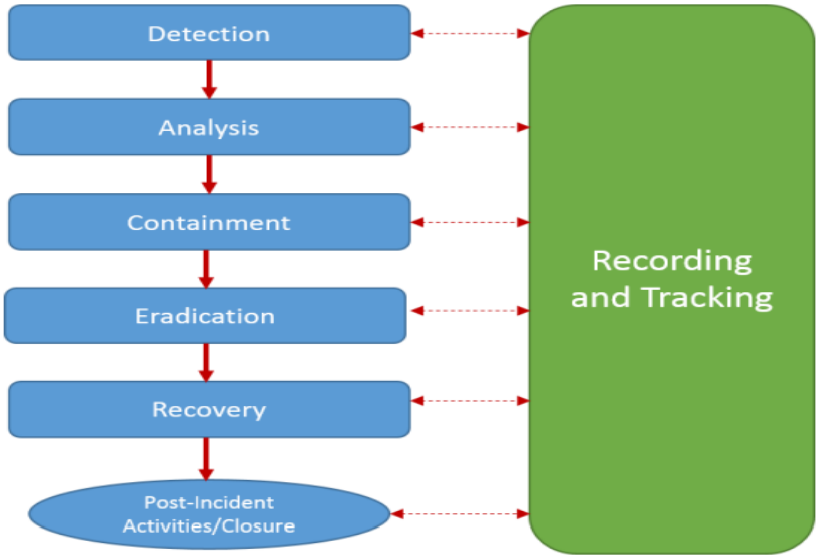
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A – Guidelines

- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to Security Incidents.
- The objectives for Security Incident management should be agreed upon with management, and it should be ensured that those responsible for Security Incident management understand the organization's priorities for handling Security Incidents.
- Security Events should be reported through appropriate management channels as quickly as possible.
- Personnel and contractors using the organization's information systems and services are required to note and report any observed or suspected Security Weakness in systems or services.
- Security Events should be assessed and it should be decided if they are to be classified as Security Incidents.

- Security Incidents should be responded to in accordance with documented Incident Response procedures.
- Knowledge gained from analyzing and resolving Security Incidents should be used to reduce the likelihood or impact of future incidents.
- Procedures should be defined and applied for the identification, collection, acquisition, and preservation of information, which can serve as evidence.
- Awareness should be provided on topics such as:
    - The benefits of a formal, consistent approach to Incident Management (personal and organizational);
    - How the program works, expectations;
    - How to report Security Incidents, who to contact;
    - Constraints imposed by non-disclosure agreements.
- Communication channels should be established well in advance of a Security Incident. Include all necessary parties in relevant communication:

B – Incident Response Process



7.1. Responsibilities and Procedures

- Information security incidents responsibilities and appropriate procedures shall be established to ensure an effective response against information security related events.
- All BESSEGGEN employees shall understand their responsibility towards reporting related security incidents.
- Chief Information Security Officer in cooperation with Business Head shall develop an information security incident management process. This process shall include, but not be limited to:
    - Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
    - Limiting or restricting further impact of the incident.
    - Monitoring and reporting the incident.
    - Tactics for containing the incident.
    - Responding and escalating the incident.

    - Corrective action to repair and prevent reoccurrence.
    - Communication across organization to those affected.
    - Collection of any evidence.
- All information security incidents resulting in disruption in the services or loss of assets shall be analyzed to identify any emerging trends. All such incidents and trend analysis shall be analyzed by CISO and Business Heads in a periodic basis.
- Potential information security incidents shall be communicated to relevant personnel who shall assist in corrective actions to be taken and avoidance of repetitive incidents
- All BESSEGGEN employees, third party/ vendor personnel shall be made aware by the IT about the types of information and cyber security incidents as well as the process of reporting the Incidents through the IT Incident Reporting System (IRS) tool, during the annual/ refresher IT security trainings.
- Any BESSEGGEN personnel/ user or IT Infrastructure department member can report information/ cyber security incident through the IT Incident Reporting System (IRS) tool.
- A clear Incident Description shall be provided while reporting the incident, as well as details including date and time of the incident occurrence
- Classification (as per categories below) of the incident and response to the incident shall be the responsibility of the IT Infrastructure team at BESSEGGEN.
- Post Incident Resolution, Closing the incident with relevant closure details and Root Cause Analysis (RCA) details, shall be the responsibility of the IT Infrastructure team at BESSEGGEN.

7.2. Reporting Information Security Events & Technical Glitches.

- CISO in cooperation with Business Head shall develop an “Information Security Incident Management Form” in order to report all security violations/incidents which establish a quick response mechanism to information security incidents.
- All BESSEGGENs employees shall understand, and be able to identify any unexpected or unusual behavior on the assets which could be a potentially software malfunction. Security events may include, but not be limited to:

    - Uncontrolled system changes.
    - Access violations (e.g., password sharing).
    - Breaches of physical security.
    - Systems being hacked or manipulated.
    - Loss of information confidentiality (e.g., data theft).
    - Compromise of information integrity (i.e., damage to data or unauthorized modification).
    - Misuse of information, assets and or services.
    - Systems infection by unauthorized or harmful program and or software.
    - Unauthorized access attempt.
    - Unauthorized changes to hardware, software or infrastructure configuration.
    - Unusual system behavior.

- All BESSEGGEN employees shall immediately report all suspected security related events to IT Helpdesk. The following information shall be generated but not be limited to:

    - Name of the Business unit involved and person(s) who were involved in the incident
    - Whether the loss of the information puts any person or other data at risk.

- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.
- Unique Incident ID
- Incident description
- Incident classification
- Impact of the incident
- Time stamps of when the incident occurred and when remedial measures were taken
- Personnel who attended to the incident
- Escalation process and contact points
- Remedial measures taken
- Learnings for future protection

- BESSEGGEN shall generate reports on incidents on monthly basis

7.3. Reporting Information Security Weaknesses

- All BESSEGGEN employees shall report any suspected information security related weaknesses in systems or services.
- Information security related weaknesses shall be reported to CISO as quickly as possible and the incident response and escalation procedure shall be followed. Security weaknesses may include, but not be limited to:
  - Inappropriate antivirus or firewall protection.
  - System Related issue or Overloads.
  - Malfunctioning of SW applications.
  - Human errors.

7.4. Assessment of and Decision on Information Security Events

BESSEGGEN shall evaluate an information security incident in terms of:

- **Criticality**
- **Possible Business Impact**
- **Maximum tolerable downtime**

Following Table is used for Incident classification and escalations

Impact severity level	Impact zone	Preferred resolution target	Escalation	Examples

Devastating (Level 3)	Facility/ Data Center	4 hours	Top Management / CISO/ Head-IT / Business Heads	Immediate and long-term threat to Data Centre, hub room, facility and/ or multiple processes for prolonged time; Downtime of an entire BESSEGGEN application or database resulting in delay in processing of reports; Unauthorized disclosure of highly confidential information. Severe Power outage, Fire
High (Level 2)	One or few Operations affected	6 hours	CISO/ Head-IT / Business Heads	Virus threat, Partial disruption of activities (affecting up to 30% of operations), Unauthorized disclosure of confidential information
Moderate (Level 1)	Operation partially	8 hours	Head IT / Business Head / CISO SPOC	Some part of the application not working, issues with Batch processing, Internal applications not functioning, office communication failure etc.
Low (Level 0)	Does not affect business operations	24 hours	IT Helpdesk / IT SPOC	Tailgating, Unclaimed Access cards, Scheduled maintenance tasks etc.

Incident Risk Management committee shall assign the classification based on the information collected from the person reporting the incident. Based on the Severity and Impact, the Incident Response SPOC/ Team shall be designated. The escalation details, contact persons and their numbers are given in ANNEXURE-C.

7.5. Response to Information Security Incidents

The response to an incident shall be logged as per the following scheme:

Impact Severity	Definition	Target Response	Target Resolution
3	Devastating	10 Min	4 Hrs.
2	High	30 Min	6 Hrs.
1	Moderate	1 Hrs.	8 Hrs.
0	Low	4 Hrs.	24 Hrs.

- The actions required to recover from the information security incident shall be under a formal control. Only identified and authorized employees shall have access to the affected systems during the incident; and all of the remedial actions shall be documented in as much detail as possible.

- CISO shall be responsible to keep a track of status of incident by following up with relevant parties or persons and handling queries related to status of incident. All information security incidents shall be recorded and allocated an incident number for tracking and future reference. The record may include, but not be limited to:

    - **Causes**: whether direct and indirect, this led to the incident to happen.
    - **Impact**: which systems suffered during the incident.
    - **Actions taken**

- **Level of Impact**: what were the losses caused.
- **Date and time of occurrence**.

- The incident response procedure shall be a seamless and include contingency plans to ensure the continuing operation of information systems during the incident

7.6 Learning from Information Security Incidents

- BESSEGGEN shall do root cause analysis (RCA) and collate and review the post incident information on a regular basis.
- Any changes to the process to avoid recurrence and further improvements suggested will be documented and implemented as a result of the post incident reviews. The followings shall be considered:
    - Conducting post incident analysis in a timely manner to determine the damage/cost incurred, confirm the cause, motive of the attack and any potential mitigating actions.
    - Performing an assessment of the involved systems , their security controls and corrective actions

7.7 Collection of Evidence

- The following factors shall be taken into consideration while collecting supporting information of the Cyber incident:
    - Supporting information Logs
    - Audit trails and
    - Related documents ensure its authenticity, integrity and completeness.
- For incidents where further legal action may be required (informing regulatory or law enforcement agencies), the following factors shall be taken into consideration while collecting evidence of the incident:
    - The evidence shall be presentable to the relevant authorities as per the legal requirements
    - Admissibility of evidence shall be in adherence to the legal requirements
    - Full back up of the system/ data shall be taken and preserved in the custody of the authorized persons
- The following shall be considered:
    - That originals are not tampered with.
    - Mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory shall be taken to ensure availability;
- Any forensics work shall only be performed on copies of the evidential material.
- The integrity of all evidential material shall be protected. Copying of evidential material shall be supervised by the IT Department and the Risk Management Team

8. Exceptions

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

ANNEXURE-A Incident Management Security Controls ISO 27001:2013

A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
		Control
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
		Control
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.
		Control
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
		Control
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
		Control
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
		Control
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
		Control
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

ANNEXTURE-B

CYBER SECURITY INCIDENT REPORTING FORM

Cyber Security Incident Reporting Form

Incident No	Department in which incident Reported
Incident Description	Incident Reporting Date & Time
Steps taken to contain the incident	
Communicated to	
<ORG> CISO / Designated Officer	Stocke Excjange, SEBI Agencies, CERT-IN

<ORG NAME> <ORG LOGO>

ANNEXTURE-C

ESCALATION AND CONTACT PERSON DETAILS

S.No.	Employee Name	Function	Office Phone	Cellular	Alternate Phone	Email	Responsibility Area
1	Vibhu Garg	CISO		9711977441		vibhu@besseggen.in	