BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

SUPPLIER RELATIONSHIP MANAGEMENT POLICY AND PROCEDURES

Reference No.: BESSEGGEN/I&CSF/ SRM

Version: 1.2

1st June 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/SRM		
Document Name	**BESSEGGEN – Supplier Relationship Management Policy & Procedures**		
Version No.	1.2		
Document Status	Definitive		
Issue Date	1st June 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 May 2022	Added
1.1	8th Aug 2024	Reviewed
1.2	1st Jun 2025	Reviewed

Table of Contents

1. Overview

BESSEGGEN INFOTECH LLP (henceforth named as “BESSEGGEN") recognizes the importance of managing relationships with suppliers to ensure the consistent delivery of quality products and services. This policy establishes the framework for the management of supplier relationships, including the selection and evaluation of suppliers, communication and collaboration with suppliers, and the ongoing monitoring and improvement of supplier performance.

2. Objectives

Establishing clear communication channels with suppliers to facilitate collaboration and problem-solving approaches keeping all information security related aspects.

- Identifying and selecting suppliers that meet BESSEGGEN's standards for quality, performance, and value;
- Monitoring supplier performance to ensure ongoing compliance with BESSEGGEN's information security requirements and expectations;

3. Scope

This policy applies to all BESSEGGEN employees, Third party vendor, and clients. This policy outlines the framework and approach to the management of assets within BESSEGGEN. As mandated by the Regulatory agencies SEBI, CERT-IN and ISO 27001:2013

4. Policy Statement:

BESSEGGEN shall adopt risk management approach when identifying third-party security controls for information processing facilities and systems

Refer: Supplier Relationship Control guidelines stated below
Appendix-A Supplier Relationship Security Controls 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 modelling, risk management and optimised decision-making techniques to establish asset lifecycle treatment options and related long term cash flow predictions.
4	**Asset**	An asset is an object (physical or intangible) that has an identifiable value and a useful life greater than 12 months, that is or could be used by the entity responsible for it to provide a service.
5	**Criticality**	Criticality is the quality, state, or degree of being of the highest importance

6	**Economic value**	The Economic value of an asset is the length of time for which maintaining and operating the asset remains the lowest cost alternative for providing a nominated level of service.
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.
16	**Key Management**	In cryptography, it is the creation, distribution, and maintenance of a secret key. It determines how secret keys are generated and made available to both parties; for example, public key systems are widely used for such an exchange. If session keys are used, key management is responsible for generating them and determining when they should be renewed

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. Guidelines for Supplier-Relationship Management:

7.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that are accessible by suppliers**.**

7.1.1 Information security policy for supplier relationships

Information security requirements for mitigating the risks associated with the supplier's access to the organization's assets should be agreed upon with the supplier and documented

- At the time of entering a contract and establishing the Service Level Agreement (SLA) under the contract, CISO to:
    - Define specific roles and responsibilities of each party.
    - Identify all required security controls (e.g., processes and procedures) to be implemented by each party.
- CISO shall only provide a supplier access (e.g., VPN access) after the supplier has signed confidentiality agreement. Confidentiality agreement executed between BESSEGGEN and the supplier shall be in accordance with BESSEGGEN legal compliance policy and business requirements.
- Reports and records provided by a supplier shall be reviewed by CISO on a regular basis.
- CISO shall update their list of contracts, outsourced services as well as SLA targets and their corresponding contact details. A similar detail of BESSEGGEN team contact shall be provided to the supplier.
- The CISO should also identify and mandate information security controls to specifically address supplier access to the BESSEGGEN information in the policy. These controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:
    - A standardized process and lifecycle for managing supplier relationships
    - Defining the types of information access that different types of suppliers will be allowed, and

monitoring and controlling the access

- Minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile
- Processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third-party review and product validation
- Accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party
- Handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers
- Resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party
- Awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes, and procedures
- Awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behavior based on the type of supplier and the level of supplier access to the organization's systems and information
- Conditions under which information security requirements and controls will be documented in an agreement signed by both parties
- Managing the necessary transitions of information, information processing facilities, and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

7.1.2 Addressing Security in Supplier Agreements

Agreements with third parties involving accessing, processing, communicating, or managing BESSEGGEN information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements. Agreements/ Contracts shall be defined to ensure that:

- The third parties adhere to the BESSEGGEN Third Party Security Policy (included in this document);
- Information Security clauses shall be revised periodically in all third-party contracts
- If the third parties' subcontract any service/work pertaining to BESSEGGEN, the sub-contracted parties and their employees shall also adhere to the BESSEGGEN ISP and Third-Party Security Policy of BESSEGGEN. Third parties shall be responsible to enforce the security requirements on their sub- contractors.
- All third parties are required to sign and submit specified documents such as the Legal Agreement, Code of Conduct etc. pertaining to information security prior to any engagement
- All third parties including partners or vendors providing IT/ network hardware need to submit a certification that: -

- Equipment permits no/ following methods of remote access (vendor to declare each method of remote access along with mitigation controls).
- Audit trail/ access logs are present for all remote accesses (location and means of access to the audit trails/ logs to be specified).
- The device software/ firmware does not have any covert channels or backdoors for information flow.
- Legal liability of any data loss or leakage directly or indirectly resulting from any vulnerability/ undeclared remote access on the device shall reside with the third party including vendor or partner.

- Service Levels, including related to security, as defined in the agreements shall be monitored and reported,
- In accordance with the BESSEGGEN ISP and Third-Party Security Risk Management Framework, third parties shall be subject to independent reviews of their compliance with the security requirements. These reviews shall be facilitated by BESSEGGEN CISO
- Cyber security incident – means any real or suspected adverse event in relation to cyber security that violates any explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization, shall be informed to relevant parties at BESSEGGEN as per the agreed interval in the agreement.

7.1.3 Information and Communication Technology Supply Chain

To mitigate information security risks associated with Network/ IT Services and the product supply chain, CISO will ensure inclusion of supply chain security, the following should be addressed:

- Defining Information security standards to refer to the Network or IT product or service creation, in addition to provider partnership information security generations
- Requiring suppliers to distribute security specifications across the supply chain for information and communication technologies services, if suppliers subcontract information and communication technology services provided to an organization
- Requiring suppliers to spread acceptable security practices through the accessibility chain for information and communication technology goods, if such goods include purchased items from other suppliers
- Implementation of a monitoring framework and appropriate validation methods that have complied with specified security criteria for information and communication technology products and services
- Ensuring that essential products can be tracked across the entire supply chain and their origin
- Getting assurance that the Network products supplied function as expected without any unexpected or unwelcome features
- define rules on information sharing and any problems and compromise between organizations and suppliers concerning the supply chain

- Implementation of detailed lifecycle and availability and related security risk protocols for the management of information and communications technologies. This involves handling the uncertainties that components are no longer available because suppliers no longer work or suppliers no longer supply such components because of the advancements made in technology.

7.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

7.2.1 Monitoring and Review of Third-Party Services

- Service reports and evidence provided by the third parties shall be reviewed at regular intervals.
- Audits and /or Assessments shall be conducted at specified intervals to assess the compliance of third parties with the agreed contracts.
- Review of third-party audit trails and/or records of security incidents, operational problems, failures, fault logging and disruptions shall be done regularly.

7.2.2 Managing Changes to Third Party Services

- Management shall review all third-party contracts / agreements annually.
- Changes to the contracts with Strategic partners/third parties shall be reviewed and approved in accordance with this policy and changes to the contracts with other third parties shall be in accordance with the BESSEGGEN Third Party Security Risk Management Framework.

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: Supplier Relationship Security Control ISO 27001:2013

A.15 Supplier relationships		
A.15.1 Information security in supplier relationships		
Objective: To ensure protection of the organization's assets that are accessible by suppliers.		
	Information security policy for supplier relationships	*Control*
A.15.1.1		Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
		Control
A.15.1.2	Addressing security within supplier agreement	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organization's information.
	Information and communication technology supply chain	*Control*
A.15.1.3		Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
A.15.2 Supplier service delivery management		
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.		
	Monitoring and review of supplier services	*Control*
A.15.2.1		Organizations shall regularly monitor, review and audit supplier service delivery.
		Control
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.