BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

NETWORK SECURITY POLICY

Reference No.: BESSEGGEN/I&CSF/NS

Version: 1.1

08th Aug 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/NS		
Document Name	**BESSEGGEN – Network Security Policy**		
Version No.	1.1		
Document Status	Definitive		
Issue Date	08th Aug 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	Vibhu Garg		
Approved by	Ankit Pruthi		
Released by	BESSEGGEN INFOTECH LLP		

Document Revision History		
Version	**Release Date**	**Change Description**
1.0	19th Aug 2022	
1.1	08th Aug 2025	Reviewed

Table of Contents

1. Overview

The policy covers the management of network components, network access control, and network monitoring, is designed to help and protect the BESSEGGEN INFOTECH LLP (henceforth named as "BESSEGGEN") information security network and computing environment from accidental, or intentional damage, and from alteration or theft of data while preserving appropriate access and use.

2. Objectives

To protect all BESSEGGEN personal, business or client's data, related application systems and operating systems software from unauthorized or illegal access.

- To periodically review all networks and network services in order to ensure that unauthorized network services are not used or authorized network services are not accessed by unauthorized personnel
- To maintain the privacy of the company information, company networks shall not be used for personal and/ or private information unrelated to business activities.

3. Scope

This document covers all processes related to Media Disposal for BESSEGGEN and all its customer facing applications, as mandated by Regulatory agencies CERT-IN, SEBI and ISO 27001:2013

4. Policy Statement:

BESSEGGEN shall adopt a risk management approach when identifying network security controls for organization networks and systems.

Refer: Network Security Control guidelines stated below
Appendix-A Communication 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 optimized 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 ne 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 eternal 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. Network Security Management Guidelines

- Network shall be segmented into zones/subnets based on function and possibly location. Each of the zone/subnet may be further segregated into separate VLANs based on business and security requirements.
- All network devices should be HARDENED based on their respective secure configuration documents before being deployed in production.
- Logical position of firewall in network architecture should ensure that firewall is not bypassed. Defense-in-depth through placement of IDS/IPS solution shall be implemented to further control the internet traffic passing through these networks. These solutions shall be regularly updated with current signatures / characteristics of threats.
- Remote access to BESSEGGEN's network resources over an un-trusted network (Internet/Extranet) shall be integrated into the overall network security management.
- Clocks of all relevant information processing systems within an BESSEGGEN or security domain shall be synchronized with an agreed accurate time source.
- Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control system of the business applications.
- There should be segregation of duties for approval and implementation of configurations for network devices.
- Adequate redundancy should be provided for network links and network devices. All single points of failure within the BESSEGGEN network shall be identified and the risks in such a design shall be assessed. Where possible, failover technologies shall be in place to address network failure. Network diagram (including wireless network) shall be documented and kept up to date
- Logs generated by critical network devices shall be collected and analyzed to identify threats and exceptions

8. Network Security Requirements

Objective: To ensure the protection of information in networks and its supporting information processing facilities

Network Controls

- The IT department shall have designated Network administrators for managing the BESSEGGEN network.
- Operational responsibilities of these employees shall be separate from the IT computer operations wherever appropriate.
- To ensure security of the BESSEGGEN network, devices such as intrusion prevention and detection systems and firewalls shall be installed at the network perimeter.
- Network monitoring tools shall be implemented to automatically provide protocol anomalies, traffic analysis, hardware malfunction signals, etc.
- These tools/ devices shall be appropriately configured to customize the protection level of the network according to the Business requirements.
- Logs of these tools/ devices shall be regularly monitored by the Network administrators.
- Any anomaly detected, should be raised as a security incident, and reported and monitored as per the cyber security incident management procedure.
- The IT department shall ensure that all the data passing over the network is encrypted using appropriate encryption techniques
- Appropriate measures to ensure web and email filtering shall be implemented.
- At the time of implementing any new network component, i.e. routers and switches etc., only the IT department should configure it to prevent the disclosure of the configuration of the internal network to external and unauthorized entities.
- Any new network device like Switch, Router, Load Balancer etc. shall be thoroughly tested for any Hardware Trojan, in-built malicious script etc. before deployment
- Any changes in the network shall be reflected in the network diagram. All single points of failure within the BESSEGGEN network shall be identified and the risks in such a design shall be assessed. Where possible, failover technologies shall be in place to address network failure
- Load balancing solution shall be implemented for critical network devices in order to ensure effective performance from the devices.
- Controls that filter the traffic by means of pre-defined tables or rules shall be implemented through network gateways.
- Routing controls shall be defined based on the source and destination address checking mechanism. Appropriate controls shall be implemented to restrict internal addresses so that it cannot pass directly from the Internet and vice versa.
- Firewalls shall mask the internal IP addresses for outbound Internet access.
- There should not be concurrent access to network devices, applications and server with same user ID.

Access to Networks and Network Services:

Logical access to the Network Equipment shall be restricted to authorized users only. The appropriate security controls shall be used to restrict access to the Network systems of BESSEGGEN. All Network Equipment's shall be tested for information security requirements.

Access to Network Services

- Appropriate interfaces shall be created to segregate BESSEGGEN's networks from the networks owned by other organizations and public networks, wherever applicable.
- Appropriate authentication mechanisms shall be applied for users and information systems.
- Users shall be provided access only to the services that they are specifically authorized to use.
- Business applications shall be accessible on the network only through the approved network services and segments

Remote Access to BESSEGGEN INFOTECH LLP Networks

- Adequate security controls shall be implemented to authenticate the user for remote access. There shall be a formal procedure documented by IT/Network to manage the remote access connections. It shall be ensured that: -
- Remote access connections to BESSEGGEN network is provided to authorized users only and appropriate controls are implemented to maintain the confidentiality, integrity, and availability of information; Strong authentication and encryption mechanism shall be implemented for clients connecting to the Network;
- An updated list of all such authorizations is maintained as per GoI guidelines;
- No external party, vendor etc. shall be allowed to access the system by remote ports.
- Exclusion: Any remote access to external vendors may be provided in case of acute business needs after proper approval of CISO/ HOD. But before granting permission for such access associated, risk shall be accessed.
- Remote access to the network of BESSEGGEN is allowed through secure channels only; and may be protected by two factor authentication;
- Appropriate controls meeting the regulatory requirements are implemented, wherever applicable.
- Applications accessible via the Internet or externally may automatically timeout the session after a maximum of 10 minutes of inactivity.

Network Connection Control

- Access to network devices is to be controlled by the AAA server.
- User ID and password for employees on AAA server will be created on need-to-know basis.
- Access of Internet for employees to be restricted by Firewalls and Internet browsing is based upon Internet Web Filtering feature of Firewalls or UTM systems also they should have unique user Id to login to system.
- The download from the Internet through insecure file transfer application(s) shall be not allowed.
- If there is a business requirement for such downloads, the secure file transfer protocol shall be used for such activities with prior authorization from the CISO.
- Insecure file transfer uploads to the Internet shall not be allowed. The only exclusion to this is when data like configuration details, fault logs, screen shots, (but not limited to these), is required to be uploaded to a manufacturer, service provider or other such authorized support third parties for the purpose of diagnostics and fault repairs. Such uploads may be executed only if authorized by the owner of the equipment.

Security of Network Services

- The IT Department shall identify and document the security requirements for the network. These include requirements such as but not limited to:
- Encryption
- Intrusion detection and prevention system
- Network monitoring
- The IT department shall ensure that all the identified network security requirements are implemented for the entire network.
- If the network services are procured from a third-party service provider, these security requirements shall be embedded in the network services agreement signed with the network service provider
- A third-party independent network assessment shall also be carried out periodically to provide assurance to the management, stakeholders, and other parties involved, and to meet any regulatory requirements.
- Once any test is concluded, test results shall be documented and officially communicated with the service provider to remedy any security issues in violation of agreed SLA security arrangements..
  Assets maintained in the inventory shall be owned.

Network Segregation

- BESSEGGEN network shall be segregated into separate logical network domains.
- These domains shall be identified based on a risk assessment and different security requirements within each of the domains, by the BESSEGGEN IT department
- The data/ user groups which do not have requirements to 'talk' to each other shall be logically segregated into separate networks.
- The data flow between separate network domains shall be controlled via secure gateways.
- For wireless networks, adequate risk assessment shall be carried out to identify controls to be implemented to maintain segregation of networks

Wireless Network

- Guest wireless network shall be separated from the BESSEGGEN internal/corporate network.
- Guest devices shall be registered, profiled, sanitized and approved before connecting to BESSEGGEN internal/ BESSEGGEN Wireless network.
- All external networking connections shall be made through BESSEGGEN managed network infrastructure and shall include network security monitoring.
- Wireless networks deployed within BESSEGGEN offices and branch premises shall be approved before implementation. Controls such as secure configuration, encryption and authentication shall be implemented for wireless networks. Management of wireless networks shall be integrated into the overall network security management, done by the BESSEGGEN IT department

Firewall and Intrusion Detection/ Prevention Systems

- Requirements of flow of traffic between BESSEGGEN network/s and the Internet shall be identified and documented. Inbound and outbound traffic passing through these networks shall be filtered and/or routed via BESSEGGEN managed security technologies such as firewall and/or Intrusion

Detection System/ Intrusion Prevention System (IDS/IPS).

1. A firewall shall be implemented at each connection to an un-trusted network, and the BESSEGGEN network.
2. Any firewall access rule request is to be assessed by Head -IT before putting to CISO for approval. CISO shall evaluate any such request from all possible Cyber Security perspectives before allowing or dis-allowing it for implementation.
3. Any changes in the firewall configuration shall be documented along with the approvals, and reported to the Risk Management Committee.

9. 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: Communication Security Control ISO 27001:2013

A.13 Communications security		
A.13.1 Network security management		
Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1	Network controls	*Control* Networks shall be managed and controlled to protect information in systems and applications.
A.13.1.2	Security of network services	*Control* Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided inhouse or outsourced.
A.13.1.3	Segregation in net works	*Control* Groups of information services, users and information systems shall be segregated on networks.