BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

Internet Usages Policy

Reference No.: BESSEGGEN/I&CSF/IU

Version: 1.2

30th May 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/IU		
Document Name	**BESSEGGEN Internet Usages 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	Issued
1.1	13th May 2024	Reviewed
1.2	30th May 2025	Reviewed

Table of Contents

1. Overview

The Internet Usage Policy outlines the acceptable use of the internet and related resources by BESSEGGEN INFOTECH LLP (henceforth named as “BESSEGGEN”)'s employees, vendors, and other authorized users. It is essential to ensure that all internet activities are appropriate, secure, and aligned with the organization's goals and values.

2. Objectives

This policy provides guidelines for the responsible use of the internet and helps to mitigate the risks associated with unauthorized or inappropriate internet use.

- To establish clear guidelines for the appropriate and secure use of the internet and related resources by BESSEGGEN's employees, vendors, and authorized users.
- Aims to ensure that all internet activities are in compliance with applicable laws and regulations, do not pose any security risks to BESSEGGEN's information systems, and do not negatively impact the organization's productivity or reputation

3. Scope

The Internet usage Policy applies to all Internet users (individual employees, third-party vendors, business partners etc.) who access the Internet through the BESSEGGEN networking resources as mandated by regulatory agencies e.g., CERT-IN, SEBI and ISO 27001:2013

4. Policy Statement:

BESSEGGEN employees and third-party vendors are expected to use the Internet responsibly and productively. Internet access is limited to job related activities only and personal use is not permitted unless prior approvals on need and role basis only as per business requirements.

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	**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	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.
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 it protects 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 standards, 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 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. Internet Usages Guidelines and Procedures:

7.1 Internet Usages Requirements

7.1.1 Acceptable Use

- All Internet data that is composed, transmitted and/or received by BESSEGGEN information systems is considered to belong to BESSEGGEN and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other regulatory agencies
- The equipment, services and technology used to access the Internet are the property of BESSEGGEN and the BESSEGGEN reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails sent via the email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by BESSEGGEN if they are deemed to be harmful and/or not productive to business
- The installation of other software's such as instant messaging technology is strictly prohibited
- Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions
- All users must follow the BESSEGGEN principles regarding resource usage and exercise good judgment in using the Internet
- However, **CISO/Management** reserves the right to add or delete services as business needs change or conditions warrant
- Following standard Internet services will be provided to users as needed:
    - **E-mail** -- Send/receive E-mail messages to/from the Internet.
    - **Navigation** -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated BESSEGGEN public web servers only.
    - **File Transfer Protocol (FTP)** -- Send data/files and receive in-bound data/files, as necessary for business purposes.
    - **Telnet** -- Standard Internet protocol for terminal emulation.

7.1.2 Prohibited Use

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorization; Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the organization
- Hacking into unauthorized websites
- Sending or posting information that is defamatory to the organization, its products/services, colleagues and/or customers
- Introducing malicious software onto the organization network and/or jeopardizing the security of the organization's information communications systems;
- Passing off personal views as representing those of the organization.
- The BESSEGGEN strongly supports strict adherence to software vendors' license agreements.

7.2 Internet Usages Procedures

7.2.1 Request & Approval Procedures

IT Team will grant internet access to users to support business activities and only as needed to perform their jobs and approved by Business Head and CISO

7.2.2 Removal of Privileges

- Internet access will be discontinued upon termination of an employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy.
- All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be re-evaluated annually.

7.2.3 Personal Usage

BESSEGGEN IT resources to access the Internet for personal purposes, without approval from the user's
Business Head and CISO, may be considered cause for disciplinary action up to and including termination.

- All users of the Internet should be aware that the BESSEGGEN network creates an audit log reflecting requests for service, both in-bound and out-bound addresses, and is periodically reviewed.
- Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The BESSEGGEN is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

7.2.4 Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage. These reviews may result in the modification, addition, or deletion of usage access rights to better suit organization information needs

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