BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

Patch Management Policy and Procedures

Reference No.: BESSEGGEN/I&CSF/PMPP

Version: 1.1

10th Nov 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/PMPP		
Document Name	**BESSEGGEN Patch Management Policy and Procedures**		
Version No.	1.1		
Document Status	Definitive		
Issue Date	08th Aug 2022		
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	**Name**	**Name**
Authored by	BESSEGGEN INFOTECH LLP		
Reviewed by	Vibhu Garg		
Approved by	Karun Singla		
Released by	BESSEGGEN INFOTECH LLP		

Document Revision History		
Version	**Release Date**	**Change Description**
1.0	08th Aug 2022	
1.1	10th Nov 2025	Reviewed

Table of Contents

1. Overview

The Patch Management Policy and Procedures of BESSEGGEN INFOTECH LLP (henceforth named as "BESSEGGEN") outlines the process for identifying, evaluating, and implementing software patches on all devices and systems that are used in the organization. The policy defines the patch management process and outlines the criteria for selecting and prioritizing patches.

2. Objectives

The policy aims to ensure that vulnerabilities and weaknesses in software applications and operating systems are addressed promptly and effectively, in order to reduce the risk of cyber-attacks and data breaches.

- To ensure that all software applications and operating systems used by BESSEGGEN are updated with the latest security patches and updates in a timely manner.
- To prioritize patches based on the level of risk they pose to the organization and to ensure that critical systems are patched first.

3. Scope

This document covers all processes related to IT Patch Management of BESSEGGEN and all its digital assets, as mandated by Regulatory agencies CERT-IN, SEBI etc.

4. Policy Statement:

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

Refer: Appendix-A Technical Vulnerability Management 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	**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 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. Patch Management Guidelines

7.1 Patch Management Requirements

- Methodology for discovering and tracking, that BESSEGGEN managed assets meet the minimum standards described in the configuration management approved baseline for hardware, software, and applications.
- BESSEGGEN monitor relevant sources of information which may alert to a need to act in relation to new security vulnerabilities.
- Conducting periodic vulnerability scanning to identify non-compliant assets for remediation.
- Patches must be obtained from a known, trusted source.
- The integrity of patches must be verified through such means as comparisons of cryptographic hashes to ensure the patch obtained is the correct, unaltered patch.
- Patches must be tested and assessed before implementation in a production environment to ensure that there is no negative impact as a result.
- A backup of the production systems must be taken before applying any patch.
- An audit trail of all changes must be created and documented.
- A Request for Change (RFC) ticket must be raised for all patch deployments including emergency updates, critical and operational updates.
- Addressing, tracking, and remediating failed updates
- In case of exceptions to the patch management policy, a formal documented approval is required from the CISO.

7.2 Patch Management Procedure

Evaluation of Patch Criticality

Patches criticality levels are decided based on below table. BESSEGGEN to ensure that the proper course of action is taken, taking the following under consideration:

- How will the patch affect the system (e.g., understanding what services and/or ports will be disabled, and what other changes may occur).
- What is the business impact if the patch is deployed?
- What is the risk to the business if deployed of the patch is delayed?

Patch Criteria	Criticality
Immediate patching is necessary to ensure the security of the individual system, and the overall security of BESSEGGEN. - Systems or applications affected are business critical, and - Exploit is likely or possible, and - No workaround exists, and - Exploit could potentially compromise additional BESSEGGEN, and - Exploit could potentially compromise BESSEGGEN information, or - Is exposed outside of other perimeter defenses.	**Critical**
Urgent patching is necessary to ensure the security of the individual system, and the overall security of BESSEGGEN. - Systems or applications affected are business critical, and - Exploit is likely or possible, and - No workaround exists, and - Exploit could potentially compromise additional BESSEGGEN assets	**Important**
Action is required soon, although it may be postponed due to business need. - Systems or applications affected are non-business critical, and - Exploit is likely or Exploit is possible, but more difficult to implement, and - No workaround exists or Undesirable, but possible, workarounds exist.	**Moderate**
Action may be required, but thorough testing should be done before installation on production servers. - Systems or applications affected are non-business critical, and - Exploit is likely or Exploit is possible, but more difficult to implement, and - Viable workarounds exist.	**Low**

Note: Response time is directly related to the criticality of the system, business impact if the system goes down, likelihood the vulnerability could occur if the system remains unpatched and the sensitivity of the data residing on or passing through the information technology asset.

Pre-Deployment Testing:

BESSEGGEN will test patches in a non-production environment for usability, security, and effects on other systems. The results of testing will then be documented and be included in the change control request and notification to business owners.

In the event a patch is found to be faulty, or the updated code is found to conflict with other software, BESSEGGEN will remediate the conflict as soon as possible to avoid the risk of the affected system/application being vulnerable to a threat that the patch is meant to prevent.

Request For Change Notification:

Once BESSEGGEN has evaluated the patch, determined deployment timeframe, and completed a change control request, the appropriate business owners will be notified. Message details will include:

a) The impact the patch has (or may have) on the affected system/application.
b) Date/time the patch will be deployed.
c) Provide a means for business owners to voice concerns.
d) Reason for the patch and the risk of not implementing it.

Patch Deployment

- Any IT system that is no longer licensed or supported by the manufacturer will be removed from the BESSEGGEN network.
- To protect the BESSEGGEN's IT systems from known vulnerabilities, security patches must be deployed in a suitable time frame. Unless prevented by BESSEGGEN IT Procedures, patches should be deployed as per the schedule defined in Evaluation of Patch Criticality.
- Where the deployment of 'Critical' or 'High risk' security patches within 14 days is not possible, either appropriate compensating controls or a temporary means of mitigation must be applied to reduce the exposure faced by the BESSEGGEN's IT systems.
- Third party suppliers must be prepared to provide evidence of up-to-date patching before IT systems are accepted into operational service.
- New systems must be patched to the current agreed baseline before coming online to limit the introduction of new threats.
- Microsoft patches are scheduled to deploy the first Monday after "Patch Tuesday". This is the unofficial name used to refer to the day Microsoft releases its security patches which typically occurs on the second Tuesday of each month.
- User Acceptance Testing (UAT) of the business system should be done only after the patching in controlled environment is done.
- A remediation plan should be deployed to return the asset to the working state prior to any patching. This could be achieved either rolling back to a last known good state or fixing forward.
- All the assets along with this policy should be reviewed every 6 months to ensure that they are accurate, effective, and up to date.

Deployment Timetable				
	Critical	**Important**	**Moderate**	**Low**
Servers in DMZ	Less than 24 hours	Less than 3 days	Less than 2 weeks	Patch included in the next scheduled maintenance cycle
Internal Servers	Less than 3 days	Less than 1 week	Patch included in the next scheduled maintenance cycle	Patch included in the next scheduled maintenance cycle
Workstations	Less than 1 week	Patch included in the next scheduled maintenance cycle	Patch included in the next scheduled maintenance cycle	Patch included in the next scheduled. maintenance cycle
Network devices - perimeter defense	Less than 24 hours	Less than 3 days	Less than 2 weeks	Patch included in the next scheduled maintenance. cycle
Network devices - Internal	Less than 1 week	Less than 2 weeks	Patch included in the next scheduled maintenance cycle	Patch included in the next scheduled maintenance cycle

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 Technical Vulnerability Management Controls ISO 27001:2013

A.12.6 Technical vulnerability management		
Objective: To prevent exploitation of technical vulnerabilities.		
A.12.6.1	Management of technical vulnerabilities	*Control* Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.