Besseggen Patch Management Policy

Doc: Version: 1.2

Document Classification: Internal

Document Control

Document Name	Besseggen Patch Management Policy
Abstract	This document describes the Patch Management policy at Besseggen Infotech LLP.
Security Classification	Internal
Location	SECTOR-94, NOIDA, GAUTAM BUDH NAGAR-201301

Authorization		
Document Owner	Reviewed by	Authorised by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	Modification Date	Section	A/M/D	Brief description of change
1.1	18 APR 2022	ALL	A	Final
1.2	28 APR 2022	5	M	Reviewed

ADDRESS: OFFICE NO 1115,ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

Distribution list
Chief Information Security Officer (CISO)
Auditors (Internal & External)
All users,committee at Besseggen Infotech LLP.

TABLE OF CONTENTS

ADDRESS: OFFICE NO 1115,ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

1. Purpose

The purpose of this policy is to ensure that the patches are rolled out on the network in a controlled and secure manner.

2. Scope

The scope of this policy includes all operating systems / applications / servers / desktops / network equipment identified in the Asset Register.

3. Policy Statement

The minimum baseline security standards shall be reviewed from the point of view of various technical vulnerabilities and vendor's recommendations for additional security patches and updated at least once in year or need based.

Guidelines for implementation

- The IT Team should document the baseline configuration of all IT assets identified in the asset inventory. The baseline is the minimum patch level required on the network. It is up to the discretion of the Head - IT to assess and establish a minimum baseline for all network components as part of the business requirements.
- Once a baseline has been established, IT shall conduct a patch analysis.
- Vulnerability assessment on the network should also be carried out at least once in a year.
- The regular updates received directly from the vendors shall also be maintained centrally and updated.
- Every patch to be deployed must be tested before being rolled out onto the production environment on need basis

ADDRESS: OFFICE NO 1115,ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

4. Responsibility for Policy

The HEAD – IT is responsible for development, maintenance, implementation, operation and escalation of enforcement of these policies and standards.

5. Procedures

5.1 Establish Current and Baseline Configuration

Once a baseline has been established the IT Team shall conduct a patch analysis to check compliance of minimum baseline for the patches. The analysis should involve determining

- If all machines on the network meet the minimum baseline established
- All approved patches for the network and
- Whether the patches are installed or missing on all the machines

5.2 Vulnerability Analysis

Vulnerability assessment on the network shall also be carried out at least once in a year. The IT Team shall analyze the severity of vulnerabilities found and prioritize and schedule the patch rollouts required on the basis of the severity found.

5.3 Procuring Patches

- The patch management coordinator shall then check and procure the required patches from the authorized vendors.
- The regular updates received directly from the vendors shall also be maintained centrally with the patch management coordinator.
- He shall record all such updates received / required in a central database.

ADDRESS: OFFICE NO 1115,ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

5.4 Testing

- Every patch to be deployed must be tested by IT and approved by the Head – IT before being rolled out by the IT onto the production environment.
- The IT Team shall maintain a test plan with acceptance criterion and also develop a roll back strategy for the same

5.5 Patch Deployment

Once the patch is successfully tested, the patch shall be deployed in the production network using change management procedure during the maintenance window period. The Head – IT shall also ensure that a roll back plan is in place, wherever possible.

6. Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or legal action as appropriate, or both. No provision of this policy will alter the at-will nature of the employment relationship at Besseggen Infotech.

7. References

None

ADDRESS: OFFICE NO 1115,ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)