Besseggen Antivirus Management Policy

Doc: Version: 1.2

Document Classification: Internal

Document Control

Document Name	Besseggen Antivirus Management Policy
Abstract	This document describes the Antivirus 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	11 APR 2022	ALL	A	Final
1.2	27 APR 2022	5	M	Reviewed

Distribution list
Chief Information Security Officer (CISO)

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)

Auditors (Internal & External)
All users, committee at Besseggen Infotech LLP.

TABLE OF CONTENTS

1. Purpose

The purpose of this policy is to implement the Antivirus controls at Besseggen Infotech.

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)

2. Scope

The scope of this policy is to provide detailed policy and procedures for implementation of Antivirus Management at Besseggen Infotech.

3. Policy Statement

3.1 Computer Virus Control

Protection against Malicious Software

- Precautions shall be taken to detect and prevent software and information processing facilities from malicious software. Users shall be made aware of the dangers of the unauthorized or malicious software like computer viruses, network worms, Trojan horses and logic bombs.
- Detection, prevention, and recovery controls to protect organization resources against malicious code shall be implemented.
- Regular reviews of the software and data content of systems supporting critical business processes should be done. The presence of any unapproved files or unauthorized amendments shall be formally investigated.
- Appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements shall be prepared.
- Installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis should be performed.

Information Leakage

- All software that is being used shall be sourced only from reputed vendors. All software from open sources shall be thoroughly tested and evaluated before being used to prevent Information leakage.

Controls against Mobile Code

- Where the use of mobile code (Active X, Java Applets etc.) is necessary

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)

as part of the business, it shall be used only after the formal approval from Head – IT. The configuration on the desktops as well as on the proxy server shall ensure that only the authorized mobile code operates, and unauthorized mobile code shall be prevented from executing.

- Management procedures shall be defined to protect against mobile code performing unauthorized actions.
- The organization shall ensure that the mobile code does not contain malicious code. Control of mobile code is essential to avoid unauthorized use or disruption of system, network, or application resources and other breaches of information security.

3.2 Anti-virus Management

- Official version with latest virus definition files of anti-virus software shall be installed on all workstations, laptops and servers. The anti-virus software shall be updated by obtaining the latest updates from the anti-virus vendor and distributed promptly across the organization.
- Personal computers (e.g. laptops, desktops) shall be scanned on a regular basis for viruses.
- System administrator shall run anti-virus software on all folders on the server on a regular basis.
- All information or files downloaded from the Internet onto a workstation and all mail attachments shall be scanned for viruses before opening them.
- Any electronic information being brought into Besseggen Infotech's IT environment e.g. diskettes, tapes etc. shall be scanned, prior to use.
- If a virus attack is suspected, the suspect personal computer shall be immediately removed from the network and the process as per the Incident Management Policy shall be followed.

4. Responsibility for Policy

The HEAD – IT is responsible for development, maintenance,

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)

implementation, operation and escalation of enforcement of these policies and standards.

5. Procedures

5.1 For control on Virus Prevention and Protection

Anti-virus software should be selected and configured in such a way that it should be capable of:

- Should be able to identify and vaccinate accurately all known viruses, macros and their variants
- Capability to scan and identify new viruses and macros depending on their signature patterns and viral activities
- Scan proactively and reactively
- Capability to vaccinate or recover original file rather than deletion
- Alert and messaging facility to notify users and administrators about the virus infection
- Anti-virus software should support the operating systems used in the organization
- The anti-virus software should be capable of scanning; memory, removable media, local and network drives, BIOS, all types of file extensions, emails, internet pages, downloads etc.
- Anti-virus should have minimum implementation issues at both the server and user end.

5.2 Procedure adopted for signatures updates & actual software update

- Signatures (virus definitions) should be updated every day or whenever available
- The anti-virus software should have timely and easy update procedures and prompt technical support

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)

5.3 Antivirus software for End Users

- Anti-virus software at desktop should be configured in such a way that it should:
- Invoke automatically at the start-up, scan for memory and all data storage devices connected to the machines
- Scan all incoming emails and attachments as and when they arrive
- Scan all incoming downloads and web pages visited by the users
- Scan all types of supported file extensions including compressed and executable files
- Anti-virus software at user end should support scanning of adware/spyware
- It should be possible to update the antivirus software manually and automatically. Periodic updates can be enforced during initial login using start-up scripts.
- If any machine is infected, it should automatically notify the details of such infection to the antivirus administrator. The antivirus administrator should present the weekly status report highlighting virus outbreaks to Head - IT.
- The antivirus software should be configured such that users cannot change the configuration settings

All users are responsible for maintaining a virus and spyware free environment. The following standards are in place to assist users in meeting this responsibility;

- Up-to-date virus/spyware-checking programs approved by Head – IT should be continuously enabled on all servers and other devices connecting to network systems.
- Since viruses and spywares are often complex and sophisticated, users should not attempt to remove them without expert assistance. Users shall contact the IT within Besseggen Infotech for assistance.
- All software and files downloaded from non-Besseggen sources via the internet or other sources should be scanned with antivirus and spyware
- Users should scan all diskettes and other media like pen drives for viruses and spyware prior to using the media

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)

6. 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)