BESSEGGEN NETWORK SECURITY POLICY

Doc: Version: 1.5

Document Classification: Internal

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)

Document Control

Document Name	Besseggen Network Security Policy
Abstract	This document describes the network security related policies at Besseggen Infotech LLP.
Security Classification	Internal
Location	SECTOR-94, NOIDA, GAUTAM BUDH NAGAR-201301

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

Amendment Log				
Version	**Modification Date**	**Section**	**A/M/D**	**Brief description of change**
1.1	06th APR 2022	ALL	A	Final
1.2	17th APR 2022	4	M	Reviewed
1.3	14th May 2024	ALL		Reviewed
1.4	21st Nov 2024	4.1.G	A	Reviewed
1.5	1st June 2025	ALL		Reviewed

Distribution list
Chief Information Security Officer (CISO)
Auditors (Internal & External)

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)

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 implement the controls for network security management at Besseggen Infotech.

2. Scope

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

3. Responsibility for Policy

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

4. Procedures

4.1. Network Server Security

Access to network services and servers must be controlled to ensure that connected users or computer services do not compromise the security of any other networked services.

Physical Controls for Network Equipment

- ✓ All critical servers and communications equipment are located in secure locked rooms.
- ✓ Additional controls such as biometric access controls are in place to secure critical or sensitive information. Access to secure areas is strictly controlled and restricted to authorize personnel.
- ✓ Secure areas will be monitored by using CCTV systems at all times.
- ✓ Visitors or third parties will not be permitted unsupervised access to secure areas.
- ✓ A separate register will be maintained in the secure areas for recording the entry of the people like vendors, contractors etc. who do not have regular access to the secure areas. Any such entry to the secure areas shall only be provided after making an appropriate entry in the register.

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)

Logical Controls for Network Equipment

a. *Protection of Network Servers:*

The following procedures must be followed to the security of the network servers:

- ✓ All servers must be protected using strong passwords, and the passwords must be managed as defined in the Password Policy Document.
- ✓ A server should be dedicated to a single network service, wherever possible. This will simplify configuration, thereby reducing the risk of configuration errors. In some cases however, it may be appropriate to offer more than one service on a single host computer (e.g. DNS, ftp and http services).
- ✓ The network services that need to be provided on a server must be identified and documented. All unwanted network services must be disabled or removed. Appropriate CRF are maintained for the same.
- ✓ A documented backup and recovery plan for critical servers must be prepared, which should include the steps needed to maintain or restore the network services after various kinds of faults.
- ✓ A documented procedure for installing the network operating system must be developed and followed. All critical parameter settings, scripts and configuration files used during installation must be documented.

b. *System and Network Logging*

- ✓ Network logs would be monitored on a whenever needed basis and incidents of abnormal activity will be reported as an exception and the same will be intimated to HEAD – IT
- ✓ At the OS level, system logs will be reviewed on defined basis and if things are normal and no incident is reported, the logs can be flushed from the system and backed up on the tapes for future reference.
- ✓ On Windows platform, event viewer (System, application and security logs) will be reviewed by the system administrator and all suspected activity reported to HEAD – IT. Event Viewer can be flushed at defined time for performance enhancement and events can be backed up on the tapes for future reference.

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)

c. *Network Switch Security*

Network Switches direct and control much of the data flowing across computer networks. Using the information presented here, the administrators can configure switches to control access, resist attacks, shield other network systems and protect the integrity and confidentiality of network traffic.

- ✓ Control physical access to switch room
- ✓ Ensure stable version of the IOS/ firmware on each switch
- ✓ Set timeouts for sessions , Configure privilege levels, Review logs
- ✓ Configure a banner, if possible, to state that unauthorized access is prohibited
- ✓ Maintain the switch configuration file offline and limit access.

d. *Router Security*

The following procedures must be adapted to ensure that the routers are properly secured:

- ✓ Routers and consoles are housed in a physically secure location.
- ✓ All router operating system upgrades from vendors are scanned for viruses before using in the production environment
- ✓ All maintenance fixes are applied on the routers during non-peak or off business-hour times
- ✓ It is ensured that a backup configuration is available in case the designated change does not work as planned.
- ✓ Network router passwords are managed as per the Password Policy. Radius Server is used for Authentication and Accounting the user logins in all the network devices.
- ✓ IP Source routing is disabled.
- ✓ Routers require a user to enter a user Id and password to gain access to the command prompt.
- ✓ Routers have appropriate login banners.

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)

- ✓ Copies of the router configuration files shall be restricted to authorize individuals only.
- ✓ The router audit logs shall be reviewed regularly

e. *Firewall Security*

Besseggen Infotech firewall is used to control the network traffic to and from the Besseggen Infotech network and avoid possible perimeter breaches. If outsiders or remote users can access the internal networks without going through the firewall, its effectiveness is diluted. The following procedures must be followed to ensure that the firewall functions appropriately.

Firewall Administration

- ✓ For any systems hosting Besseggen Infotech critical applications, or providing access to sensitive or confidential information, internal firewalls or filtering routers must be used to provide strong access control and support for auditing and logging. These controls must be used to segment the internal Besseggen Infotech network to support the access policies developed by the information/data owners.
- ✓ In case, if remote access needs to be provided to service providers, the Head – IT authorizes such access. Remote access facility to service providers is removed as soon as the job is complete.
- ✓ Physical access to the firewall terminal is limited to authorize people only. Radius Authentication is used for the same.
- ✓ The firewall administrator evaluates each new release of the firewall software to determine if an upgrade is required. Before an upgrade of any firewall component, the firewall administrator confirms with the vendor that an upgrade is mandatory.
- ✓ All security patches recommended by the firewall vendor are implemented in a timely manner.

Firewall Logs: The firewall is configured to log all events. Firewall logs are reviewed whenever needed.
Firewall Backup: The firewall (systems software, configuration data, database files, etc.) is backed up and a copy of current configuration / last configuration is available on a Central Storage Server which has

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)

appropriate access controls applied on the configuration files.

Remote Access Security

The following procedures must be followed to secure IT systems of Besseggen Infotech when they are accessed remotely.

User Authentication for Remote Access

- ✓ Firewall is used to separate the Besseggen Infotech network from an external network or a standalone network.
- ✓ Firewall is used to protect from all incoming network connections
- ✓ External parties are not allowed to connect to the Besseggen Infotech internal network.

Modem Security

Dialing in and dialing out via modems allows users to gain remote access to the network and services respectively. Users are prohibited to setup a dial in modem within Besseggen Infotech internal network.

Login Banner

- ✓ The login banner is displayed at login to all individuals gaining access either intentionally or unintentionally to any Besseggen Infotech system. It advises users that the system is for authorized personnel only and its use may be monitored. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process.
- ✓ The warning banner does not include any system or application identifiers like the type of host hardware or operating system present on the host, information about the organization, the network configuration or other internal matters, which may provide valuable information to a would-be intruder.

Clock Synchronization

System clocks are synchronized regularly, especially between the organization's various processing platforms. This allows for generating time based audit trails

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)

Access to malicious sites

We should block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.

5. 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.

6. References

Firewall CRF

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)