Besseggen Cyber Security Policy

Doc: Version: 1.2

Document Classification: Internal

Document Control

Document Name	Besseggen Cyber Security Policy
Abstract	This document describes the cyber security 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	19 APR 2022	ALL	A	Final
1.2	29 APR 2022	5,6	M	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

1. Introduction

An organization's Cyber Security and Cyber Resilience framework provides the safeguard from the:

- Cyber-attacks and threats attempt to compromise th Confidentiality, Integrity and Availability (CIA) of the computer systems, Networks and

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)

databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users).

- Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. c) Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber attack

Our Cyber Security and Cyber Resilience policy and framework cover the following areas of information security and controls as mandated by the SEBI circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018:

a. Governance
b. Identification
c. Protection
   I. Access controls
   II. Physical Security
   III. Network Security Management
   IV. Data security
   V. Hardening of Hardware and Software
   VI. Application Security in Customer Facing Applications
   VII. Certification of off-the-shelf products
   VIII. Patch management
   IX. Disposal of data, systems and storage devices
   X. Vulnerability Assessment and Penetration Testing (VAPT)
d. Monitoring and Detection

2. Governance

- The policy document approved by our Partners and required to review this policy document at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.
- This policy documents Include the following process:

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. 'Identify' critical IT assets and risks associated with such assets.
2. 'Protect' assets by deploying suitable controls, tools and measures.
3. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes.
4. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.
5. 'Recover' from incident through incident management and other appropriate recovery mechanisms.

- To implement the above framework, a Internal Technology Committee is formed comprising of following person:
    1. Mr. Vibhu Garg (Designated Partner & CISO)
    2. Mr. Karun Singla (Designated Partner)
    3. Mr. Ankit Pruthi (Designated Partner)

  This Technology Committee required to review on a yearly basis the implementation of the Cyber Security and Cyber Resilience policy and also include review of our current IT and Cyber Security and Cyber Resilience capabilities, set goals for a target level of Cyber Resilience, and establish plans to improve and strengthen Cyber Security and Cyber Resilience.

- We have trading through APIs based terminal and follow the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time. We have also followed and referred to the best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
- We have also defined the responsibilities of our employees, outsourced staff,and employees of vendors, members or participants and other entities, who may have privileged access or use our systems / networks towards ensuring the goal of Cyber Security.

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)

3. Identification

- We have a system to identify critical assets based on their sensitivity and criticality for business operations, services and data management.

- We have maintained an up-to-date inventory of our hardware and systems and the personnel to whom these have been issued, software, and information assets (internal and external), details of its network resources, connections to its network and data flows.

- We have a system to identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate with the criticality.

4. Protection

Access Control -

- We have not granted any intrinsic rights to any person by Virtue of rank or position to access our confidential data, applications, system resources or facilities.
- Access granted for our systems, applications, networks, database, etc. only for a defined purpose and defined period and on a need to use basis and based on the principle of least privileges.
- In our Access Policy, strong password controls are defined for user's access to system, applications, networks and databases.
- We have maintained the records of our user access to critical systems for audit and review purposes and retained such records for a minimum period of 6 months.

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)

- We deployed controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) of our critical systems. Such controls and measures should inter alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing system logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
- We have defined a system to deactivate the access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security -

- All our trading servers are in NSE colocation and physical access is only possible through permissions by the management.

Network Security Management -

- We have established baseline standards to facilitate the consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within our IT environment. The LAN and wireless networks are secured within our premises with proper access controls.
- For algorithmic trading facilities, adequate measures are taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.

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)

Data Security -

- We have implemented measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. Confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
- We have allowed only authorized data storage devices within our IT infrastructure through appropriate validation processes

Hardening of Hardware & Software -

- We have only deployed hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.
- We have blocked and taken measures to secure all open ports on networks and systems which are not in use or that can be potentially used for exploitation of data.

Certification of off-the-shelf products -

- We ensure that off the shelf products being used for core business functionality (such as Back-office applications) should bear Indian Common criteria certification of Evaluation Assurance Level 4.
- We understand that Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc.

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)

Patch Management -

- Patch management procedures include the identification, categorization and prioritization of patches and updates.
- Performs rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches does not impact other systems.

Vulnerability Assessment and Penetration Testing (VAPT)

- We have started conducting vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet. We do not have our trading servers connected to the internet.
- We have also carried out penetration tests with systems publicly accessible over the internet, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet.
- Remedial actions immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

5. Monitoring and Detection

- We have established appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet are also monitored for anomalies.
- Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, also

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)

implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet.

6. Response and Recovery

- We have a system to investigate the alerts generated from monitoring and detection systems in order to determine activities that are to be performed to prevent expansion of such incidents of cyber attack or breach, mitigate its effect and eradicate the incident.
- Our response and recovery plan ensures the timely restoration of systems affected by incidents of cyber-attacks or breaches.
- In case of any unforeseen incidents of loss or destruction of data or system, we will thoroughly analyze and learn lessons learned from any such incident and incorporate such results to strengthen the security mechanism and improve recovery planning and processes.

7. Periodic Audit

- We shall arrange to have our system audited on a periodic basis and shall obtain certification from any independent auditor, capable to do the same.

8. Responsibility of CISO and Other senior members

Chief Information Security Officer (CISO):

- Develop and implement the organization's overall information security strategy and policies.
- Oversee the design, implementation, and maintenance of the organization's security systems and controls.
- Establish and manage the organization's security incident response plan.

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)

- Stay up-to-date with the latest security threats, vulnerabilities, and industry best practices.
- Coordinate with other departments and senior management to ensure security measures align with business objectives.
- Provide regular reports to senior management and the board of directors regarding the organization's security posture.
- Collaborate with external parties such as auditors, regulators, and law enforcement agencies on security-related matters.
- Conduct security awareness training and education programs for employees.
- Ensure compliance with relevant laws, regulations, and industry standards.

Other Senior Personnel:

- Assist the CISO in developing and implementing security policies and procedures.
- Manage specific areas of information security, such as network security, application security, or physical security.
- Conduct risk assessments and vulnerability assessments to identify and address security gaps.
- Monitor security systems, analyze security logs, and investigate security incidents.
- Develop and implement security controls to protect the organization's data and systems.
- Collaborate with IT teams to ensure security measures are integrated into the development and operation of systems and applications.
- Stay informed about emerging security technologies and recommend their adoption if appropriate.
- Support the CISO in reporting security-related metrics and compliance status.

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)