Bajaj Hindusthan Sugar Ltd.

Cyber Security Policy

Approved on May 10, 2024

1. Preamble

Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by the worldwide distribution of information and communication technology, devices, and networks. Considering the growing role and dependency on information technology in today's business, providing the right kind of focus for creating a secure computing environment and adequate trust and confidence in electronic transactions, software services, devices, and networks, has become one of the compelling priorities for the business.

2. Purpose

The purpose of this policy is to prevent the loss, unauthorized access, disclosure, destruction, and alteration of **Bajaj Hindusthan Sugar Limited** ("C*ompany")* information produced by, entrusted to, or under the control of the c*ompany*. This policy identifies and documents the rules, responsibilities, and procedures for all individuals accessing and using *company* information, infrastructure, assets, and resources to continuously provide for the confidentiality, integrity, and availability of company information systems.
This cyber security policy is built on standards, guidelines, and specific procedures that have been determined appropriate to ensure the best affordable protection and practices are in place to securely support the growing customer and organizational needs of *Bajaj Hindusthan Sugar Limited* information systems. A violation of this policy may result in disciplinary action.

3. Cyber Security Components

Three fundamental components of this cyber security policy are:

- **Confidentiality.** Provides protection of assets from unauthorised entities. The company's information and information entrusted to the company (i.e., personal, financial, vendor, partner, etc.) should only be accessible to personnel, or systems, that have been given expressed and documented permission.
- **Integrity.** Provides assurance that the information is trusted and not manipulated. The assurance that the data and assets are uncorrupted and complete and any modification of assets is handled in a specified and authorized manner.
- **Availability**. Provides assurance that the infrastructure, services, and systems will be accessible and available to authorized users when needed. This is tied to business continuity, redundancy, and resilience. Availability may be affected by cyberattacks, misuse, or environmental risks, such as hurricanes, floods, or earthquakes.

4. Scope and Applicability

This policy applies to **everyone who has access to Bajaj Hindusthan Sugar Limited's Information Technology Resources,** and it shall be the responsibility of all IT Heads at the corporate office and plant locations to ensure that this policy is clearly communicated, understood, and followed by all users.

This Policy also applies to all contracted staff and vendors/suppliers providing services to Bajaj Hindusthan Sugar

Limited that bring them into contact with Bajaj Hindusthan Sugar Limited's Information Technology resources. The HR / Admin department and the respective Plant Heads who contract for these services shall be responsible to provide the contractor/vendor/supplier with a copy of this Policy before any access is given to them.

5. Policy Objectives

Bajaj Hindusthan Sugar Limited is committed to ensuring the protection of all aspects related to information and data assets of the organization. This includes ensuring that regulatory compliance, and contractual, and operational requirements are satisfied. The following is a list of cybersecurity goals for the *company:*

- Maintain compliance with all current and applicable legal, regulatory, and contractual security obligations.
- Establish and apply security controls to provide protection to *Bajaj Hindusthan Sugar Limited* against information systems and data against threats, such as cyber-attacks, theft, or loss.
- Ensure all employees, from the top down, are educated on the objectives of this policy
- Privacy and personal data protection.
- Resiliency, continuity, and availability of information systems and infrastructure tied to business functions and prioritized assets.

6. Internet and Computer acceptable use policy

This policy applies to all company employees and vendors provided with authorized access to company computing and communications resources.

The company recognizes that having access to the internet and e-mail from the workplace is necessary to perform the activities of employment. Unauthorized access and inappropriate use of systems can place the company, employees, shareholders, customers, and partners at risk. This policy documents the guidelines for the acceptable use of company computers, networks, digital assets, and communications systems, to mitigate the risk.

- Employees are trusted to use company-provided technology responsibly and in an appropriate manner in accordance with job requirements. Internet access and email use are provided as a privilege for work-related activities. Minimal personal use is acceptable, with discretion.
- Company employees shall not use company-provided internet, email, or any company-furnished communications devices to transmit, receive, retrieve, or store data or content that may be viewed or interpreted as defamatory, pornographic, harassing, or discriminatory.
- All employees are responsible, and are held accountable for, transmitted, stored, or downloaded content of text, images, audio, and video associated with the company's internet and email infrastructure.
- It must be understood, by all employees, that there should be no expectation of privacy when using company information systems or communications networks.
- In order to ensure the protection of the company's corporate interests, the company reserves the right to

monitor, access, record, copy, filter, retrieve, search, modify, and/or delete any document or message, that has been composed, sent, received, or stored on company information systems and log files related.

- All outgoing e-mail communications will identify the company and, therefore, shall reflect company ethics, and values and will reflect the appropriate language, content, and conduct.

7. Prohibited Activities

Prohibited activities include, but are not limited to:

- Abusive, offensive, profane, or disparaging remarks or language.
- Illegal activities, such as piracy, extortion, cracking, hacking, and unauthorized access to computers or hosts on the company network or the internet.
- The intentional downloading, installing or running of malicious code, software, or program (e.g., virus, worm, bot, trojan horse, etc.) intended to cause damage to or place excessive load on the network, subnet, host, or computer system.
- Sharing passwords, usernames, or forms of login credentials.
- Downloading unauthorized applications, program files, software, or online services from the internet without prior approval from the IT support department.
- Sender obfuscation or hiding. It is prohibited to send an email or other electronic communication with the intent to hide the identity or association of the sender.
- The use of a computer or user account that the user/employee is not authorized to use. Obtaining a password or other login credentials for a computer account to access the system.
- Attempts to circumvent data protection, event logging, or auditing activities.
- Disruption of services and activities impacting infrastructure availability. This includes sending or receiving large files and spamming activities. This also includes any activity that interferes with the normal operation of the network, hosts, computers, peripherals, or terminals.
- Copyright infringement. Copyrighted materials attributed to non-company persons or entities shall not be transmitted by employees via the company's internet-connected infrastructure without the copyright holder's permission.
- Solicitation for political, religious, or commercial endeavors, or organizations without prior and proper authorization.

8. Confidentiality

The protection and understanding of confidential information is of the utmost importance at *Bajaj Hindusthan Sugar Limited*. For the purposes of this policy, Confidential information is information that is disclosed to an individual employee or becomes known to that employee in the course of the employee's employment at *Bajaj Hindusthan Sugar Limited*, and not generally known outside of the company, or is protected by law. Confidential may include proprietary information, trade secrets, and private or personal information. Employees will, in the course of their duties, receive and handle confidential information regarding our company, other employees, our clients, partners, and vendors. We are committed to ensuring that this information remains protected. This is important to the company because it is a legal obligation and it allows us to maintain a competitive advantage,

which constitutes an important cornerstone of our business.

Each employee shall have the following responsibilities regarding *Bajaj Hindusthan Sugar Limited* Confidential Information:

- During employment and after the termination of employment, an employee will hold all confidential information in trust and confidence, and will only use, access, store, or disclose confidential information, directly or indirectly, as appropriate in the performance of the employee's duties for *Bajaj Hindusthan Sugar Limited*.
- All employees and authorized users of *Bajaj Hindusthan Sugar Limited* must comply with all applicable state and union laws and *Bajaj Hindusthan Sugar Limited* policies relating to access, use, and disclosure of confidential information.
- Employees will not remove materials or property containing confidential information from company physical or logical spaces unless it is absolutely necessary for the performance of the person's job duties. Removal of confidential information materials will be handled appropriately.
- Always lock or secure confidential information.
- When no longer needed, documents containing confidential information shall be properly destroyed.
- For questions relating to the appropriate use or disclosure of confidential information, consult with the immediate supervisor or other appropriate management personnel.

9. Data Protection

Bajaj Hindusthan Sugar Limited is committed to protecting the proprietary data of the company, and personal data and to ensuring compliance with applicable data protection and privacy laws. Data Protection describes the methods and policies in place to secure data against unauthorized access, compromise, or loss.

The *Bajaj Hindusthan Sugar Limited* policy on data protection is to ensure that the company will follow best practices and comply with data protection laws of the state, federal, and international laws that apply.

Bajaj Hindusthan Sugar Limited follows best practices to protect against the risk of unauthorized access resulting in a data breach and protects the interest of company stakeholders and the rights of employees, partners, and consumers.

A. General Data Protection Guidelines.

Every employee shares responsibility for ensuring data is collected, stored, and handled properly, and in accordance with this policy.

- Data collection shall be limited to that which is consistent with the context of the specific transaction or the consumer's relationship as required or specifically authorized by law.
- If data must be transferred electronically, it will be encrypted prior to the transfer. The IT department can be contacted for encryption methods and details on how to send data to authorized external contacts.
- Electronically stored data shall be protected from unauthorized access using robust identity and access management techniques, such as strong passwords, multi-factor authentication, and group policy.

B. Personal Data and Privacy Protection.

For the purposes of conducting business functions, it is often required to collect, store, process, transmit, and use certain information about individuals. This may include customers, suppliers, business contacts, employees,

and other personnel, for which the company has a relationship or may need to contact.

Personal information has no real value to the company unless it can be used for legitimate business purposes. It is when this data is accessed, transmitted, or used that it is at the most risk of theft, exploitation, or loss.

Training is provided to all employees to ensure the responsibilities for handling personal data is clear and understood by all company personnel.

Bajaj Hindusthan Sugar Limited adheres to the following data protection guidelines:

- Only the personnel who are required, due to the nature of their position, shall access personal data.
- Access to personal data is controlled through strict administrative and technical access control.
- Data shall not be shared informally or to unauthorized personnel.
- Data shall be reviewed and updated on a regular schedule. If data is determined to be out of date, no longer relevant, or needed, it will be deleted or destroyed appropriately.
- Express consent shall be obtained prior to the collection of personal data and clear notice will be provided to consumers of the collection of personal data use and sharing practices.
- When personal data is being used, *Bajaj Hindusthan Sugar Limited* employees shall ensure computer screens computers are always locked when left unattended.
- Details on how personal data is stored, used, and processed shall be provided upon request.

10. Business Continuity, Disaster Recovery, and Resilience.

- A business continuity and disaster recovery plan shall be implemented in line with business requirements to recover quickly after any type of disruption in critical business operations.
- A comprehensive backup procedure shall be implemented to protect business transactions. Backups shall be tested on a regular basis in accordance with the company's backup policy and procedures.

11. Security Incident Management Process:

a) A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality, and authority of data owned by the Company.
b) IT Department reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of the system.

12. Awareness and Training

It is important that company employees understand and are briefed on the policy for the use of company computers. Users will receive initial cybersecurity awareness training at the time of hire and subsequent annual refresher training to ensure they are kept aware of their responsibilities and any new threats.
IT Department may use newsletters, banners, bulletin boards, corporate Websites and Intranet etc. to increase awareness about this policy amongst their users.

13. Policy Compliance and Dissemination

a) It is the responsibility of all employees to adhere to the policy and the management has all right to take disciplinary action in case of its violation.
b) All employees of the organization need to be aware of the cyber Security Policy of the organization.
c) Employees while operating from remote/outside organization networks should strictly connect via VPN for accessing Applications and Corporate Networks.
d) Company network will be always protected from the Internet through a firewall and no system should be allowed to directly connect with the internet.
e) All employees should implement appropriate controls to ensure compliance with this policy by their users.
f) IT Department will ensure the resolution of all incidents related to the security aspects of this policy reported by their users.
g) Users should not install any network/security device on the network without consultation with the Implementing Department
h) The IT Department should ensure that training and awareness programs on use of IT resources are organized at regular intervals.

14. Maintenance and Review

The Company shall have the right to audit networks and systems at regular intervals, from the point of compliance with this policy. The company for security-related reasons or for compliance with applicable laws may access, review, copy, or delete any kind of electronic communication or files stored on devices under intimation to the user. This includes items such as files, e-mails, Internet history, etc.

Monitoring and reviewing this policy is governed by the IT department. A periodic reporting mechanism to ensure compliance with this policy should be established by the IT Department.

The Managing Director in consultation with the IT- Head is authorized to make modifications to this policy as and when deemed necessary and appropriate to ensure the purpose of the policy being served

----------****----------