Cyber Security Data Privacy & Protection Policy

Definitions

DSIL: Dwarikesh Sugar Industries Limited

Policy: Policy refers to this Cyber Security Policy

Introduction

Dwarikesh Sugar Industries Limited (herein referred to as "The Company" or "DSIL"), recognizes the critical importance of cybersecurity in safeguarding its digital assets, operations, and reputation. This Policy serves to establish a robust framework for ensuring the confidentiality, integrity, and availability of data, systems, and networks. The primary objective is to protect against cyber threats and vulnerabilities through proactive measures, risk management strategies, and employee awareness.

Objective

Our goals include preserving the confidentiality, integrity, and availability of company data, as well as mitigating cyber risks that could disrupt operations or compromise information. Additionally, we aim to ensure compliance with relevant laws, regulations, and industry standards.

Applicability/Scope

This Cybersecurity Policy applies to all employees, contractors, consultants, vendors, and third-party entities with access to the DSIL's systems, networks, and data, regardless of location or device used.

Roles & Responsibilities

Director on the board: With a relevant background in IT, the Director is engaged in the cybersecurity strategy process and oversees the Company's cybersecurity strategy.

Senior Management: Responsible for setting the overall cybersecurity strategy, allocating resources, and ensuring compliance with policies and regulations.

IT Department: Responsible for implementing and maintaining cybersecurity measures, conducting risk assessments, monitoring systems, and responding to security incidents.

Employees: Responsible for adhering to cybersecurity policies and procedures, reporting security incidents promptly, participating in training and awareness programs, and practicing vigilance in their digital activities.

Policy Statement

- The Company ensures the confidentiality, integrity, and continuous availability of information and systems, encompassing electronic and print data, across various platforms and mediums.
- The Company is dedicated to adhering to all legal, regulatory, and contractual security obligations applicable in cyberspace.
- The Company has a clear escalation process that employees can follow in the event of suspicion.
- The Company evaluates business risks from an information security perspective, striving to minimize undesired effects on business and customers.
- The Company safeguards all information from unauthorized access, use, disclosure, or modification through appropriate technical and organizational security measures.
- The Company maintains a virus-free network by auto-updating Information processing systems with the latest security patches and using approved antivirus systems.
- The Company establishes a framework to manage and address security breaches, violations, and business disruptions effectively.
- The Company ensures the continuity of critical operations aligned with business and contractual requirements.
- A comprehensive backup procedure is implemented to safeguard business transactions, with data integrity verified through SOP-compliant restoration of backup tapes.
- Only authorized and licensed software is permitted on corporate systems.
- The Company network is safeguarded from the Internet through a firewall.
- All third-party partners utilizing Company IT assets are required to sign a non-disclosure agreement (NDA).
- Servers are in secure areas with restricted access.
- All information assets used in production have either a warranty or a support contract from authorized vendors/partners.
- Disposal of media and information processing systems follows the E-waste policy.
- All changes in the information processing system are managed through the change control process.
- The Company provides relevant Information security/cybersecurity awareness training to the stakeholders. Moreover, Information security/cybersecurity is also part of the employee performance evaluation (e.g. disciplinary actions).
- Our IT infrastructure and information security management system is certified to ISO 27001.
- Our IT infrastructure and information security management systems undergo an auditing process by external auditors.

Implementation of the Policy

1. **Authentication of Access:** All devices on the network of the Company should not be accessible without proper authentication. Authentication for access to the Company's computer networks shall be obtained after following the due process and procedure as prescribed by the IT team.

2. **Data integrity:** Data is protected from unauthorized changes or tampering. We encrypt sensitive data both in transit and at rest to prevent unauthorized access or disclosure. Additionally, we regularly back up critical data and establish disaster recovery plans to ensure data availability in case of system failures.

3. **System integrity**: Our system provides consistent and expected results with expected performance.

4. **Use of IT Devices**: IT devices issued by the Company to a user should be primarily used for official purposes and lawfully and ethically.

5. **E-mail Access from the Company's Network**: E-mail service authorized by the Company should only be used for official correspondence. All incoming SMTP e-mails will be scanned for spam and virus infection. Our Email Security Policy ensures secure email communications by implementing encryption for outgoing emails, training employees to identify and report phishing attempts, employing authentication protocols to verify email authenticity, and enforcing strong password policies. We also utilize third-party tools to protect against various vulnerabilities.

6. **Endpoint Security:** We implement endpoint security solutions such as antivirus software, third-party software updates and patches, and tools to protect against malware and unauthorized access.

7. **Network Security:** Our network infrastructure is secured with firewalls and other measures to prevent unauthorized access and intrusions. We also prioritize regularly updating and patching software and firmware to address known vulnerabilities and protect against cyber threats.

8. **Access to Social Media Sites from the Company's Network:** Use of social networking sites by employees is governed by the IT Department. Users should comply with all applicable provisions under this policy while posting any data about the Company on social networking sites.

9. **Filtering and blocking of sites:** The IT Department may block content over the Internet that is in contravention of this Policy and other applicable laws of the land in force which may pose a security threat to the network.

10. **Security Incident Management Process:** A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality, and authority of data owned by the Company.

a. 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.
b. User should report any suspicious incident as soon as possible to the IT Department.
c. Users should always use high-security settings on social networking sites.
d. User should not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
e. User should not disclose or use any confidential information obtained in their capacity as an employee/contractor of the organization.
f. User should not make any comment or post any material that might otherwise cause damage to the organization's reputation.

Policy Compliance and Dissemination

1. It is the responsibility of all employees to adhere to the Policy, and the management has all right to take disciplinary action and build a corrective action plan in case of its violation.

2. All employees of the organization are necessarily to be aware of this Policy of the organization.

3. Employees while operating from remote/outside organization networks should strictly connect via VPN for accessing Applications and Corporate Networks.

4. All employees should implement appropriate controls to ensure compliance with this Policy by their users.

5. The IT Department will ensure the resolution of all incidents related to the security aspects of this Policy by their users.

Implementation Process and Risk Management

- **Risk Assessment:** The Company conducts risk assessments to identify potential threats, vulnerabilities, and risks to the organization's assets and operations.
- **Risk Mitigation**: The Company implements appropriate controls, safeguards, and countermeasures to mitigate identified risks and minimize their impact on the organization.
- **Incident Response:** The Company develops and maintains an incident response plan/Business continuity plan outlining procedures for detecting, responding to, containing, and recovering from cybersecurity incidents. The Business Continuity plan is tested annually at DSIL.

Reporting

Any questions, concerns, or incidents related to cybersecurity matters shall be promptly reported to the IT Head, Corporate. Employees are encouraged to report any suspicious activities, potential vulnerabilities, or security incidents without delay to ensure timely investigation and remediation.

Remedy

DSIL assures through this Policy that any cybersecurity matters resulting from or caused by the Company's business activities shall be appropriately and adequately remedied in a time-bound manner. Upon detection or notification of a cybersecurity incident, the IT department, in collaboration with relevant stakeholders, shall promptly initiate remediation efforts to contain the incident, mitigate its impact, and restore affected systems and data. Remediation activities may include but are not limited to:

- Isolating affected systems or networks to prevent further spread of the incident.
- Investigating the root cause of the incident to identify vulnerabilities or weaknesses in existing controls.
- Implementing immediate countermeasures or patches to address identified security gaps.
- Restoring data from backups to ensure data integrity and availability.
- Communicating with affected parties, stakeholders, and regulatory authorities as necessary to fulfil reporting and compliance requirements.
- Conducting post-incident analysis and lessons learned sessions to improve future incident response and prevention efforts.
- DSIL is committed to promptly addressing and resolving cybersecurity incidents to minimize disruption to business operations, protect sensitive information, and uphold the trust and confidence of customers, partners, and stakeholders in the Company's cybersecurity posture.

All the issues related to Cyber Security and Data Privacy can be raised via https://www.dwarikesh.com/investers-relation.html

Monitoring Mechanism

DSIL will implement a monitoring mechanism to implement systems, tools, and processes for continuous monitoring of networks, systems, and endpoints to detect and respond to anomalous activities or potential security breaches. DSIL is committed to conducting periodic reviews and evaluations of cybersecurity measures to assess their effectiveness, identify areas for improvement, and ensure compliance with industry standards and regulatory requirements.

Policy Review

This Policy undergoes an annual review to maintain its relevance and effectiveness. Adjustments are made as needed to align with changes in technology, industry standards, regulatory requirements, and emerging cyber threats.

This Policy has been reviewed and approved by the Board of Directors of DSIL.

Issuing Authority: Approved in Board meeting held on 30th April 2024