GANESH BENZOPLAST LIMITED

CYBER SECURITY AND DATA PRIVACY PROTECTION POLICY

GANESH BENZOPLAST LIMITED

CYBER SECURITY AND DATA PRIVACY PROTECTION POLICY

Ganesh Benzoplast Limited (herein referred to as "The Company" or "GBL"), recognizes the 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 along with to ensure compliance with relevant laws, regulations, and industry standards.

Scope

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

THE POLICY STATEMENT

The Policy requires:-

i. To comply with the applicable national and international cyber security standards.
ii. Implementation of control and monitoring measures for all hardware and software assets in use throughout the organization.
iii. Critical information is protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.
iv. To establish clear-cut reporting channels for any form of violation of the Cyber Security and Data Privacy policies
v. To protect GBL stakeholders, information and assets from threats that could potentially disrupt business and brand and reputation.
vi. To communicate the importance of cyber security and to continually enhance information security capabilities to all the concerned.
vii. To collaborate with cyber security and data privacy experts to continually upgrade the information management infrastructure.
viii. All Business Heads/Department Heads are directly responsible for ensuring compliance with this policy in their respective business domains.
ix. All breaches of information security, actual or suspected, are reported, investigated by the designated personnel and appropriate corrective and preventive actions initiated.

IMPLEMENTATION OF POLICY

i. 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.

ii. Data is protected from unauthorized changes or tampering and regular back up of critical data and establish disaster recovery plans to ensure data availability in case of system failures.

iii. IT devices issued by the Company to a user should be primarily used for official purposes and lawfully and ethically.

iv. 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 and all email communications are secured 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.

v. The Company implement endpoint security solutions such as antivirus software and other tools to protect against malware and unauthorized access.

vi. 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.

vii. 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.

viii. 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.

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. 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.

POLICY COMPLIANCE AND DISSEMINATION

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.

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

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 counter measures to mitigate identified risks and minimize their impact on the organization.

REPORTING

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

REMEDY

GBL 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.
- GBL 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.

COMMUNICATION OF POLICY

The Policy shall be communicated to all employees of GBL, under the Section of 'Code of Conduct' Policies. Any changes in the Policy shall be notified through the internal email by way of updated

Policy document and the Policy Awareness shall be conducted regularly through various discussion / communication forums.

AMENDEMENT TO POLICY

GBL's Board of Directors/Committee will monitor the effectiveness and review the implementation of this Policy, and it can amend the terms of this Policy from time to time, as required to align with changes in technology, industry standards, regulatory requirements, and emerging cyber threats.