Borosil Scientific Limited

DATA PRIVACY POLICY

Document Name	Data Privacy Policy
Effective date	November 23, 2023
Approving Authority	Board of Directors
Current Version	Version 1 (V1)
Version History	-
Last Review Date	November 23, 2023

Introduction

This Data Privacy Policy ("Policy") lays down the security objectives and expectations of Borosil Scientific Limited ("Borosil/Company/we/our"), which will help maintain the privacy of and protect the personal information of employees, contractors, vendors, interns, associates, customers and business partners of Borosil Scientific Limited and ensure compliance with laws and regulations as applicable. Borosil is committed to establish and consistently improve cybersecurity processes and minimize exposure to risks.

Scope and Applicability

This Policy applies to Borosil employees, contractors, vendors, interns, associates, customers and business partners who may receive personal information, provide information to the Company, have access to Borosil's information or are involved in management of information systems. The Policy shall also be applicable for all related subsidiaries of Borosil. No Third Party may access personal information held by the organization without having first entered into a confidentiality agreement.

Information Security and Data Privacy Principles

- This Policy is a framework to ensure that our data is comprehensively protected against the consequences of breaches of confidentiality, failures of integrity, interruptions to their availability, loss of authenticity and/or repudiation of an action.
- Applying effective risk management framework to identify, manage and mitigate risks associated with Borosil through undertaking a data vulnerability assessment on a yearly basis.
- Provide stakeholders with notice about how it collects, uses, retains, and discloses personal information about them.
- Provide stakeholders the choice and obtain their consent regarding how it collects, uses, and discloses their personal information.
- Company shall not retain personal information longer than is necessary to fulfil the purposes for which it was collected and to maintain reasonable business records. The Company shall dispose the personal information once it has served its intended purpose or as specified by the stakeholder.
- Company shall disclose personal information to Third Parties / partner firms only for purposes identified in the privacy notice / SoW / contract agreements. Borosil shall disclose personal information in a secure manner, with assurances of protection by those parties, according to the contracts, laws and other segments, and, where needed, with consent of the stakeholder.
- Protect all Borosil information assets from possible threats which could potentially disrupt the business and functioning of Borosil.
- A backup management system for creating copies of information which is essential to recover and restore original data in the event of data loss.
- Consistently improve and upgrade technology, systems, and processes to protect Borosil against known and unknown cybersecurity threats.
- Implement incident management procedures for detecting, reporting, and responding to incidents.
- Provide access to information systems based on least privileged access model and segregation of duties.
- Applying business continuity and disaster recovery management controls.

Compliance

All Borosil employees are required to attend awareness programs on Information Security and Data Privacy with regular trainings made available by the management. Borosil will educate employees upon hiring and conduct at least an annual awareness program through emails, posters, and meetings. Employees are encouraged to report any suspicious activity to the Information Security Team through designated channels. All reported incidents shall be handled in a proper and timely manner with corrective actions being implemented immediately without comprising on the confidentiality, integrity, and availability of information of Borosil.

The Information Security Team regularly conducts violation checks on employees' laptops – including email violation, installation, and the use of prohibited software etc. It is the responsibility of each employee to clearly understand and adhere to the Data Privacy Policy and in case of any violations to this policy, the Management reserves all rights to take disciplinary action, up to and including termination of employment.

Governance

Borosil Head-IT is responsible for overseeing cybersecurity governance as per Borosil's Risk Management Framework. Reports pertaining to cybersecurity risks are to be presented from the Information Security Team to the Head-IT as part of regular reviews with the Board of Directors or it's Committees and Company's management.

The Head-IT is responsible for clearly outlining expectations, providing support in implementing and monitoring progress on safeguarding Borosil information and assets. The Information Security strategy, policy, and cybersecurity programs are to be driven with a top-down approach from the Head-IT to all business units and function heads further down to all the employees. Business units and function heads are responsible for implementing adequate security policies, process, and controls to protect confidentiality, maintain integrity and ensure availability of all information assets.

Policy Review:

The Policy will be reviewed by Risk Management Committee at regular intervals or in case of any significant changes to check for effectiveness, changes in technology and changes in risk levels that may have an impact on confidentiality, integrity and availability, legal and contractual requirements, and business efficiency.