Protection of Company Information and Intellectual Property Policy

Version 1.0

Approval and Effectiveness

This Policy was reviewed and approved by the Board of Directors of Saatvik Green Energy Limited during its meeting held on 11th December 2025. The Policy is effective from the same date and shall remain in force until amended or replaced by the Board/ ESG Council of Saatvik.

1. Prologue

The Saatvik Group of Companies ("Saatvik") is committed to protecting all sensitive and proprietary information, covering its own data and intellectual property ("IP") and that entrusted to us by employees, customers, suppliers, and other business partners. We uphold confidentiality, integrity, availability, and lawful use of information, and we respect third-party IP rights in all operations. We also ensure traceability of information across its lifecycle, maintaining visibility over access, movement, and modifications of sensitive data.

2. Objective

Saatvik Group ("Saatvik") has adopted this Policy in order to protect its own IP and minimize the possibility of infringement of IP rights of Saatvik and third parties. This Policy aims to provide a transparent administrative system for the ownership, control, and transfer of the IP created and owned by Saatvik.

Through this Policy, Saatvik aims to:

2.1 Safeguard company and third-party confidential information and IP from unauthorized access, use, disclosure, alteration, or destruction.

2.2 Ensure responsible, lawful handling of information and IP across their lifecycle.

2.3 Embed simple, risk-based controls, training, and oversight to prevent incidents and enable rapid response when required.

2.4 Saatvik strives to align its information protection framework with recognized international standards such as ISO/IEC 27001, thereby reinforcing its commitment to continual improvement in information security management.

3. Scope of the Policy

This Policy, titled "Protection of Company Information and Intellectual Property Policy" ("Policy"), is applicable across operations of Saatvik Green Energy Limited and its subsidiaries (collectively referred to as the "Saatvik Group" or "Saatvik").

The Policy applies to all employees (including directors, officers, permanent staff, trainees, probationers, and temporary workers), as well as contractors, suppliers, agents, business partners, and any other third parties representing Saatvik directly or indirectly.

4. Policy, Procedure & Guidelines

4.1 Company Information and Intellectual Property

The protection of confidential business information and trade secrets is vital to the interests and success of Saatvik. Examples of Saatvik's confidential information include, but are not limited to, the following:

- Customer lists, financial information, pending projects or proposals, pricing/costing and other employee compensation data; any data or information relating to business information, strategies, list of present or potential clients/customers, equipment, software, designs, marketing plans, pricing information, processes, ideas, inventions (whether patentable or not), schematics and other technical business, models, design, product drawings (such as 2-D drawings or 3-D models) performance specifications, concepts, progress reports and the like employed by us in the operation and development of its business or otherwise.
- Such confidential information may be in writing, or presented electronically, orally, or visually, in readable form, whether on USB flash drives, memory cards, cloud-based media, or in any form whatsoever, and stored in any medium.
- In the course of their work or relationship with Saatvik, employees, contractors and agents may acquire or have access to confidential information, and it is a condition of employment or work that employees, contractors and agents treat this as the property of Company (or relevant customer) and refrain from disclosing it to any unauthorized person(s) under any circumstances without Saatvik's prior written permission.
- Employees, contractors, and agents shall not disclose, part with possession of, or remove confidential information, now or at any time in the future, whether during employment or thereafter at any time, to any person(s) (except to those authorized by Saatvik).
- Employees, contractors and agents are hereby prohibited from using, for their own purpose or for any purpose other than for Saatvik's purposes, any private, confidential or secret information, know-how, writings, records, notes, letters, drawings, plans or any other data belonging to Saatvik,

which may have been obtained or come across by virtue of employment or other relationship with Saatvik.

- Further, all copyrights, works, inventions, trademarks, trade secrets, innovations, improvements, developments, methods, know-how, designs, analyses, drawings, reports, and all similar or related information which relate to the actual or anticipated business, research and development or existing or anticipated future products, processes, or services of Saatvik and which are conceived, developed or made by an employee or contractor in the course of his/her employment/engagement or on Saatvik's time or property, whether acting alone or in conjunction with others are deemed work product or are works "made-for-hire" and belong to Saatvik.
- Individuals are required to promptly disclose all such work product to Saatvik, and perform all actions reasonably requested by Saatvik (whether during the term of employment or thereafter) to establish and confirm such ownership at the Saatvik's expense (including, without limitation, assignments, consents, powers of attorney and other instruments).
- However, inventions that an employee or contractor develops entirely on his/her own time without using Saatvik's equipment, supplies, facilities are generally not subject to this Policy.

4.2 Information Handling and Access Control

- All confidential information must be classified and stored according to its sensitivity.
- Access shall be granted on a strict need-to-know basis and revoked immediately upon role change or separation.
- Company-approved systems, devices, and encrypted channels must be used for creating, storing, or transmitting confidential data.
- Records shall be retained for the required duration and securely destroyed or anonymized once obsolete, ensuring no unauthorized recovery or disclosure.
- Use of personal email, unlicensed software, or external storage devices for company data is prohibited.

4.3 Information Security Risk Assessment

Saatvik shall conduct periodic information security risk assessments to identify and evaluate key risks, vulnerabilities, and controls. The assessment will cover critical assets, potential threats, likelihood and impact of incidents, and mitigation measures. Results shall inform updates to this Policy and related procedures.

4.4 Third-Party Information and Due Diligence

Business partners or vendors handling Saatvik data must sign confidentiality agreements and may be screened for information security and IP-protection controls.

4.5 Training and Awareness

All employees, contractors, and relevant partners will receive periodic training on confidentiality, data handling, and intellectual-property protection. Refresher sessions shall be conducted annually or when major policy changes or incidents occur. Quick reminders and awareness materials may be circulated regularly to reinforce good practices.

Saatvik aims to achieve 100% training coverage for all eligible employees each year by FY 2028.

5. Incident Reporting and Response

Any suspected loss, leak, or misuse of company or third-party information must be reported immediately to the IT/Information Security Head or through the Whistle-blower channel.

Saatvik will take prompt and proportionate corrective action whenever a breach or non-compliance with this Policy is identified.

a. The IT/Information Security Head shall promptly assess the report, contain the issue, and coordinate with relevant teams to prevent further impact.

b. All incidents will be documented, investigated, and resolved through appropriate corrective and preventive actions.

c. Where required, affected stakeholders will be informed, and necessary actions will be taken to strengthen controls and prevent recurrence.

d. Employees, contractors or partners who report a genuine concern or suspected breach in good faith will be protected from any form of retaliation or adverse consequence.

e. Any violation of this Policy will be treated seriously. Employees, contractors, or partners found to be in breach may face disciplinary action, which may include suspension, termination of employment or contract, and, where applicable, legal proceedings under relevant laws. Deliberate misuse of confidential or proprietary information will be considered gross misconduct.

6. Roles and Responsibilities

Saatvik's management is responsible for approving and overseeing the implementation of this Policy and for ensuring that adequate resources are allocated to maintain effective information protection controls. The IT/Information Security Department shall maintain and monitor these controls, coordinate incident responses, and lead periodic training and audits. Department Heads are expected to ensure that all employees within their teams comply with this Policy and that access to sensitive information is granted strictly on a need-to-know basis. Every employee, contractor, and partner must handle company and third-party information responsibly, complete assigned trainings, and promptly report any suspected breaches or misuse of information.

7. Monitoring and Review

Saatvik will regularly monitor and review the effectiveness of this Policy and its related procedures. The IT/Information Security Head shall conduct an annual review covering information-security risks, vendor compliance, incident trends, and training completion rates. Any improvements identified through these reviews will be implemented after management approval, ensuring continuous enhancement of Saatvik's information and intellectual-property protection practices.

8. Review and Amendments

This Policy shall be reviewed annually, or in the event of significant regulatory or operational changes, to ensure its continued alignment with best practices, stakeholder expectations, and legal requirements. Any amendments to this Policy shall be made in writing and will become effective upon approval by ESG Council of Saatvik.

Disclaimer:

This Policy shall be implied in addition to all Saatvik's current and future IT and/or Information Security policies and procedures. The IT/Information Security Department of Saatvik is the final authority in interpreting and deploying the clauses, rules, and procedures mentioned in the Policy. Saatvik reserves the right to modify the Policy from time to time.