MEGHMANI ORGANICS LIMITED

INFORMATION SECURITY POLICY

POL/CIT/001

Version 3.0 | SEPTEMBER-2025

Next Review/ Revision: AUGUST-2028

	Prepared by:	Reviewed By	Approved by
Signature	JRK Khambhati	Dgohel	
Name	Jignesh Khambhati	Dharmendra Gohel	Ankit Patel
Designation	Assistant Manager	Deputy General Manager	Chairman and Managing Director
Date	03-09-2025	03-09-2025	03-09-2025

Registered & Corporate office
1st to 3rd Floor, Meghmani House
B/H. Safal Profitaire,
Corporate Road,
Prahlad Nagar,
Ahmedabad 380015

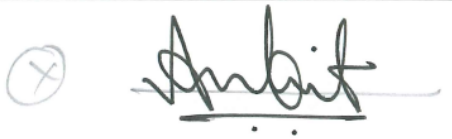
Information Security Policy

Meghmani Organics Limited is commitment to protect the **confidentiality, integrity, and availability** of all information assets—physical, digital, and intellectual—across all locations and business processes.

We recognize information security as a **strategic enabler of trust, operational resilience, and business continuity**. Accordingly, we pledge to:

- Safeguard all sensitive business, employee, and customer data against **unauthorized disclosure, corruption, manipulation, and misuse**.
- Ensure reliable and uninterrupted **availability of critical systems, networks, and data** to support seamless business continuity.
- **Comply with all applicable legal, regulatory, contractual, and industry standards** relating to information security, privacy, and data protection
- Strengthen vendor and supplier relationships through **stringent contractual obligations and assurance mechanisms**, ensuring that third parties handling our information adopt equivalent security standards.
- Provide continuous awareness programs, simulated exercises, and mandatory training for all employees, contractors, and partners.
- Continuously **assess risks, implement controls, and improve resilience** to safeguard our systems against evolving threats
- Implement a proactive **incident response and recovery mechanism**, ensuring rapid detection, containment, and corrective action for all security breaches and cyber threats.
- Ensure business continuity and ensure emergency preparedness through effective backup systems, contingency plans, and controls to protect our information and operations during any disruption
- Embed **continuous monitoring, auditing, and performance reporting** into our information security framework, ensuring measurable accountability and transparency.
- Drive **continuous improvement** of our Information Security Management System (ISMS) by learning from incidents, audits, and industry benchmarks to stay ahead of evolving threats.
- Align our practices with **global frameworks and report security performance in our public disclosures**.

Through this policy, we aspire to be a **secure, resilient, and sustainable organization** that protects its people, systems, and stakeholders, while enabling operational excellence, and long-term value creation. This commitment extends to our employees, contractors, suppliers, customers, and all stakeholders.

	12th Jan' 2025

1. Objective:

The objective of this Information Security Policy is to:

- Establish a structured framework for protecting the confidentiality, integrity, and availability (CIA) of all Meghmani Organics Limited's information assets—digital, physical, and intellectual.
- Support business continuity, operational resilience, and stakeholder trust through robust security practices.
- Ensure compliance with legal, regulatory, contractual, and international standards relating to information security, privacy, and data protection.
- Extend accountability to employees, contractors, suppliers, and third-party partners handling MOL's information assets.
- Align information security practices with our sustainability, ESG, and Responsible Care commitments, ensuring long-term value creation.

2. Policy Statement

Meghmani Organics Limited is commitment to protect the **confidentiality, integrity, and availability** of all information assets—physical, digital, and intellectual—across all locations and business processes. We recognize information security as a **strategic enabler of trust, operational resilience, and business continuity**. Accordingly, we pledge to:

- Safeguard all sensitive business, employee, and customer data against **unauthorized disclosure, corruption, manipulation, and misuse**.
- Ensure reliable and uninterrupted **availability of critical systems, networks, and data** to support seamless business continuity.
- **Comply with all applicable legal, regulatory, contractual, and industry standards** relating to information security, privacy, and data protection
- Strengthen vendor and supplier relationships through **stringent contractual obligations and assurance mechanisms**, ensuring that third parties handling our information adopt equivalent security standards.
- Provide continuous awareness programs, simulated exercises, and mandatory training for all employees, contractors, and partners.
- Continuously **assess risks, implement controls, and improve resilience** to safeguard our systems against evolving threats
- Implement a proactive **incident response and recovery mechanism**, ensuring rapid detection, containment, and corrective action for all security breaches and cyber threats.
- Ensure business continuity and ensure emergency preparedness through effective backup systems, contingency plans, and controls to protect our information and operations during any disruption
- Embed **continuous monitoring, auditing, and performance reporting** into our information security framework, ensuring measurable accountability and transparency.
- Drive **continuous improvement** of our Information Security Management System (ISMS) by learning from incidents, audits, and industry benchmarks to stay ahead of evolving threats.
- Align our practices with **global frameworks and report security performance in our public disclosures**.

Through this policy, we aspire to be a **secure, resilient, and sustainable organization** that protects its people, systems, and stakeholders, while enabling innovation, operational excellence, and long-term value creation.

3. Scope of Policy:

This commitment extends to our employees, contractors, suppliers, customers, and all stakeholders.

4. Governance and Responsibilities

- **Board of Directors / Risk & Audit Committee**: Provide strategic oversight and review policy effectiveness.
- **Chief Information Security Officer (CISO)**: Accountable for ISMS operations, incident management, and compliance reporting.
- **Functional Heads / Site Leadership**: Ensure departmental compliance with security requirements and risk controls.
- **Employees, Contractors, and Partners**: Comply with the policy, report incidents, and safeguard information within their control

5. Guiding Principles

Our information security practices are anchored in the following principles:

- **Confidentiality** – Protect sensitive data against unauthorized access and disclosure.
- **Integrity** – Ensure accuracy, completeness, and protection of data against corruption and misuse.
- **Availability** – Guarantee uninterrupted access to critical systems and information to maintain operations.
- **Compliance** – Adhere to ISO 27001 standards,Indian IT Act, contractual requirements, and global best practices.
- **Awareness & Training** – Build a security-conscious culture through structured training and awareness programs.
- **Supplier & Third-Party Assurance** – Extend security requirements to vendors, contractors, and service providers.
- **Incident Management** – Maintain readiness through detection, response, containment, and recovery plans.
- **Business Continuity & Resilience** – Ensure preparedness via tested contingency and recovery mechanisms.
- **Continuous Improvement** – Regularly audit, monitor, and enhance ISMS to meet evolving risks and stakeholder expectations

6. Monitoring, Reporting, and Continuous Improvement

- Information security performance shall be tracked using key metrics, leading/lagging indicators, and periodic audits.
- Findings from audits, incident investigations, responsible care –security code and other sustainability assessments of customers and EcoVadis assessments shall be reported to top management and integrated into corrective actions.
- A formal management review of the ISMS will be conducted at least annually to ensure adequacy, suitability, and effectiveness.
- Results and improvements will be reflected in sustainability reporting and public disclosures to ensure transparency and accountability

7. Review and Revision History

- This policy shall be reviewed once in three years or whenever significant changes occur in regulatory requirements, business operations, or the threat landscape.
- Updates will incorporate lessons learned from incidents, audits, and benchmarking with global standards.
- The revised policy will be re-approved by the Board / Risk & Audit Committee and communicated across all levels of the organization

SN	Details of revision	Reason for revision
1	Revision-01: 15th Oct 2023, Information security Policy first time developed to initiate journey of Information security management system.	Security Policy developed first time
2	Revision-02 of policy released on 12th June shall be effective from Date: 12th Jan 2025. Next Review Date: 11th Jan 2028	Security Policy revised to align clauses with ISO 27001 standard. Improved commitments towards stakeholders' information protection.
3	Revision-03 of Policy released on 1st September shall be effective from date 1st September 2025. Next Review Date: 31st August 2028.	No change in policy content. Document Numbering system updated and revised number provided to policy