Information Security Policy

Document History

Author	Version History	Reviewer	Approver	Date	Changes
Basant Kati	Ver1.0.0	U N Narayana Maiya	Srinivas Naik	23-07-2024	Initial Draft
Basant Kati	Ver2.0.1	U N Narayana Maiya	Srinivas Naik	29-07-2025	Added Security Awareness Training

Table of Contents

1. Purpose
2. Scope
3. Information Security Objectives
4. Governance and Responsibilities
5. Core Policy Principles
6. Continuous Improvement and Review
7. Compliance and Exceptions
8. Contact

1. Purpose

This Information Security Policy outlines atyati ’s commitment to protecting the confidentiality, integrity, and availability of information assets. Our goal is to secure data against internal and external threats, comply with applicable regulations, and uphold the trust of our clients, partners, and employees in alignment with the ISO/IEC 27001 standard.

2. Scope

This policy applies to all atyati employees, contractors, consultants, and third-party service providers who interact with company information assets, across all systems, platforms, and physical locations.

3. Information Security Objectives

atyati commits to:

- Protecting information from unauthorized access, disclosure, alteration, and destruction.
- Ensuring availability of systems and services to authorized users.
- Complying with legal, contractual, and regulatory requirements.

- Promoting a culture of security awareness across the organization.
- Continually improving our Information Security Management System (ISMS).

4. Governance and Responsibilities

- The Risk and Governance Committee, led by the IT Security Team is responsible for governing the ISMS.
- Employees and contractors are responsible for adhering to security practices, reporting incidents, and participating in training.
- Information security responsibilities are defined and documented for all relevant roles.

5. Core Policy Principles

- Risk Management: Information security risks are identified, assessed, and treated through a formal risk management process.
- Access Control: Access to systems and data is controlled based on business needs and the principle of least privilege.

- Asset Management: All information assets are identified, classified, and managed throughout their lifecycle
- Cryptography & Data Protection: Sensitive data is protected through industry-standard encryption and secure handling procedures.
- Incident Management: Security incidents are promptly reported, recorded, and resolved in accordance with defined response procedures.
- Business Continuity: Controls are in place to ensure the continuity of critical operations during disruptions.
- Supplier Management: Third-party service providers are required to comply with our information security requirements.
- Awareness & Training: All personnel receive regular security awareness training to uphold a secure organizational culture.

6. Continuous Improvement and Review

This policy is reviewed at least annually and updated as necessary to ensure ongoing relevance, effectiveness, and alignment with ISO/IEC 27001 requirements and business objectives.

7. Compliance and Exceptions:

Non-compliance with this policy may result in disciplinary action. Exceptions to the policy must be approved by the VP, Technology with documented justification.

8. Contact

For questions regarding this policy or to report a security concern, please contact:

Email: infosec@atyati.com

Phone: 080-42921999