

Information Security Policy Summary

1. Introduction

- 1.1. This document summarizes Intellicene's **Information Security Policy**, which defines the core principles of its Information Security Management System (ISMS).
- 1.2. The policy, established and approved by company management, demonstrates a commitment to protecting the business and personal information of Intellicene, its employees, and its customers.

2. Background

- 2.1. Intellicene's operations depend on the confidentiality, integrity, availability, and resilience of its information assets.
- 2.2. Information, its management systems, and associated technological infrastructure are critical assets that require robust protection.
- 2.3. Compromised information can result in operational, technological, financial, reputational, and privacy-related damages.
- 2.4. The Information Security Policy is designed to address dynamic security risks and align with operational and organizational needs, forming the foundation for security procedures.
- 2.5. This policy is based on the ISO 27001:2022 Information Security Management Standard.

3. Managerial Commitment to Information Security

- 3.1. Intellicene's management prioritizes data protection.
- 3.2. Management leads all efforts to comply with laws, regulations, and ISO 27001 certification requirements.



- 3.3. Resources are allocated to safeguard the company's information assets and support the ISMS.
- 3.4. Employees must be aware of security risks, take preventive measures, and report incidents to the information security officers.

4. Company Information Security Objectives

- 4.1. Protect sensitive information of customers and employees across systems, facilities, and cloud services.
- 4.2. Ensure IT systems' availability to maintain business continuity and customer service.
- 4.3. Safeguard information integrity to provide reliable results in all business processes.
- 4.4. Protect Intellicene's business information, products, operations, and services.
- 4.5. Maintain confidentiality of employees' personal data.
- 4.6. Comply with mandatory regulations and customer/stakeholder requirements.
- 4.7. Increase information security awareness among employees and managers.
- 4.8. Enhance system resilience and recovery from internal and external threats.

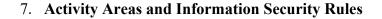
5. Risk Assessment

5.1. The policy emphasizes a risk management approach to identify, mitigate, and prevent security risks to information and systems.

6. Responsibilities

- 6.1. The Information Security Steering Committee defines goals and ensures ISMS implementation.
- 6.2. The Chief Information Security Officer (CISO) manages day-to-day information security activities.
- 6.3. All managers and employees are responsible for maintaining security and confidentiality.





7.1. The policy outlines specific rules for key activity areas, including:

- *Logical Security*: Implementing controls based on information sensitivity and criticality.
- *Physical Security*: Enforcing access controls and a clean desk policy to safeguard information.
- *HR Security*: Mitigating risks related to employee reliability and awareness.
- *Education and Awareness*: Providing security training and raising awareness.
- Secure Development: Integrating security in solution development processes.
- *Cloud Security*: Securing data in cloud environments.
- Supply Chain: Enforcing ISO 27001-aligned security practices with third parties.
- *Backups*: Ensuring reliable and confidential data backups.
- Access Control: Preventing unauthorized access to systems and data.
- *Encryption*: Using encryption to protect data confidentiality and integrity.
- *Remote Access*: Securing remote connections and portable devices.
- Incident Handling: Defining processes to address security incidents.
- *Business Continuity*: Establishing plans to address disruptions.
- *Monitoring*: Implementing continuous security monitoring.
- *Penetration Testing*: Conducting regular vulnerability assessments.
- *Legal Compliance*: Aligning practices with local laws and ISO 27001 standards.

SECURITY. EVOLVED.





8. Expectations from Employees and Contractors

8.1. Executive management requires all employees and contractors, full- or part-time, to actively participate in protecting information assets and fully comply with this policy.

Sincerely,

Aug Cololom

Greg Colaluca General Manager