

Intelligent Innovations N.V.
Groot Kwartierweg 10, Livestrong Building,
Curacao

Information Security Policy

Table of content

General information	2
Introduction	2
Objectives	3
Risk Management	4
Security Controls.....	6
Regulatory Adherence and Governance Structure.....	8
Internal Organisation	9
Human Resource Security.....	9
Asset Management.....	10
Access Control.....	11
Cryptography	12
Physical and Environmental Security.....	13
Communication Security.....	14
Information Security Incident Management	15
Regulatory Compliance and Assurance	16
Version History	17

General information

Document ID:	
Document type:	Policy
Version:	
Version Date:	01/05/2025
Developed by:	
Approved by:	
Owner of the Document:	
Review periodicity:	
Confidentiality level:	For internal use

Introduction

This Information Security Policy outlines a unified and strategic approach to safeguarding digital and physical information assets across Intelligent Innovations (hereafter referred to as “the Company” or “the Organization”). It establishes a framework of administrative, physical, and technical safeguards designed to preserve the **confidentiality**, **integrity**, and **availability** of organizational data.

The objective of this document is to articulate the Company's commitment to data protection and its proactive stance in creating a secure environment for the systems and information entrusted to us. It reflects the value the Company places on security and the investment it makes to mitigate risks across its infrastructure, especially in anticipation of product launch and operational scaling.

Our Information Security approach prioritizes the safeguarding of personal data—particularly that of end users and players—from unauthorized access, misuse, and manipulation. This includes but is not limited to:

- Deployment of encryption and secure access control mechanisms;
- Continuous monitoring for malware and other threats;
- Systematic, automated backups of critical data;
- Implementation of tested disaster recovery and business continuity procedures;
- Controls against internal and external manipulation or sabotage;
- Full traceability and auditability of system activities to maintain system integrity.

The Company has established an Information Security Management System (ISMS) modeled on ISO/IEC 27001 standards. This ISMS is endorsed and actively supported by senior leadership, ensuring that information security is embedded within the organizational culture. Executive management plays a pivotal role by asking the right questions, setting security objectives, and ensuring alignment with both strategic and operational goals.

To uphold transparency and accountability, the ISMS is subjected to **at least one independent audit annually** by certified third-party assessors.

Objectives

The primary goal of this Information Security Policy is to define the essential principles, behaviors, and technical measures necessary to minimize information-related risks and to protect the Company, its partners, clients, and employees from data compromise, service disruptions, and reputational harm.

This document establishes a proactive and structured approach to Information Technology (IT) and Information Security (IS) by ensuring the following objectives are consistently met:

- Minimize IT and security-related risks across systems, infrastructure, and operations.
- Safeguard company, client, and employee data from unauthorized access, misuse, or disclosure.
- Preserve the confidentiality of sensitive and proprietary information.
- Ensure the accuracy and consistency (integrity) of all information processed or stored.
- Comply with applicable legal, regulatory, and contractual requirements, including data protection and industry-specific mandates.
- Maintain and regularly test business continuity and disaster recovery plans to ensure operational resilience.

- Promote a strong security culture and awareness across all levels of the organization.
- Enforce the reporting, investigation, and remediation of all security incidents, including suspected breaches and vulnerabilities.
- Protect intellectual property rights, including copyrights and licensed software.
- Mitigate threats from malware, ransomware, and other malicious code through technical defenses and vigilant monitoring.
- Fulfill professional and contractual obligations to clients, partners, and stakeholders by maintaining trust and compliance.
- Continuously improve the maturity of the information security program, including its governance, documentation, and controls.
- Implement risk-based decision making to prioritize and manage security threats efficiently and effectively.

Together, these objectives form the foundation of the Company's security posture and support its commitment to protecting information assets in a rapidly evolving digital landscape.

Risk Management

Proactive risk management is a cornerstone of the Company's information security strategy. By identifying, assessing, and mitigating risks before they materialize, the Company reduces its exposure to cyber threats and operational disruptions. In an environment where advanced persistent threats are increasingly common, our approach combines technology, threat intelligence, and user education to manage risk in real time.

Understanding adversary tactics—such as denial-of-service attacks, phishing campaigns, and social engineering—is key to developing resilient defenses. Moreover, employee awareness remains one of the most effective ways to mitigate threats targeting human vulnerabilities.

Risk Management Objectives

The Company is committed to:

- Establishing and maintaining an **information security risk management process** aligned with the ISO/IEC 27001 standard.
- Conducting **systematic and repeatable risk assessments** that evaluate the potential impact of threats and vulnerabilities on the organization.
- Designing and implementing a **comprehensive suite of security controls** to mitigate architectural and operational risks.
- Integrating risk management into an overarching governance framework that ensures controls remain effective and responsive to the Company's evolving threat landscape.

Requirements of the Risk Assessment Process

The information security risk assessment must:

- Define and maintain clear **risk criteria**, including:
 - Risk acceptance thresholds.
 - Standards for consistent and objective risk assessment.
- Ensure **repeatability and validity** of assessments, allowing for consistent and comparable results over time.
- Identify security risks within the ISMS scope by:
 - Evaluating risks that threaten the **confidentiality, integrity, and availability** of information assets.
 - Clearly **assigning ownership** of each identified risk.
- Analyze each risk by:
 - Estimating the **impact** if the risk were to materialize.
 - Determining the **likelihood** of occurrence.
 - Calculating the **risk level** using a standardized scoring model.

- Evaluate risks by:
 - Comparing assessed risks to predefined acceptance criteria.
 - **Prioritizing risks** for treatment based on severity and likelihood.

Risk Treatment

Following the risk assessment, the Company applies a formal risk treatment process to select and implement appropriate mitigation strategies. Treatment options may include:

- **Mitigating** the risk through security controls.
- **Transferring** the risk (e.g., through insurance or third-party arrangements).
- **Avoiding** the risk by altering activities or processes.
- **Accepting** the risk, with justification and approval from the designated **risk owner**.

A formal **Risk Treatment Plan** is created for each significant risk, assigning responsibility for implementation and monitoring. Risk owners, or their delegates, are responsible for executing mitigation measures and deciding whether to accept any residual risk.

The information security policies are reviewed no less than annually or upon significant changes to the information security environment.

Security Controls

Effective protection of organizational data relies on the implementation of robust technical, administrative, and physical security controls. The Company's Information Security Management System (ISMS) is designed to incorporate a comprehensive set of safeguards that align with ISO/IEC 27001 and industry best practices.

These controls are structured into functional domains to ensure coverage across all areas of potential risk. Each domain contains specific policies, procedures, and technical mechanisms tailored to the Company's operational environment.

Categories of Security Controls

1. Information Security Policies

Foundational policies define the overall approach to information security and provide governance for the implementation of control measures across the organization.

2. Organization of Information Security

Responsibilities and reporting lines are clearly defined. Information security is embedded at all levels of the organization, supported by management and enforced through dedicated roles and committees.

3. Human Resource Security

Security responsibilities are addressed at all stages of employment—from recruitment to termination. Staff receive training and are expected to uphold the organization's security posture.

4. Asset Management

All information assets—including data, hardware, and software—are inventoried and classified. Ownership is assigned, and controls are in place to protect assets throughout their lifecycle.

5. Access Control

Access to information and systems is restricted based on the principle of least privilege. Multi-factor authentication, role-based permissions, and regular access reviews are used to enforce this control.

6. Cryptography

Encryption is used to protect data at rest and in transit. Secure key management practices are implemented to ensure that cryptographic assets are adequately protected.

7. Physical and Environmental Security

Critical systems and information are housed in secure facilities with controlled access. Environmental controls protect against fire, flood, and unauthorized entry.

8. Communication Security

Network infrastructure is protected through firewalls, intrusion detection/prevention systems (IDS/IPS), and segmentation. Data exchanged internally or externally is secured using approved protocols and encryption.

9. Information Security Incident Management

A formal incident response framework ensures that security incidents are identified, reported, analyzed, and resolved in a timely and controlled manner. Lessons learned are documented and integrated into future defenses.

10. Compliance

The Company ensures compliance with applicable laws, regulations, and contractual obligations. This includes regular internal audits, third-party assessments, and adherence to privacy legislation such as the GDPR.

Regulatory Adherence and Governance Structure

The structure for regulatory adherence and governance within the Company is built upon its Information Security Policies, which are central to the Information Security Management System (ISMS) and benchmarked against the ISO/IEC 27001:2013 standard. These policies clearly stipulate the required conduct, assigned duties, and specific control mechanisms applicable to all employees, contractors, and external collaborators.

Policies are reviewed at least annually and updated as needed to reflect evolving threats and industry standards. Based on the ISO 27000-series framework, our policies ensure clarity, enforceability, and consistent training across the organization. Mandatory onboarding and annual training reinforce awareness and accountability for all stakeholders.

Internal Organisation

The Company maintains a clear internal structure for managing information security responsibilities:

- **Information Security Officer (ISO):** Oversees the development and maintenance of information security policies, advises on their implementation, supports secure project management, and acts as the liaison with security interest groups.

- **Management:** Ensures the enforcement of information security policies and international standards within their areas of responsibility. They are accountable for raising awareness, ensuring compliance, and maintaining appropriate engagement with external authorities.

- **Employees, Contractors, and Third Parties:**

All personnel must:

- Act ethically and responsibly in all system interactions.
- Avoid misuse of data or exploiting system vulnerabilities.
- Protect sensitive information and seek guidance when classification is unclear.
- Report suspected breaches, weaknesses, or violations promptly to security personnel or line management.
- Adhere to the Company's Incident Management Policy in the event of a security incident.

Human Resource Security

Human resource practices play a vital role in maintaining a secure environment by embedding security responsibilities throughout the employee and contractor lifecycle.

- **Pre-Employment:**

All candidates for employment, contractual roles, or third-party access must undergo

appropriate background checks (screening) in accordance with local laws and Company policy.

- **During Employment:**

Security responsibilities are defined in employment contracts and reinforced through mandatory onboarding and periodic training. Employees are expected to act in alignment with the Company's values and security protocols.

- **Post-Employment or Contract Termination:**

Exit procedures ensure access rights are revoked, company assets are returned, and confidentiality obligations continue to be upheld.

The Company is committed to hiring qualified individuals who support its mission and contribute to a secure and trustworthy user experience.

Asset Management

The Company maintains a structured approach to managing information assets to ensure their confidentiality, integrity, and availability.

- **Asset Identification and Inventory:**

All information assets—including hardware, software, data, and media—must be identified, classified, and recorded in an up-to-date asset inventory. Each asset is assigned an owner responsible for its proper use and protection.

- **Classification of Information:**

A formal data classification scheme is applied to categorize information based on its sensitivity and criticality. This classification guides the handling, storage, and access of data to prevent misuse, loss, or unauthorized disclosure.

- **Media Handling and Protection:**

Procedures are in place to prevent the unauthorized access, modification, or destruction of information stored on physical or electronic media. Special attention is given to the secure disposal and transfer of media.

- **Use of Portable Devices and Media:**

Personal or sensitive data must never be stored in an unencrypted or unprotected format on portable devices such as USB drives, laptops, or external storage.

Access Control

Access control is a critical component of the Company's information security framework and must be considered during the planning and design of all new or significantly modified systems and services.

Key Principles

To protect against internal and external threats, access control designs follow these core principles:

- **Defence in Depth:**

Access security is built using multiple, overlapping controls to reduce reliance on any single mechanism.

- **Least Privilege:**

Users are granted only the minimum level of access necessary to perform their job functions.

- **Need to Know:**

Access to information is restricted strictly to what is essential for an individual's responsibilities.

- **Need to Use:**

Physical and logical access is provided only where operationally necessary.

Access Management Practices

Formal access management policies and procedures are established to:

- Define access requirements and roles during the design of systems and services.
- Control user access through identity verification, role-based permissions, and authentication mechanisms.
- Ensure access rights are reviewed regularly and revoked promptly upon role changes or departures.

These controls help ensure that access to Company resources remains secure, traceable, and aligned with business needs

Cryptography

The Company applies encryption to safeguard sensitive data throughout its lifecycle—during storage, transmission, access, and backup. Encryption practices are governed to ensure data remains accessible to authorized personnel for business continuity and investigative purposes.

General Encryption Requirements

Encryption standards must define:

- Approved algorithms and key lengths appropriate to data sensitivity.
- Full key lifecycle management, including secure generation, storage, distribution, rotation, and destruction.
- Mechanisms to ensure authorized access to encrypted data when required.

Data at Rest

- Sensitive data on mobile devices, file servers, and publicly accessible systems must be encrypted.

- Payment card information stored in databases must be encrypted using strong cryptographic methods.

Data in Transit

- Unencrypted transmission is permitted only within secure, non-public internal network segments.
- VPN or SSH with strong cryptography is required for transmitting sensitive data between remote systems.
- Remote access to internal systems must use VPN with preferred authentication via X.509 certificates and public keys.

Web Services Protection

- All public-facing web interfaces must use HTTPS with TLS v1.2 or higher.
- Mutual SSL authentication is preferred for all web servers.
- Web server certificates must be issued by a trusted internal or third-party Certificate Authority and have a maximum validity of two years.

Backup Data Protection

- All system backups must be encrypted during transfer and while stored offsite.
- Only encryption-capable solutions are approved for Company data backup.

Physical and Environmental Security

The Company enforces physical security controls to prevent unauthorized access, damage, or interference to its information assets and processing facilities.

Physical Security Measures

- **Security Perimeters:** Clearly defined and constructed based on the sensitivity of assets and risk assessments.
- **Access Controls:** Secure areas are protected by entry systems that allow access only to authorized personnel.
- **Barriers and Isolation:** Physical barriers and access points (e.g., loading docks, delivery areas) are controlled and separated from critical systems.
- **Visual and Acoustic Protection:** Office and facility layouts are designed to prevent confidential information from being visible or audible from outside.
- **Environmental Resilience:** Facilities are safeguarded against natural disasters, malicious actions, and accidents through appropriate physical protections.
- **Secure Operations:** Procedures for working within secure areas are defined, enforced, and regularly reviewed.

These measures are integral to safeguarding the Company's infrastructure and ensuring continuity of operations.

Communication Security

- The Company is committed to securing its network infrastructure to protect information as it is transmitted across systems and applications.
- All communication and network controls are designed based on:
 - **Business requirements and risk assessments**
 - **Data classification levels**
 - **Operational needs and segregation requirements**
- Appropriate technical measures are implemented to prevent unauthorized access, ensure data integrity during transmission, and maintain the confidentiality of sensitive communications. This includes the use of firewalls, encrypted protocols, secure gateways, and controlled remote access.

- Network security is continuously monitored and adjusted to align with evolving threats and organizational changes.

Information Security Incident Management

The Company recognizes that security incidents are inevitable and must be managed promptly and effectively.

A **security incident** includes any deviation from expected behavior—whether related to systems, applications, operations, or human actions.

All personnel, including contractors and third parties, are responsible for reporting actual, suspected, or potential incidents immediately.

A formal incident response process is in place to **log, assess, classify, contain, and resolve** incidents efficiently. Streamlined procedures and continuous communication enable faster response, even outside of business hours, minimizing potential damage.

Incident management stages:

- Preparation
- Identification and investigation
- Containment
- Eradication
- Recovery
- Lessons Learned

All security incidents within a Company should be classified. The next levels are used for security incident classification:

- Low
- Medium
- High

- Critical

Appropriate incident management policies and procedures should be created and set out how to prevent incidents or notify responsible personnel of an incident that has already occurred, ongoing or even suspicion of a possible incident.

Regulatory Compliance and Assurance

The Company upholds a meticulously designed, risk-centric compliance architecture to guarantee the confidentiality, availability, and integrity of all information assets under its stewardship—whether stored, processed, or transmitted. Acknowledging the diverse and evolving nature of cybersecurity mandates across industries and legal territories, our compliance initiative is inherently adaptive, consistently updated to reflect the shifting threat environment and prevailing regulatory benchmarks.

Adherence to internationally recognized frameworks — such as ISO/IEC 27001—and relevant legal obligations forms the foundation of our approach. In particular, the Company places emphasis on meeting the requirements of other applicable national and international mandates.

Compliance Management Principles

- Dedicated **IT and ISMS** personnel receive ongoing training in all pertinent regulatory obligations and industry-specific security standards to ensure proficient compliance management.
- A **comprehensive risk assessment plan** supports compliance efforts.
- **Security controls** are clearly defined, implemented, and regularly evaluated.
- **Security policies** undergo routine reviews and updates.
- **All employees** are made aware of their responsibilities for safeguarding information.

Monitoring and Review

- Information systems and related processes are regularly audited to verify alignment with internal policies and external requirements.
- Independent reviews are conducted periodically or following major changes to validate the effectiveness of control objectives, policies, and procedures.
- Both internal and third-party audits are used to demonstrate regulatory compliance and continually strengthen cybersecurity posture.

This ongoing review process ensures that the Company remains aligned with best practices while satisfying its legal and contractual obligations.

Version History

Version	Modified Date	Reason/Comments
1.0		Initial creation