Information Security Policy

Version:	**1.5**
Date of version:	13/10/2024

1. General

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for information security management.

This Policy applies to the entire Information Security Management System (ISMS), as defined in the Information security system.

2. Goal

The purpose and objective of this Information Security Policy are to set out a framework for the protection of the organization's information assets:

- To protect the organization's information from all threats, whether internal or external, deliberate or accidental,
- to enable secure information sharing,
- to encourage consistent and professional use of information,
- to ensure that everyone is clear about their roles in using and protecting information
- to ensure business continuity and minimize business damage,
- to protect the organization from legal liability and the inappropriate use of information.

3. Definitions

Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

Integrity – characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

Availability – characteristic of the information by which it can be accessed by authorized persons when it is needed.

Information security – preservation of confidentiality, integrity, and availability of information.

Information security management system (ISMS) – part of overall management processes that take care of planning, implementing, maintaining, reviewing, and improving information security.

Asset - Anything that has value to the organization, including data, devices, or other components of the environment that supports information-related activities.
Compliance - Ensuring that a standard or set of guidelines is followed, or that proper, consistent accounting or other practices are being employed.

Control - Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

Threat - A threat is anything that might exploit a vulnerability. Any potential cause of an incident can be considered a threat. For example, a fire is a threat that could exploit the vulnerability of flammable floor coverings. This term is commonly used in information security management and IT service continuity management but also applies to other areas such as problem and availability management.

Vulnerability - A weakness that could be exploited by a threat – for example, an open firewall port, a password that is never changed, or a flammable carpet. A missing control is also considered a vulnerability.

4. Roles & Responsibilities

The security of information will be managed within an approved framework through assigning roles and coordinating implementation of this security policy across the organization and in its dealings with third parties.

Specialist external advice will be drawn upon where necessary to maintain the Information Security Policy, processes, and procedures to address new and emerging threats and standards.

The CEO is the designated owner of the Information Security Policy and is responsible for the maintenance and review of the Information Security Policy, processes, and procedures.

All staff and employees of the organization, contractual third parties, and agents of the organization accessing the organization's information are required to adhere to the Information Security Policy, processes, and procedures.

All employees are required to review the Information Security Policy, Privacy Policy, and other internal documents on an annual basis and electronically affirm their agreement to follow all policies and procedures.

5. Company policies

5.1. ISMS policy

The company conducts the Information Security Management System in accordance with the requirements of ISO 27001 to comply with the requirements of the management, customers, laws, and regulations as well as accepted standards in the market and providing customers with reliable and dependable service.

The company will perform the work while complying with the rules and requirements of customers as well as data security regulatory standards.

The company recognizes the need to implement security mechanisms and information security in its sphere of activity.

The company management will strive to prevent embezzlement or fraud by employees or anyone with a business relationship with the company.

The company will always conduct a dynamic system of risk management in the information security field and act to reduce the risks in accordance with the development of the activity. Risk will be managed by setting clear severity criteria for comparing various risks.

The company will take all appropriate steps to maintain the confidentiality, integrity, and availability of data and prevent its information and that of the customer from reaching unauthorized parties and or even beyond.

To comply with the requirements of the information security management system, the Company will set goals in the areas of human resources, availability, and confidentiality

The company will raise the awareness of its own employees and agents regarding all aspects of information security and ensure that all related information transferred by the company employees will be kept confidential without them fearing disciplinary or other action by the company.

The company management will create an infrastructure for business continuity in case of an unusual event or failure that would prevent the company from operating or providing quality, reliable service.

The company management will review and strengthen the policy once a year as part of the company management review and after information security events.

5.2. Asset Management

The organization’s assets will be appropriately protected.

All assets (data, information, software, computer and communications equipment, service utilities and people) will be accounted for and have an owner.

Data assets will be classified as follows and appropriate controls put in place:

- Public: Information is not confidential and can be made public without any implications for the company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.
- Internal use: Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence the company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.
- Restricted: Information collected and used by the company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.

- Client Confidential Data: Information received from clients in any form for processing in production by the company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.
- Personal Data: Any information relating to an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.

5.3. Human Resources Security

The organization's security policies will be communicated to all employees, contractors and third parties to ensure that they understand their responsibilities.
In the event of employee violation of the organization's security policies, disciplinary action will be taken.

5.4. Security Awareness Training

New employees will be trained in information security awareness. Security awareness refresher training must be repeated on an annual basis.

5.5. Encryption in Transit and at Rest

The company ensures the security and privacy of user information by encrypting data while it's stored and transmitted.

Our systems are designed to ensure data is always protected. Specifically, we're using TLS v1.2 with strong ciphers to protect data in transit and AES-256 to protect data while at-rest.

The company's cloud-based solution is deployed using two major clouds, enabling us to guarantee high security through utilizing a series of high tech, best in the industry solutions that work to ensure the safety of all user data on the network.

Also, the company encrypts all personal data that is kept for development and testing purposes. Key management of this encryption will be done by registering the password in a restricted location and access to employees who use the information

5.6. Physical and Environmental Security

Confidential or proprietary information processing facilities will be housed in secure areas.

The secure areas will be protected by defined security perimeters with appropriate security barriers, entry controls, and environmental controls.

Confidential and proprietary information will be physically protected from unauthorized access, damage, and interference.

The company has selected industry-leading IaaS providers, such as AWS, AZURE and GCP. Please refer to their White Paper for additional information.

5.7. Communications and Operations Management

Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities will be established.

Appropriate operating procedures will be put in place.

Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

A formal Change Management policy will be established, including documentation of all changes, assignment of ownership for each change, and emergency change procedures.

Operational and production environments will be logically separated to reduce the risks of unauthorized access or changes to the operational system.

Monitoring, including audit logging, will be put into place wherever possible to detect potential unauthorized access and other information security violations.

5.8. Access Control

Access to all information will be controlled.

Access to information and information systems will be driven by business requirements. Access will be granted, or arrangements made for employees, partners, suppliers according to their role, only to a level that will allow them to carry out their duties. The principle of least privilege will be applied in all cases.

Formal user registration and de-registration procedure will be implemented for access to all information systems and services.

In the event of employee termination or role change, access to information resources will be revoked or updated within 24 hours. Human Resources will be responsible for collecting any physical assets from the employee.

User access will be reviewed by the director of information security every six months in conjunction with each department head to ensure access levels remain appropriate.

5.9. Information Security Incident Management

Information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner. Appropriate corrective action will be taken.

Formal incident reporting and escalation will be implemented.

All employees, contractors and third-party users will be made aware of the procedures for reporting the different types of a security incident, or vulnerability that might have an impact on the security of the organization's assets as part of the company Information Security Awareness Program.

Information security incidents and vulnerabilities will be reported as quickly as possible to the company Information Security team.

5.10. Business Continuity Management

The organization will put in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A business continuity management process will be implemented to minimize the impact on the organization and recover from the loss of information assets. Critical business processes will be identified.

Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability for both the company and its customers.

5.11. Third Party & Subcontractor Security

All subcontractors and third parties are required to adhere to the Information Security Policy, processes, and procedures.

The director of information security will be responsible for evaluating the security controls and policies of all third-party vendors. Security controls will be re-evaluated upon each contract renewal.

Information security requirements and obligations will be included in third-party contracts and subcontractor agreements.

5.12. Compliance

The organization will abide by any law, statutory, regulatory or contractual obligations affecting its information systems.

The design, operation, use, and management of information systems will comply with all statutory, regulatory and contractual security requirements.

The requirements of the Information Security Policy, processes, and procedures will be incorporated into the organization’s operational procedures and contractual arrangements.

5.13. Clean desk policy

Every user will be responsible for preventing any external and/or internal party who comes to his desk from having access to information that is not relevant to that party.

Every user will be responsible for ensuring the implementation of all the work processes and procedures in use at the company concerning everything connected with the transfer/exposure/release of information to external parties (clients, suppliers, etc.) and internal parties alike.

Every user will be responsible for ensuring that a document that reaches him and is not relevant to his department will be returned to its owner.

Every user will be responsible for ensuring that his access passwords are not stored in his work environment.

Every user will be responsible for ensuring that sensitive information that he is handling will not reach the public domain.

5.14. Teleworking

Access to the production environment: Access is provided only to the infrastructure team through a dedicated VPN connection. Connection to the office via VPN or Point-to-Point.

Access to the system: access will be made through encrypted communications. Remote access will be via computers and not smartphones. There is no limit to remote work in relation to location and / or hours of operation.

5.15. Information transfer

Information transferred to and from the client in the system will be encrypted.

The transfer of the company’s business information must be documented by the transferring party {email is sufficient documentation}.

5.16. Mobile device

The devices will be locked with a password or biometric lock

Mailboxes that will be set on the device can be erased remotely.