INFORMATION SECURITY AND CYBERSECURITY POLICY

iTeam

making a difference

SUMMARY

1 Objective

This document, supported by **iT.EAM** 's senior management, aims to define secure information security and cybersecurity processes through the adoption of standards, business requirements and risk management, allowing employees and other stakeholders to follow a standard of behavior related to information protection and cybersecurity. We are committed, through compliance with the four pillars of information security — confidentiality, integrity, availability and compliance — to meeting the needs of our customers and our market, in addition to ensuring that our image as a supplier of high-quality products and services is maintained and continually improved.
iT.EAM is an information technology and security company located in Prinses Margrietplantsoen 33, 2595 AM Den Haag, Netherlands and is based on the adoption of best information security practices and adoption of applicable legislation.

2 Terms and Definitions

- **Availability:** Systems and data must be available so that when the user needs them, they can use them.

- **Integrity:** Systems and data must always be intact and in a usable condition; Property of safeguarding the accuracy and completeness of assets.

- **Confidentiality:** Private data must be presented only to the owners or to people or groups authorized by them; Property that the information is not available or revealed to unauthorized individuals, entities or processes.

- **Authenticity:** Systems and data must be able to verify the identity of users, and the user must be able to analyze the identity of the system; Property that an entity is what it claims to be.

- **Cybersecurity:** Set of practices, technologies and processes designed to protect systems, networks and data against cyberattacks, unauthorized access, damage or theft.

- **Effectiveness:** Extent to which planned activities are carried out and planned results achieved.

- **Efficiency:** Relationship between the result achieved and the resources used.

- **Supplier:** Any organization that provides goods and services. The use of these goods and services can occur at any stage of the design, production, and use of the products. Thus, suppliers can include distributors, resellers, third-party service providers, transporters, contractors, and franchises, as well as those who supply the organization with materials and components. Suppliers also include providers of health care, training, and education services.

- **Stakeholders:** An individual or group of individuals with a common interest in the performance of the organization and the environment in which it operates. Most organizations have the following stakeholders: customers, workforce, owners, suppliers, business partners, and society. The number and names of stakeholders may vary depending on the profile of the organization.

- **Product:** Result of activities or processes. Consider that:

    - The term product may include services, materials and equipment, information or a combination of these elements;
    - A product can be tangible (such as equipment or materials) or intangible (such as knowledge or concepts), or a combination of the two; and
    - A product may be intentional (e.g., offered to customers), or unintentional (e.g., a pollutant or undesirable effects).

- **Quality:** Degree to which a set of inherent characteristics (activity or a process, a product, an organization or a combination of these), satisfies the explicit and implicit requirements of customers.

- **Requirement:** A need or expectation that is expressed, generally, implicitly or obligatorily.

- **Compliance:** Meeting a requirement.

- **Non-conformity:** Failure to meet a requirement.

- **Information security and privacy management:** Set of interrelated or interactive elements to control and direct an organization with regard to information security and personal data protection.

- **Materials and Services:** Materials or services that impact product quality.

- **Indeterminate:** That which is not defined. The retention period for our SGPI records that are defined as indeterminate due to their archiving in electronic media.

- **Project:** Means the design of a solution, system or product.

- **Access Control:** Means to ensure that access to assets is authorized and restricted based on security and business requirements.

- **Indeterminate:** That which is not defined. The retention period for our SGPI records that are defined as indeterminate due to their archiving in electronic media.

- **Project:** Means the design of a solution, system or product.

- **Access control:** Means to ensure that access to assets is authorized and restricted based on security and business requirements.

- **Accountability:** Responsibility of an entity for its actions and decisions.

- **Information Asset:** Anything that adds value to the organization.

  NOTE: There are several types of assets, including:

  a) information;
  b) software, such as a computer program;
  c) physical, such as the computer;
  d) services;
  e) people and their qualifications, skills and experience; and
  f) intangibles, such as reputation and image.

- **Attack:** An attempt to destroy, expose, alter, disable, steal, or otherwise gain unauthorized access to or make unauthorized use of an asset.

- **Availability:** The property of being accessible and usable on demand by an authorized entity.

- **Business continuity:** Process and/or procedure to ensure continued business operations.

- **Control:** Means of risk management, including policies, procedures, guides, practices or organizational structures, which may be administrative, technical, management or legal in nature.

- **Control objective:** Statement describing what is to be achieved as a result of implementing controls.

- **Corrective Action:** Action to eliminate the cause of an identified nonconformity or other undesirable situation.

- **Effectiveness:** Extent to which planned activities are carried out and planned results achieved.

- **Efficiency:** Relationship between the result achieved and the resources used.

- **Event:** Occurrence of a certain set of circumstances.

- **Guide:** Recommendation of what should be done to achieve an objective.
- **Impact:** Adverse change to the level of business objectives achieved.
- **Information asset:** Knowledge or data that has value to the organization.
- **Information security:** Preservation of confidentiality, integrity and availability of information;

  Note: Additionally, other properties such as authenticity, accountability, non-repudiation and reliability may also be involved.

- **Information security event:** An identified occurrence of a system, service or network state, indicating a possible violation of information security policy or failure of controls, or a previously unknown situation, which may be relevant to information security.

- **Information security incident:** A single or series of unwanted or unexpected information security events that have a high probability of compromising business operations and threatening information security.

- **Information Security Risk :** The potential that a threat will exploit a vulnerability in an asset or group of assets and thereby cause harm to the organization.

- **Management system:** Structure of policies, procedures, guides and associated resources to achieve the organization's objectives.

- **Non-repudiation:** The ability to prove the occurrence of an alleged event or action and its originating entities in order to resolve disputes about the occurrence or non-occurrence of an event or action and the involvement of entities in the event.

- **Policy:** Intent and direction as formally expressed by top management.

- **Procedure:** A specified way of performing an activity or process.

- **Process:** Set of interrelated or interactive activities that transform inputs into products (outputs).

- **Record:** Document that presents results obtained or provides evidence of activities carried out.

- **Reliability:** Properties of consistent desired behavior and results.

- **Vulnerability** : Weakness in an asset or control that can be exploited by a threat.

- **Threat :** Potential cause of an unwanted incident, which may result in damage to a system or organization.

- **Risk:** Combination of the probability of an event and its consequences.

- **Risk assessment:** The entire process of risk analysis and risk evaluation. Process of comparing the estimated risk with predefined risk criteria to determine the significance of the risk.

- **Risk analysis:** Systematic use of information to identify sources and estimate risk.

- **Risk Communication:** Exchange or sharing of information about risks between the decision maker and other stakeholders.
- **Risk criteria:** Terms of reference by which the significance of the risk is assessed.

- **Risk estimation:** Activity to assign values to the probability and consequences of a risk.

- **Risk management: :** Coordinated activities to direct and control an organization with regard to risks.

- **Risk acceptance:** Decision to accept a risk

- **Residual risk:** Remaining risk after risk treatment.

- **Risk treatment:** Process of selecting and implementing measures to modify a risk.

  Note: In this International Standard the term "control" is used as a synonym for "measurement".

- **Threat:** Potential cause of an unwanted incident, which could result in damage to a system or organization.

- **Mitigation:** Limiting the negative consequences of a given event.

3 Scope

Leadership

The leaders of our organization are responsible for knowing and applying the security policies defined in the organization, ensuring full involvement in the purpose of achieving the organization's security objectives.

People involvement

It is the responsibility of all levels of our employees to know and comply with the organization's policies by getting involved in issues related to security, allowing their skills to be used to guarantee and continuously improve the organization's processes.

Processes and continuous improvement

It is the responsibility of senior management, management representatives and the security team to be constantly alert to the procedures and processes established within the organization. These must be regularly reviewed and improved, ensuring the effectiveness of the established policies.

External relationships

It is our company's responsibility to ensure our policies are followed in internal matters and in external relationships when our customers, suppliers and other interested parties do not have their own information security policy. When a customer or supplier presents us with a policy that is different from ours, the management representative together with the information security team must evaluate whether the new policy affects our security in any way and has the freedom to adopt the third-party policy in this relationship.

4 Guidelines

4.1. General

Information is knowledge or data that has value to a company's business. This information can be stored in any format and must therefore be adequately protected. Information comes in many forms and, regardless of the form in which it is presented or the means by which it is shared or stored, it must be used only for the purpose for which it was authorized.

The Information Security Policy's main guideline is to protect information from various types of threats, access, destruction, disclosure or unauthorized modification, to ensure business continuity by minimizing damage and maximizing return on investment and business opportunities .

4.2. Information Asset Management

Assets associated with information and information processing resources are classified, identified and inventoried.

For each information asset, an owner is defined who is responsible for ensuring that it is used in accordance with the company's security policy.

Guidelines for the proper use of assets are provided during the hiring process. Specific assets are handled by a qualified professional responsible for their handling, ensuring proper use.

4.3. Access Control

Access control is one of the mechanisms used to physically and logically protect the IT environment. Access to IT assets must be allowed only to authorized persons in accordance with the items of this Information Security and Cybersecurity Policy.

The right to use the assets is controlled and transferred at the time of contracting and ceases when the relationship with the company ends, at which point the physical assets are collected.

If the contractor needs access to a specific corporate system, this will be provided via authorization from the information manager involved.

4.4. Physical Access Control

Employee entrance

Access to information, equipment, documents and secure areas are properly controlled so that only authorized people have access to these resources.

The identification of employees at the company's facilities is controlled by a security device that guarantees access only to authorized personnel.

Within the facilities, employees have access to common areas, restricted areas are controlled by key and access is permitted via authorization from the person in charge.

Dismissed employees may only enter the company if accompanied by a responsible employee.

Visitors' entrance

There are no time restrictions for visitor service, however access to visitors without the proper accompaniment of a responsible employee is restricted.

Visitors must go through the security procedures carried out by the condominium's reception desk and, during the visit to iT.EAM's facilities, they will be received and accompanied by a company representative. At the end of the visit, they will be accompanied until they leave the company's facilities. During the entire period that visitors are on iT.EAM's facilities, they must always be accompanied by a company employee, except for private areas such as restrooms.

Supplier input

Suppliers must access iT.EAM by requesting service from the supplier.

A responsible employee must monitor the supplier's activities while they are on the company's premises. Except for activities carried out outside business hours,

provided that they are duly formalized and authorized by the responsible employee.
The service provider must carry identification capable of certifying that he or she is the person hired for the service.

Clean Table

Our employees must adopt the practice that no confidential information should be left in view, whether on paper or written down in a visible or accessible place. Special attention must also be paid when using collective printers, collecting the printed document immediately.

Delivery and loading areas

Products purchased by the organization must be received and delivered in secure locations without compromising the information security and operations of the organization. In any case, personnel must be identified and accompanied by an iT.EAM employee at all times while on our premises.

4.5. Logical Access Control

Access in the Contracting Process

During the hiring process, our employees receive the necessary release of logical access to the information assets necessary for their activities.
The employee will receive access to information assets, such as networks and systems, and must be responsible for the confidentiality of the information received. No employee is allowed to provide their access password to other employees unless requested by the manager, formalizing the reason why the password is being requested and changing the password as soon as the cause of the request is addressed.
Specific accesses not covered in the contracting process must be handled directly with the person responsible for the information asset.

Cancellation of accesses

The employee termination process involves withdrawing access rights to various information assets.

Internet access

iT.EAM provides internet access to employees and visitors, with access for visitors being made through a specific network separate from our corporate network.
The internet made available by iT.EAM to its employees, regardless of their contractual relationship, may be used for personal purposes, as long as this use

does not involve pornographic, fraudulent, defamatory, racially offensive, illegal content or content that violates any regulatory standards such as downloading illegal software or causes risks to our infrastructure.

Disclosure of confidential organizational information in any discussion groups, lists or chats is prohibited.

Failure to follow the policy will result in sanctions ranging from disciplinary procedures to verbal or written warnings.

Access to Electronic Mail

iT.EAM email users have a corporate email account enabled to send and receive external messages.

The standard institutional email address is firstname.lastname@it-eam.com. In exceptional cases of duplication or embarrassment to users, the standard may be revised.

The corporate email account is made available exclusively for institutional use and is not permitted for personal use.

Source code access

Access to program source code and associated items (such as drawings, specifications, verification and validation plans) is restricted to the development area.

All products generated during the systems development life cycle must be stored in repositories subject to access control mechanisms, ensuring that only authorized employees have access. Systems development must observe the principles of Information Security and DP protection, and if applicable, the best practices in the market.

The source codes of information systems owned by iT.EAM must be adequately maintained, including version control, correct classification of information and protection against undue access or changes.

Granting, withdrawing or adjusting access

Access granting must be carried out in accordance with the principle of least privilege, function and need to know.

The release of access to systems, directories, access groups or administrative profiles defined for users is reviewed periodically to ensure that access is compatible with the position, area of activity and functions performed. The following must be subject to a periodic review process:

- Access granted to systems and applications;
- Access granted to IT infrastructure.

The review of access to systems must be carried out according to the classification of the information contained in each system, or other criteria established by Senior Management.

The review process must be carried out each time the employee undergoes a change of position or function or in a critical analysis to be carried out annually by the information security team.

Privileged access

Privileged access credentials, which correspond to access to system administrator activities or physical assets, must be granted upon approval by the manager based on the function and the need to carry out work activities.

Sharing the use of privileged access credentials should be prohibited. However, if sharing is necessary for technical reasons, this must be authorized by the manager, formalizing the reason why the password is being requested and changing the password as soon as the cause of the request is addressed.

All users holding a privileged access ID must also have an access ID for non-privileged activities, so that access is only used when strictly necessary.

Use of privileged utility programs

The use of utility programs to access information related to the administrative and financial sector is prohibited.

The operational sector adopts the security measures listed in the iT.eam policies, and the consulting team is permitted to use utility programs to access the sector's tools. In any case, the team must adopt secure measures to ensure that the use of utility programs does not compromise system and application controls for information security.

Secure access to systems and password management

The logon procedure should disclose only the information necessary for the activities of a given employee, avoiding providing an unauthorized user with inappropriate information.

Login process help messages must not contain hints that could allow an unauthorized user to access the system.

Every user must have a unique, personal and non-transferable identification, qualifying him/her as responsible for any activity carried out under this identification.

The holder assumes responsibility for the confidentiality of his/her personal password, and is responsible for any action performed with his/her login/password.

Sharing, disclosure to third parties or making notes on paper of personal identification is not permitted.

hWe encourage the use of strong passwords, we recommend that the password as at least the following format:

- 8 (eight) or more characters;
- Inclusion of uppercase, lowercase letters, numbers and special characters.

It is not permitted to use weak passwords, such as those based on first names, personal data such as name, date of birth, document number, among others.

Our employees are not allowed to write down passwords in a visible place or where they can be accessed by another person.

Company system passwords should be changed whenever there is any indication that the system or password itself has been compromised. We also recommend that you do not reuse passwords.

When an employee receives a password created by a third party, they must change it to a secure password upon their first access, as suggested above.

Access to iT.EAM systems have two-factor authentication configured.

Remote access

We provide remote access to our infrastructure, as long as it is necessary to carry out the company's work activities through a secure connection with the approval of the area manager and IT team.

The tools we provide for remote access are tested and meet our security requirements.

Access to our customers' information is carried out through a secure, password-protected connection.

Company information that is stored remotely must be done via software that guarantees the security of the stored data and the information traffic.

In all cases of remote access, all security measures adopted by the company apply.

Clean Screen

Our employees, where applicable, must lock all equipment, workstations and servers during any temporary absence to prevent misuse of the equipment.

Information and data, whether in physical or digital format, must not be available at the workstation in the absence of the employee and cases of critical or confidential information must receive due care with regard to third-party access, even if the employee is present.

4.6. Use of Mobile Devices (user endpoints)

We do not allow personal mobile devices to access our corporate network, so all of our employees' mobile devices are only allowed to access the guest network.

Personal mobile assets are not registered as iT.EAM information security assets.

Personal mobile devices used by our employees for work activities must be protected by a password or visual identification.

Only software licensed by the organization may be used on a personal mobile device for work activities.

It is not permitted for working documents to be stored on a personal mobile device unless within the organization's own licensed tool repository.The company's mobile assets are registered as information security assets and follow all the requirements of the information security policies defined by iT.EAM.

The storage of DP (personal data) on personal mobile devices of our employees is not permitted.

However, when it is unavoidable to store DP in our company's mobile assets, they must be protected by all means available in the organization. If the personal data comes from an irregular source and risks to the security of the personal data are identified, a procedure for treatment must be opened with the iT.EAM security committee.

4.7. Network and communications security

It is prohibited to use Information Systems for the purpose of carrying out actions that are against national and international legislation and standards that may cause intentional damage to the network or other systems, intentionally damaging network traffic or access to resources.

iT.EAM maintains identified, implemented and monitored security mechanisms, service levels and network service requirements based on the best frameworks on the market regarding cybersecurity measures in order to ensure security in the use of network services.

4.8. Supplier Security

The relationship with suppliers is defined in iT.EAM and documented in order to seek the same level of security defined in the organization's processes.

Agreements with third parties, partners and suppliers are established and documented ensuring that there are no misunderstandings between the parties regarding their obligations to the applicable security requirements.

In cases of visits to customers where security standards are defined for access to secure areas, it is mandatory that our employees participate in all security training provided and follow all guidelines, ensuring their physical integrity and third-party standards.

4.9. Conformities

Through our Legal department, we identify and follow all applicable legislation that regulates the business, as well as aspects of intellectual property. We also ensure that only official, approved and authorized software and licenses are used to avoid infringing the intellectual property rights and copyrights of manufacturers and their representatives.

4.10. Information Security Incident Management

A work instruction was established and describes the guidelines for the management of Information Security incidents, ensuring a consistent and effective approach to incident management, ensuring that information security weaknesses and events are detected, recorded, investigated and, whenever possible, prevented.

All company employees must know and follow this instruction.

4.11. Business Continuity Management

We have established procedures for the recovery of critical services and processes in order to ensure that activities considered essential continue to be carried out and that critical services remain available to the user in situations of crises or unscheduled outages.

The iT.EAM's Business Continuity Management relies on the adoption of actions in the event of external events resulting from unforeseeable circumstances or force majeure, as well as situations of public calamity declared by the State or competent bodies that imply a risk to the continuity of the company's security or business and the physical integrity of its employees.

4.12. Continuous Improvement Management

The iT.EAM has several resources for continuous improvement management of its processes and makes a resource available to internal and external stakeholders to contribute to the improvement of their processes.
Interested Parties, if they identify the need or possibility of any corrective or preventive action in our processes, may contribute by sending suggestions to sac@it-eam.com.

The requesting Interested Party must inform in the email:

- Name of the applicant
- Request date
- Need to contact competent authority and which

- Whether it involves personal data or not
- Problem Description with Evidence (What happened? / What could happen?)
- Probable Cause (Why Did It Happen? / Why Could It Happen?)
- Proposed Action (What to do to prevent it from happening again? / What to do to prevent it from happening?)
- Submit evidence of the facts described, if possible
- Indicate whether you wish to receive a response to the proposed action

Requests will be analyzed by the organization's Security Committee and, if approved, measures will be adopted, with publication for Interested Parties and training of its Employees and third parties, if applicable.

5 Responsibilities

5.1. Users

iT.EAM 's information security policies in full.

Report occurrences or suspected security incidents to the Organization's Security Committee.

Ensure information security within the organization.

5.2. Manager

Be a multiplier agent, informing, encouraging and raising awareness among each user to comply with the Information Security and Cybersecurity Policy, Information Privacy Policy and related policies.

Ensure that at the time of contracting, the service provider is aware of and accepts the Information Security and Cybersecurity Policy and the Information Privacy Policy.

5.3. Information Security Committee

Be the guardian of information and personal data within the company;

Maintain and improve the information security and personal data protection system;

Review and update the documents that make up the Information Security Policy and Information Privacy Policy; Raise awareness and guide users regarding the Information Security Policy and Information Privacy Policy. Assess information security incidents and communicate the results to managers so that appropriate disciplinary measures can be taken.

Define the content of the information that will be available to users.

5.4. Human Resources Area

Ensure, at the time of hiring, that the process related to information security and privacy and protection of personal data is carried out.

6 Specific cybersecurity measures

In addition to the defined security measures, iT.EAM adopts the following actions as fundamental cybersecurity rules:

1. Monitoring your activities 24x7 with intrusion detection service.
2. Reducing vulnerabilities through active risk management.
3. Preventive actions against security incidents and leaks of personal data and information.
4. Secure communication channels via VPN.
5. Periodic vulnerability detection and updates.
6. Protection against malicious software.
7. Incident management and business continuity.

7 Information Security Policy Changes

This Information Security and Cybersecurity Policy is reviewed annually or at shorter intervals if necessary, and may be changed or updated by iT.EAM , subject to approval by the organization's management, in order to comply with legal obligations or relevant changes in the company's activities. All changes made come into effect when published, unless otherwise indicated.

Document revised and approved on 09/27/2024.

making a difference

INFORMATION SECURITY AND CYBERSECURITY POLICY

Published by: iT.eam in December/2024

+55 (31) 4063-7340 www.it-eam.com