IVEX's Information Security Policy

Version 1.1

Date: 03/05/2023

IVEX NV

KAPELDREEF 60

3001 HEVERLEE

BELGIUM

www.ivex.ai

Contact

Mario Torres

mario@ivex.ai

Information Security Policy

Objective: Provide an overview of this policy's purpose and goals.

In carrying out its mission of enabling the scalable development and validation of AD/ADAS systems, IVEX personnel create, receive, transmit and collect many different types of confidential and non-confidential information.

An Information Security Policy and culture are a fundamental requirement for protecting the confidentiality, integrity and availability of IVEX and its customers information and IT Resources. IVEX security strategy is to create a security culture which emphasizes learning over punishment.

All IVEX's employees, contractors, service providers, share a common set of responsibilities to protect Institutional Information and IT Resources, regardless of working location, device used, storage location (physical or cloud) or access method. Some members carry additional security responsibilities based on their roles and functions. Besides that, all IVEX's collaborators are required to sign an NDA (Non-disclosure agreement) which details how they should treat confidential information.

Information at IVEX is classified as:
Internal Use: Documents for internal usage. Information is available to all employees and selected third parties such as customers, partners
Confidential: Any confidential information belonging to IVEX or its customers and has to be treated as confidential unless explicitly marked otherwise. Materials marked as "Confidential" can never be shared without an NDA. Confidential information is clearly communicated as Confidential, and receivers are instructed about its possible uses.
Unrestricted/public: Information which can be openly disclosed publicly, such as any information posted on blog posts, IVEX websites and media campaigns or presentations without confidential information. If you have doubts if a certain information is unrestricted or confidential, ask your direct supervisor. Preferably, presentations which contain unrestricted information should have a clear marking "Unrestricted".

Goals

This policy establishes the framework for IVEX to achieve five electronic information security goals:

Protect privacy

IVEX is committed to maintaining and protecting privacy for individuals. Privacy consists of: (1) an individual's ability to conduct activities without suspected or actual observation; and (2) the appropriate use and release of information about individuals. Be compliant with privacy legislation, such as GDPR.

Follow a risk-based approach

IVEX is committed to following a risk-based approach to information security, which allocates resources to protect Information and IT Resources based on threats and their likelihood of causing an adverse outcome. This approach balances IVEX's information security goals with its other values, obligations and interests.

Maintain confidentiality

IVEX is committed to maintaining and protecting the confidentiality of Institutional Information. This requires the handling of information to ensure that it will not be disclosed in ways that are inconsistent with authorized use and its original purpose. This also requires the employment of state-of-the-art practices in information security.

Protect integrity

IVEX is committed to protecting the integrity of Institutional Information. Protecting integrity requires guarding against the improper modification or destruction of information.

Ensure availability

IVEX is committed to maintaining and protecting the availability of Institutional Information and IT Resources. This requires the management of Institutional Information and IT Resources to ensure that they are accessible and able to meet the IVEX's employees' and customers' needs.

Security is embedded in the life cycle of systems, services, software and processes. Information security must be incorporated into the entire lifecycle for any system, service, software or engineering processes. This includes identifying, planning, developing, implementing, maintaining security processes and controls and educating IVEX's collaborators and customers.

Roles and responsibilities

Maintaining and achieving a high level of information security is a joint responsibility shared between all IVEX's collaborators. The role for collecting incident information is allocated to the IVEX's CISO, while the role of improving the Information Security Policy is a shared responsibility between IVEX's CISO and CEO.

Responsibilities for the ISMS are the following:

- CEO is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
- CISO is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS
- The management team must review the ISMS at least once a year or each time a significant change occurs, and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the ISMS.
- CISO will implement information security training and awareness programs for employees
- the protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset
- all security incidents or weaknesses must be reported to the CISO.

Access Control & Protection

IVEX follows the principle of least privilege principle, which states that a user or user's account only receives privileges which are essential to perform its intended function. For example, a user's account for business users does not have SSH access to any IVEX servers.

Conversely, only collaborators working on a certain project can have access to materials pertaining to the project. Each project has a shared folder and a project manager which is responsible for giving access to the shared folder.

Access control is centralized on a single account which uses 2-factor authentication. Each access to IVEX's services is logged and stored in backups for at least 6 months. Besides that, access to computational resources is restricted to be accessed via VPN (Virtual Private Network) and only from IPs listed in IVEX firewall.

Encryption

Every IVEX's computing device must use the most updated encryption methods available. Employees must use encrypted devices and encrypted communication channels to store and transmit confidential information.

Physical and Environmental Security

IVEX ensures appropriate physical access to protect Institutional Information and IT Resources. Physical access to local IVEX's servers is limited to collaborators with the correct access code. Local servers are constantly monitored by video surveillance.

Protection from malware and intrusion

IVEX's collaborators must ensure that any device connected to an IVEX's network is free from malware. They are also trained to constantly monitor their own devices for the presence of malware or detecting unusual device functioning.

IVEX networks are monitored and unusual network activity is logged and reported.

Information Security Incident Management

Security incidents must be reported to the CISO, logged into a document describing the incident in detail and stored in a company-wide's shared folder. The incident report details the time and location of the incident, besides detailing precisely what is the incident and how it is fixed.

Examples of security incidents include:

- Computer system breach
- Unauthorized access to, or use of systems, software or data
- Unauthorized changes to systems, software or data
- Loss or theft of equipment storing institutional data
- Denial of service attacks
- Interference with the intended use of IT resources
- Compromised user accounts