*Date of last revision: 2025-04-01*

# Information Security Standards Policy

## 1. Policy Statement:

This Standards Policy is a supplemental document that provides specific, actionable protocols and requirements. For the foundational guidelines on information security at Evira, please refer to our core Information Security Policy.

Evira is committed to maintaining the confidentiality, integrity, and availability of information assets and electronic systems. This Information Security Standards Policy outlines specific security measures, protocols, and requirements aimed at achieving this goal.

## 2. Scope:

This policy applies to all employees, contractors, and volunteers who have access to Evira's information systems, including computers, networks, and data storage solutions. It also applies to management officers in charge of making sure the locations and devices provided to employees follow the proper security protocols.

## 3. Procedures:

### 3.1 Password Management:

- **General Requirements**: All employees are mandated to use a company-approved password manager for managing credentials associated with any system or service they access as part of their work responsibilities. This ensures consistent security practices and a centralised approach to password management across all company activities. Passwords must adhere to a minimum of 12 characters and a combination of uppercase and lowercase letters, numbers and special characters where the relevant service allows it. The password manager master password must adhere to the described password complexity. Longer passwords are highly recommended (30+ characters).
- **Initial setup:** Employees are required to set up an account with a company-approved password manager upon their induction. As of the last review of this policy, "LastPass" is the standard password manager in use. Any alternative password manager must offer a security level equivalent to or surpassing that of LastPass and requires explicit approval from the Data Protection Officer.
- **Password Complexity**: Passwords stored in the password manager must adhere to complexity standards, including the use of alphanumeric characters, symbols, and varying cases. All company-approved password managers provide a password generation tool for this purpose.

- **Default Passwords Prohibition:** Under no circumstances are default passwords to be used on any system, device, or application within the organisation. Immediately upon installation or deployment of any new hardware or software, any default passwords must be changed to a secure one that meets the company's password complexity standards.
- **Multi-Factor Authentication**: Employees must enable multi-factor authentication for their password manager accounts.
- **Shared Accounts**: For accounts that are used by multiple individuals or departments, the password manager's secure sharing features must be used.
- **Password and Key Rotation:** Passwords and cryptographic keys used to access specific sensitive or personal data must adhere to a rotation schedule. This rotation can either be enforced by the service itself or, if such enforcement is lacking or deemed insufficient, must be set and approved by the Data Protection Officer, tailored to the sensitivity level of the specific data being accessed.

**3.2 Multi-Factor Authentication (MFA/2FA):**

- **General Requirements**: Multi-factor authentication must be enabled for all services and systems that support it.
- **2FA Methods:** Acceptable methods of MFA include hardware tokens, mobile app-based tokens, and biometrics, as approved by the Data Security Officer.
- **Exceptions:** If a service does not support MFA but is essential for business operations, an exception may be granted by the Data Security Officer. Any such exception will be documented and reviewed annually. The exception may not be granted to privileged accounts. Passwords used must still adhere to the company password management requirements, see 3.1.

**3.3 Office Network Security:**

- **Internal Network**: All Evira office locations must operate a secure internal network.
- **Access Control:** Proper network access controls should be implemented, including firewalls and intrusion detection/prevention systems.
- **Guest Network:** Guest networks should be isolated from the internal network.
- **Responsibility:** The IT Department head of each respective office is responsible for ensuring the office network meets the standards defined above. It is the responsibility of each individual employee to use the network appropriately and protect it from unauthorised access.

**3.4 Avoiding Public Wi-Fi:**

For the security of company data, the use of public Wi-Fi networks is prohibited on all work-related devices unless an approved VPN is activated. Employees should only use secure, trusted networks for work activities.

**3.5 Software and File Downloads:**
Employees must not download or install unknown, unverified, or risk-associated files, applications, or software on computers or mobile devices used for work purposes. All software must be approved by the IT Department or the Data Protection Officer.

**3.6 Secure Remote Connections:**
Remote connections must be encrypted in transit and employ sufficiently complex authentication protocols.

**3.7 Third-Party Access Requests**
Evira employees are required to exercise caution and conduct a thorough evaluation of the ramifications associated with any third-party access requests to data held by Evira.

- **Decline by default:** Any request for access to sensitive data made by an entity that is not in strict collaboration with, and deemed trustworthy by, the management team must be declined.
- **Exercise caution:** Should an employee of Evira wish to grant access to any data held by Evira, a thorough consequence analysis must be conducted to ensure that no sensitive data is exposed.
- **Explicit approval:** If there are uncertainties regarding access grants, or if granting access to sensitive data is deemed to significantly benefit our workflow, such access must not be granted without first bringing the suggestion to the Data Protection Officer and obtaining explicit approval.

**3.8 Device Security:**
Device security is essential to protect Evira's information assets from threats and vulnerabilities associated with the use of electronic devices. This chapter establishes the minimum security standards and controls required for all devices, including but not limited to desktops, laptops, smartphones, tablets, and storage devices, that access, process, store, or communicate corporate information.

- **Device hardening:** All company-issued MacBooks must follow a secure build process. This includes activating FileVault encryption, enforcing Gatekeeper and Secure Boot, disabling unnecessary services, applying automatic updates, restricting admin rights, enforcing strong passwords, limiting software to approved applications and enabling the software Firewall. These controls should be applied during onboarding and reviewed regularly as part of our security assurance process. Contact your IT administrator if you need assistance.
- **Devices:** Devices must be kept up to date with the latest security patches and antivirus software.
- **Encryption:** All devices must employ full-disk encryption to protect data at rest. Devices must comply with industry-standard encryption protocols.

- **Browser Compliance:** Employees must use supported browsers such as Firefox and Chrome when accessing company resources or conducting company-related tasks online. These browsers must be kept updated to the latest version to ensure they are equipped with the most recent security features.
- **Responsibility:** The IT Department is responsible for setting up device security features. Each individual employee is responsible for maintaining the security features of their respective devices while in their possession. Audits are conducted regularly to ensure compliance with the company security standards.
- **Software updates:** All software must be configured for automatic updates if possible. Employees must also weekly check for updates in all softwares. All unused software must be removed as soon as possible.
- **Decommissioning hardware:** The IT Department is entrusted with overseeing the secure decommissioning of hardware. This includes conducting a thorough data sanitization process and ensuring all sensitive information is irretrievably erased from devices prior to disposal.

**3.9 Data Access Control:**

- **General Requirements**: All systems, applications, and databases that house sensitive or personal data must employ robust access control systems. Access to such data should be granted on a need-to-know basis and should be regularly reviewed to ensure compliance with this policy.
- **Access Revocation for Departing Staff**: Upon termination of employment, the IT department is responsible for promptly revoking the departing staff's access to all company systems, applications, databases, and any other digital resources used by the company.
- **Emergency Access Revocation:** In cases where an employee's mobile device or computer is lost, stolen, or otherwise compromised, administrators must have the ability to immediately revoke that employee's access to all systems containing sensitive or personal data. The IT department should regularly test and audit these emergency access revocation capabilities to ensure their effectiveness.
- **Routine Access Control Audits:** The IT department shall conduct routine audits to ensure that access controls are properly maintained and up-to-date across all company systems, applications, and databases. The audit must be performed annually at minimum. Any discrepancies or vulnerabilities identified during these audits will be addressed promptly to maintain the security integrity of company data and resources.
    - **Date of last audit:** 2024-03-04

**3.10 Privileged Accounts:**

- **General Requirements:** Privileged accounts must be used for sensitive configurations, reading or altering sensitive data, and accessing critical resources. Privileged accounts refer to accounts with elevated permissions used by appropriate administrative personnel with high security clearance.
- **Use Limitations:** Privileged accounts must not be used for day-to-day activities such as email access, web browsing, or other high-risk functions that expose them to potential security threats.
- **Device Restrictions**: Privileged accounts may only be accessed and utilised from company-provided devices, ensuring a controlled and secure environment for their operations.

**3.11 Session Timers for Handling Sensitive Data:**

- **General Requirements**: For systems, applications, or websites where sensitive data is accessed or manipulated, session timers must be implemented to automatically log the user out after a predefined period of inactivity.
- **Inactivity Duration:** Many services that handle sensitive data come with built-in session timers that are already calibrated to the sensitivity of the data. In instances where Evira has the ability to customise the session timer, the duration must be set in accordance with the level of data sensitivity and must be approved by the Data Protection Officer.

**3.12 Physical entry controls**

To ensure the security of Evira's headquarters and protect its assets, personnel, and sensitive information, the following physical entry controls are implemented:

- **Entry code system**: Access from the street to the hallway of the premises requires an entry code
- **Video surveillance**: All individuals who enter the premises are monitored by the property manager, thereby enhancing the ability to detect and respond to unauthorised access attempts.
- **Key access**: Physical keys to enter the headquarters are given to Evira staff and consultants. Distribution of keys is carefully managed, and records of key holders are maintained and reviewed regularly.
- **Double locked steel gate**: An additional layer of security is provided by a double-locked steel gate, serving as the primary physical barrier to access the office spaces. This gate is only accessible to individuals who have been granted explicit entry rights, ensuring a high level of protection against unauthorised entry.

**3.13 Physical Security in Alternative Environments:**

Any alternative office used temporarily must have physical security controls approved by the Management Team.

**3.14 IT Asset Management:**
For information on IT Asset Management, please refer to our IT Asset Management (ITAM) policy.

**3.15 Clear desk and screen policy**
To enhance our commitment to information security and data protection, Evira has adopted a clear desk policy. This policy mandates that all employees must ensure no sensitive or confidential information, whether in paper or on electronic devices, is left unsecured at their workspace at the end of each working day. Proper adherence involves security storing and destroying documents, locking electronic devices, and removing portable storage media from workstations to prevent unauthorised access and maintain the integrity of our data.

**3.16 Lock screen**
To maintain the confidentiality and integrity of personal and sensitive data, all devices and systems used by Evira staff must employ automatic session locking. Screens must automatically lock after no more than 15 minutes of user inactivity.

This measure applies to all workstations, laptops, and devices used to access systems where personal data is processed, including remote and office-based environments.

**3.16 Compliance:**
Failure to comply with the Information Security Standards Policy may result in disciplinary action, up to and including termination.

**4. Policy Review:**
This Information Security Standards Policy will be reviewed annually, or when new legislation is enacted or new guidance is issued, whichever occurs first. Changes will be communicated to all employees to ensure continued awareness and compliance. Date of last review: 2024-05-20.

**5. Validity of the Information Security Standards Policy:**
The policy was established by the company's management team and owners on 2023-08-31 and is valid until 2025-12-31.