Information security policy

Purpose and Scope

This Information Security Policy (ISP) defines the principles, measures, and procedures to ensure information security according to the requirements of the ISA catalog by enx® and ISO 27001. It applies to all employees, contractors, partners, and third parties who have access to the information and information systems of our company.

Responsibilities

Management

- Responsible for defining and approving the ISP.
- Provision of the necessary personnel and financial resources for implementing the ISP.
- Establishing information security strategies.

Information Security Officer (ISO)

- Implementation and monitoring of the ISP.
- Conducting regular training and awareness sessions on information security.
- Performing and coordinating information security audits and assessments.
- Reviewing and updating the ISP regularly (once annually and during significant changes).

Department Heads

- Ensuring the implementation of the ISP in their respective departments.
- Supporting the ISO in implementing security measures.
- Promoting a security culture within the departments.

Employees

- Compliance with the ISP and participation in information security training.
- Reporting security-related incidents through the following channels:
  a) Via email to IT and VJE
  b) Via Incident Report Button in the AIRSKIN Monitor
  c) By phone to the ISO
- Completing the online training within the set deadline.
- Confidential handling of company information.

Information Classification

Classification

Information is assessed according to three protection goals (integrity, confidentiality, and availability). This assessment determines the protection need. Information assets and carriers are marked accordingly in the asset list.

Categories of Information

- Category 1 – Non-sensitive Information

Information that holds no value for the company or partners, e.g., general internet research or publicly available information.

- Category 2 – Confidential Information

Information of higher importance to the company and partners, e.g., business processes whose leakage does not have serious consequences for us as a company.

- Category 3 – Protected Information

Information, e.g., protected by an NDA with a partner, whose leakage would have severe consequences for us as a company.

Transmission and Storage Forms

Any data transmission using USB sticks not issued by the company's IT is prohibited.
For all data transmissions with customers and/or suppliers, SharePoint links must be used. Under no circumstances may data be sent as email attachments. This primarily concerns external recipients but also applies to internal recipients, as links can be deactivated later.
If data storage on external hard drives or storage options is necessary, this must be coordinated with IT and ISO on a case-by-case basis.

Protective Measures

Categories 2 & 3 must be protected with strong encryption. Additionally, access to these categories is limited per user matrix (user groups in Active Directory).
The delivery of initial passwords or reset passwords must use encryption tools such as One-Time Secret.

Data Destruction

Secure and complete destruction of information that is no longer needed.
Creation and implementation of a data destruction plan covering all types of data media (e.g., paper documents, hard drives, USB sticks, CDs/DVDs, backup tapes).
Ensuring all employees are informed and trained on the data destruction guidelines and procedures.
Use of certified data destruction services for destruction conducted outside the company.

Methods of Data Destruction

Paper Documents: Use of shredders that meet at least security level P-4 (particle cut).
Electronic Media: Use of software tools for secure data deletion (e.g., multiple overwrites) or physical destruction (e.g., shredding, melting).
Hard Drives and SSDs: Destruction by certified service providers or use of specialized devices rendering drives physically unusable (e.g., degaussing, shredding).

Documentation of Data Destruction

Logging of all data destruction actions, including date, type of medium, destruction method, and responsible person.
Retention of destruction logs for a defined period in accordance with legal and regulatory requirements.

Access Control, Physical Security, and Protected Zones

User Access

Access to information systems is regulated through a role-based access control system.
All user accounts are unique, personalized, and traceable.
Regular review and updating of user rights.
Two-factor authentication (2FA) is mandatory for all accounts running on Office365.
Shared accounts may only be used in limited circumstances and when traceability is unnecessary.
All users are required to use strong passwords, as outlined in the application guidelines.

Physical Security and Protection Zones

The following areas within the company are defined as protection zones:

- Both server cabinets (Server and NAS)
- HR cabinet

Additionally, all monitors visible from outside or by visitors must be equipped with privacy filters.
All doors are lockable with specific keys assigned to employees based on their data security clearance.
General entry areas are video-monitored outside official office hours (delivery and main entrances).

Remote Access
Secure configuration of VPN connections for remote access—VPN settings may not be changed independently.
Use of endpoint security solutions on mobile devices and home workstations.

Incident Management

All employees are required to immediately report security incidents (incidents) to the ISO and IT.

What Counts as an Incident?

Any event potentially affecting data security, e.g., phishing emails, accidental entry of credentials on insecure or suspicious sites, or other incidents causing concern.

The ISO is responsible for initiating investigations of security incidents and taking appropriate measures to mitigate damage and restore normal operations.

The ISO ensures documentation of all security incidents and actions taken.

Training and Awareness

All employees are trained on information security policies during onboarding.
There is an annual update training, and additional training sessions occur if IT infrastructure changes affect employee behavior.

Risk Management

Regular risk analyses (once annually and when changes occur) to identify and assess information security risks.
Prioritization of measures based on risk severity and likelihood.
Adaptation of action plans based on new findings and changes in the risk landscape.

Data Backup and Backup Creation

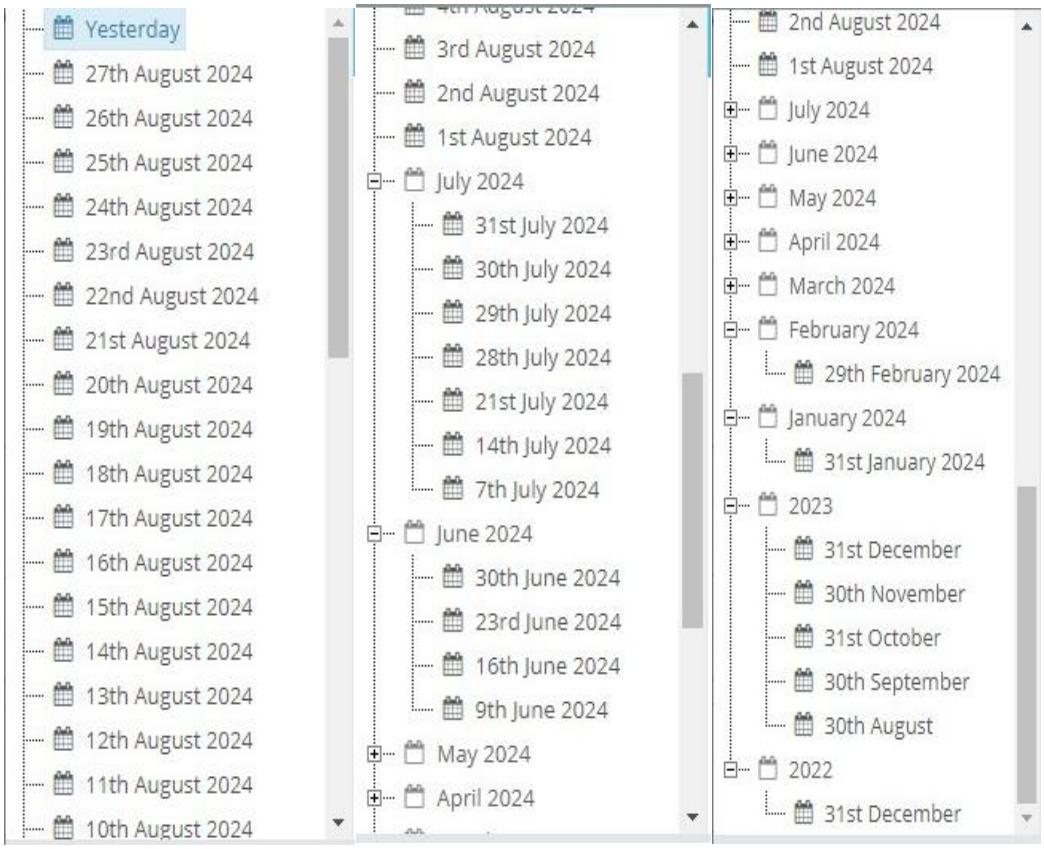
Current Backup Rules:

The DC01 (Domain Controller, Active Directory), which also contains file servers N/Z/H (internal designations), is backed up daily at 8:00 PM in three locations:

- NAS (Network Attached Storage) in the server cabinet.
- NAS in the distribution cabinet above production.
- Cloud service in a Vienna data center.

Backups are deleted after one month, except:

- 1 backup per week for 12 weeks.
- 1 backup per month for 12 months.
- 1 backup per year for two years.



The second server also backs up virtual machines under the same rules, including:

- APP01
- CRM01
- DC02
- GitLab
- Nextcloud-PUBLIC
- OpenProject
- UBUNTU01-ATLASSIAN

Review and Improvement

Regular internal audits to ensure ISP compliance.
Documentation and implementation of measures based on audit results.
Identification and implementation of improvements from training feedback and incident reports.
Participation in external audits and certifications to validate security practices.

Emergency Management and Recovery

This is covered in separate policies, including a general emergency plan, an IT-specific emergency plan, and a Business Continuity Concept.
An annual disaster recovery test is conducted to identify improvements.
External penetration tests provide valuable input for faster recovery during emergencies.
This translation aims to preserve the structure and terminology of the original text as closely as possible.