ISMS Information Security Policy

Purpose

This policy introduces the concept of the Information Security Management System (ISMS) applied to the organization.

Scope

This policy applies to every person working under the ISMS in the organization.

Acceptance

This policy should be understood and accepted by people who work under an ISMS Employee (PUBLISHED) role in the organization. The policy is defined and accepted by the people working in the ISMS Top Management (PUBLISHED) role in the organization.

Policy

The organization defined, introduced and has been managing the Information Security Management System (ISMS) compliant with the ISMS ISO/IEC 27001:2022 (PUBLISHED) standard in the organization. This policy is the highest, entry level document, explaining the scope and structure of the ISMS.

1.1 ISMS Scope

The organization applies the ISMS to all persons in the ebadu.pl sp. z o.o. organization, and to those persons from WiLabs organization that provide R&D services of ebadu products. All such persons are called employees.

The ISMS Top Management (PUBLISHED) defines the following certification statement for the ISMS:
“Research and development, service delivery and consulting services related to the ebadu products”.

The scope of the ISMS applies to the following organizations:

1. ebadu.pl sp. z o.o. ul. Skowronkowa 1, 55-093 Kiełczów, Polska
    a. Services - all service lines;

   b. Products - ebadu.PKUP, ebadu.R&D, ebadu.IPBox;
   c. Roles - all roles in the organization;
2. WiLabs sp. z o.o. ul. Skowronkowa 1, 55-093 Kiełczów, Polska
   a. Services - R&D services of product developed for ebadu.pl organization;
   b. Products - none;
   c. Roles - only these of the R&D roles which are engaged in the R&D activities of ebadu products;

1.2 Normative Sources Compliance

The top management declares the compliance with the following standards and regulations by implementing the ISMS:

1. ISMS ISO/IEC 27001:2022 (PUBLISHED)
2. ISMS ISO/IEC 27002:2022 (PUBLISHED)

The top management decides that the Information Security Management System shall be certified by an independent notified body, to prove maturity of the approach to information security as well as to identify opportunities for improvements.

While the ISMS supports the confidentiality, integrity and availability of information, including personal data, it does not directly result in compliance with either ISMS General Data Protection Regulation (GDPR) (PUBLISHED) or ISMS Ustawa o ochronie danych osobowych(PUBLISHED) regulations. This is achieved by the definition of the personal information management system in the organization in addition to the ISMS.

1.1 Declaration of Top Management

The top management of the organization declares to commit to the protection of the information security in the organization as well as lawful processing of personal data. To achieve this goal the top management introduces the **Information Security Management System (ISMS)** compliant with ISMS ISO/IEC 27001:2022 (PUBLISHED) standard. The security of information in the organization depends on daily activities of all people employed or contracted in the organization hence they shall be made aware of the ISMS setup, educated and supported in executing information security activities.

1.2 Information Security Objectives

There are the following common security objectives established for the ISMS:

1. Assuring confidentiality, integrity and availability of the information and key assets in the organization.
2. Ensure lawful processing of personal data in the organization.
3. Supporting building security awareness among the employees.
4. Continual improvement of the ISMS.

The organization can further extend its information security objectives specifically for each year and document them in ISMS Information Security Objectives.

1.3 Policies

The full ISMS documentation is located in 1. Information Security Management System folder. The top management introduced the following high level policies to guide and direct organization ISMS' operations.

Policy	**Audience**
ISMS Information Security Policy (PUBLISHED)	ISMS Employee (PUBLISHED)
ISMS Information Classification Policy (PUBLISHE...	ISMS Employee (PUBLISHED)
ISMS Assets Acceptable Use Policy (PUBLISHED)	ISMS Employee (PUBLISHED)
ISMS Access Control Policy (PUBLISHED)	ISMS Employee (PUBLISHED)
ISMS Network Security Policy (PUBLISHED)	ISMS Employee (PUBLISHED)
ISMS External Communication Management Poli...	ISMS Employee (PUBLISHED)
ISMS Information Transfer Policy (PUBLISHED)	ISMS Employee (PUBLISHED)
ISMS Mobile Devices Management Policy (PUBLI...	ISMS Employee (PUBLISHED)
ISMS Storage Media Management Policy (PUBLIS...	ISMS Employee (PUBLISHED)
ISMS Passwords Management Policy (PUBLISHED)	ISMS Employee (PUBLISHED)
ISMS Security Risk Management Policy (PUBLISH...	ISMS Information Security Off...
ISMS Suppliers Management Policy (PUBLISHED)	ISMS Information Security Off...
ISMS Cryptographic Controls Policy (PUBLISHED)	ISMS Administrator (PUBLISH...
ISMS Backups Policy (PUBLISHED)	ISMS Administrator (PUBLISH...

1.4 Roles

The ISMS introduces the following crucial roles. It is required that every person in the organization assigned to a role reads and accepts related ISMS documentation to understand their impact on the information security in the organization.

Role
ISMS Employee (PUBLISHED)
ISMS Administrator (PUBLISHED)
ISMS Information Security Officer (PUBLISHED)
ISMS Top Management (PUBLISHED)

1.5 Continual Improvement

The ISMS reflects the current approach to the security risk and possible vector attacks. The ways the organization is attacked are continuously evolving and so shall our ISMS. This process of continual improvement is a key characteristic of any management system.

The top management encourages everybody in the organization to suggest or report any:

1. Event
2. Opportunity for improvement
3. Security weakness
4. Security incident
5. Nonconformity

that could help us to improve information security in the organization.

This shall be done in a way supporting transparent and open communication within the organization. Our common goal is to protect information security by improving processes around the ISMS and the organization operations.

Policy Compliance

The organization will monitor compliance with the policy of its employees by different methods like monitoring, measurements, periodic reviews, and audits. The ISMS Employee (PUBLISHED) must follow this policy, while noncompliance may trigger the disciplinary process.

References

Normative source	Chapter
ISMS ISO/IEC 27001:2022 (PUBLISHED)	5.1; 5.2; 6.2; 7.3; Annex A: 5.1; 5.4; 5.36; 6.3; 6.4