

POLICY FOR INFORMATION SECURITY

DeLorentz & Partners is a Managed Service Provider in the field of ICT Management & Support and Projects & Advise. The focus is on the Hospitality sector, financial service providers such as Private Equity and pension funds, and not for profit organizations (charity) and (semi) government institutions. DeLorentz & Partners provides Cloud, security and infrastructure services. Information security is of crucial importance within these services.

DeLorentz & Partners has established an Information Security Management System (ISMS) that meets all the requirements of the ISO 27001 standard and the regulations of relevant supervisory authorities.

The management has established an information security policy that demonstrates the organization's implementation and effectiveness of the measures that have been taken. This policy has the following objectives:

- Demonstrably being in control in the field of information security;
- Keeping identified information security risks at an acceptable level;
- Ensuring the availability, integrity, and confidentiality of business information in all phases of business processes and within the used information systems;
- Ensuring security within information systems and applying security requirements in the process of implementation, development, and maintenance;
- Registering, investigating, and handling actual and suspected information security incidents;
- Registering, investigating, and mitigating possible vulnerabilities;
- Complying with legal and contractual requirements, the security controls in information systems, audits, and periodically performing checks;
- Aiming for continuous improvement of information security and the ISMS.

Important components of the information security policy are:

- Policy for Protection and control (security principles and standards)
- Policy for Information classification
- Policy for protecting information during storage and transport
- Policy for the use of company assets
- Policy for suppliers
- Business continuity plan
- IT policy for employees
- AI policy for employees

The Security Officer is responsible for maintaining the information security policy and achieving its objectives. The Security Officer provides support and advice during the implementation and execution.

The policy is periodically adjusted based on new developments, incidents, risk assessments, and checks.

The organization provides the necessary people and resources to secure its assets, work processes, and information systems as described in the information security policy.

Compliance with the information security policy is mandatory.

The management DeLorentz & Partners reviews this information security policy framework every two years or earlier if necessary.