Information security in ZENTITY

1. ZENTITY has a set of information security policies which define rules for specific aspects of the information security management system and are valid for employees and external subjects. Information security policies are available within the company intranet or on demand.
2. Employees or external parties are obliged to report any violation of information security policies, security incidents or discovery of a system vulnerability to the security team at the email address **security@zentity.com**.
3. Information processed by ZENTITY is labeled according to the rules defined in the policy for classification and labeling of information. The classification scheme consists of the following levels:

   C1 - Public: Information shared with the public.

   C2 - Restricted: Information restricted to ZENTITY personnel or authorized individuals.

   C3 - Confidential: Sensitive key information available to a narrow group of individuals.

   C4 - Secret: Strategic information dedicated mostly to the management board.
4. All relevant policies need to be followed when handling information, especially the asset handling policy. Access to information in both electronic and digital form is managed in compliance with access control policy. Sharing of information classified as C3 or C4 with unauthorized personnel is prohibited. This includes forwarding of electronic messages and emails.
5. Account passwords, their protection and handling must be in compliance with the password policy. Sharing of passwords with unauthorized personnel or storing of passwords in an unencrypted form is prohibited.
6. ZENTITY is compliant with all legal requirements in the area of information security, including protection of personal information and intellectual property.
7. Information processing equipment is protected and maintained on a regular basis in order to meet all security requirements. Software is used in compliance with the license requirements of suppliers and is regularly updated, including application of all security patches. Zentity is also continuously monitoring vulnerabilities of utilized information systems.
8. Internal networks and network services are protected from unauthorized access by use of suitable security elements. Secure communication channels and cryptographic techniques are used to transfer information securely.
9. Information security is also addressed in the area of supplier relations. Information security requirements are transferred to the suppliers in the required scope and properly communicated.
10. All software products developed by ZENTITY meet the high security standards and requirements defined by **ISO/IEC 27001:2013** and undergo regular security and quality testing.