Certum by asseco	Certum information security policy	
	CC-DK02-ZK-01	Version: 1.0
Valid from: January 31, 2020		

Purpose of all Certum activities, as a qualified trust service provider, in ensuring information security is to achieve organizational and technical level that:

1. ensures:
    a. information confidentiality - i.e. ensuring that information is disclosed only to authorized persons,
    b. information integrity - i.e. ensuring the accuracy and completeness of information and methods of its processing,
    c. information availability - i.e. ensuring that authorized persons have access to information and related assets when necessary;
2. guarantees an adequate level of security of processed information in both IT and paper systems,
3. significantly reduces the risk of threats to information security,
4. ensures correct and safe functioning of information processing systems,
5. ensures readiness to take action in crisis situations.

Consistent protection of information is implemented by identifying groups of information that will be protected, systems and the area of their processing. Objectives set for information protection are achieved through:

1. appropriate determination of the organizational context,
2. division of non-confidential and protected information,
3. defining information constituting the company's secret as being protected due to its prosperity, interest and market position,
4. defining protected information due to legal requirements and expectations of internal and external stakeholders,
5. dividing protected information into groups and managing them,
6. adding an appropriate clause to protected information,
7. defining of organizational and technical security requirements for the processing of protected information groups,
8. creation of organizational structures responsible for managing information security and processing,
9. information processing continuity management,
10. procedures standardization and development of necessary documentation in the form of principles of security management of information groups and their processing systems,
11. implementation of technical solutions ensuring the required level of processed information security,
12. effective promotion of information security principles among management and employees,
13. basic information security training for new employees and subcontractors,
14. training updating news on information security for employees and subcontractors,
15. cyclical documentation reviews as part of the review of the information security system and internal audits,
16. limiting the risk of information leakage by monitoring the flow of information in processing systems.

This document describes general security principles applied in Certum - an organizational unit of Asseco Data Systems S.A.

Certum Security Policy is available on the Certum website under the link: https://www.certum.pl/pl/cert_wiedza_repozytorium_pl_en/.

Document change history

1.0	January 31, 2020	Document preparation.