Information Security Policy

Key Solutions Polska Sp. z o.o. · Summary for business partners

1 Definition of the security strategy

1. Security of Key Solutions Polska is a state defined by an adopted set of standards, rules, solutions, and resource protection measures and methods, measured by the level of risk of a breach of the availability, confidentiality or integrity of those resources.
2. Information security of Key Solutions Polska is ensured if the risk of a breach of the availability, confidentiality or integrity of protected resources at Key Solutions does not exceed acceptable parameters while the rules set out in this Policy are observed.
3. The purpose of introducing the Information Security Policy (ISP) is to reduce identified risks.

2 Objective of the security strategy

1. To ensure the required commitment of employees to maintaining the security of information systems, to set the direction for developing the security management of these systems while meeting all requirements of applicable law, and to guarantee the efficient operation of Key Solutions Polska.

3 Management Declaration of Key Solutions Polska

1. The ISP sets the direction of action for the Management and employees of Key Solutions Polska in order to ensure systematic supervision over the collection, processing, storage and disclosure of information, regardless of how these processes are carried out.
2. The Management of Key Solutions Polska ensures the security of resources and of information contained in the information systems of Key Solutions Polska and outside them, as described in the ISP, because they are of fundamental importance for achieving the mission and statutory objectives of Key Solutions Polska.
3. The ISP expresses the will of the Management of Key Solutions Polska with regard to the protection of its resources.
4. The Management of Key Solutions Polska actively supports processes aimed at ensuring the security of information processing by implementing, developing and updating the ISP and the regulations deriving from it.
5. The ISP and the regulations deriving from it apply to all employees, trainees, interns, volunteers and other natural persons, legal persons or organisational units without legal personality that gain access to the resources of Key Solutions Polska, except users of publicly available information.
6. The Management of Key Solutions Polska is responsible for providing the resources for these purposes.
7. The ISP sets out guidelines for creating rules for the protection of information systems, with particular regard to the ICT system of Key Solutions Polska and the information contained in it.
8. Every employee, trainee, intern, volunteer and other natural person, legal person or organisational unit without legal personality that obtains a right/authorisation to access the resources of Key Solutions Polska

is made familiar with the ISP, confirms this in a written statement, and undertakes to comply with the principles, rules and provisions deriving from it.

9. Internal procedures and regulations of Key Solutions Polska may not infringe the provisions of the ISP.

4 General regulations

1. Human life and health are the highest value, and their protection in an emergency takes precedence over the protection of any other resources.
2. In addition, the following are protected:
   a. information processed at Key Solutions Polska, regardless of its form and medium, including personal data,
   b. equipment used to process, transmit and store information at Key Solutions Polska,
   c. premises housing key IT equipment and documents containing legally protected secrets, including personal data,
   d. software used at Key Solutions Polska,
   e. the image of Key Solutions Polska,
   f. other property used at Key Solutions Polska.
3. The purpose of establishing the ISP is to ensure the confidentiality, availability and integrity, while maintaining the authenticity, non-repudiation and accountability, of information processed at Key Solutions Polska.
   a. Confidentiality of information – means that it is available only to persons authorised to use that information.
   b. Availability of information – means that an authorised person can use the resource upon every justified request, within a set time.
   c. Integrity of information – means that the information has not changed since its last authorised modification and has not been deleted in an uncontrolled manner.
   d. Authenticity – the property that the origin or content of data is as declared.
   e. Non-repudiation – the impossibility for one of the parties to a data exchange to deny its participation in all or part of that exchange.
   f. Accountability – the property that allows a specific action to be attributed to a natural person or process and placed in time.
4. Information security at Key Solutions Polska is achieved by implementing technical and organisational safeguards, in particular through orders, procedures, rules and instructions ensuring a transparent organisational structure, and through ongoing review of the correct functioning of the software and hardware used to process information. These safeguards are monitored for continuous improvement.
5. Information security at Key Solutions Polska covers not only the registered office of Key Solutions Polska but also all situations in which information related to the business of Key Solutions Polska is processed

outside its office. This includes, in particular, remote access to the computer network of Key Solutions Polska.

English translation of the Polish document “Polityka Bezpieczeństwa Informacji (PBI) dla kontrahentów”.