ERBUD GROUP

Information Security Policy



ERBUD GROUP

INFORMATION SECURITY POLICY

§ 1
Introduction

1. The Information Security Policy is the basic component of the Information Security Management System in the ERBUD Capital Group.

2. The Policy contains general requirements, rules, procedures and instructions for the protection of information processed by the ERBUD Capital Group. The Information Security Policy is an overriding document in relation to other internal acts on information security. It forms with them a comprehensive security documentation.

3. The Information Security Policy is subject to regular review in terms of up-to-datedness, relevance and adequacy.

§ 2
Objective

1. The ERBUD GK establishes, taking into account applicable regulations, information security principles and requirements, as well as the results of the risk analysis and information security objectives.

2. The established security objectives support the adopted strategy and the implementation of the goals of ERBUD Capital Group, as well as the tasks performed by ERBUD Capital Group employees, interns, trainees, volunteers and other persons and external entities performing activities on behalf of and for the benefit of ERBUD Capital Group entities and/or having access to ERBUD Capital Group information assets

3. The major goals of ERBUD Capital Group's information security are as follows:

   a) to ensure the safety of ERBUD Capital Group's information assets (including protection of its image and relations with external entities) in accordance with the requirements of applicable law and in accordance with the results of the information security risk assessment,

b) to improve the ERBUD Capital Group's operations by organizing the principles of information processing and managing information assets in an orchestrated manner to facilitate improvement and alignment with the current ERBUD Capital Group's goals,

c) to minimize risks and limiting the effects of information security loss,

d) to raise awareness of employees and other persons and entities referred to in Section 2 above regarding information security.

4. As part of the objectives' implementation process, in adherence to the level of identified risks, measures are taken to achieve a level of organizational and technical levels of the ERBUD Capital Group, which, in particular, will ensure the following:

a) raising awareness of employees and other persons and entities, referred to in Section 2 above regarding information security,

b) integrity of information and its availability,

c) inclusion of additional security elements in accordance with requirements and decisions, and ensuring secure information processing, including the ability to take action in emergency situations,

d) documented information on information security objectives and the degree to which they have been achieved.

5. The ERBUD Capital Group carries out a periodic assessment of the progress in the achievement of set information security goals.

§ 3

Scope of the Information Security Management System

1. The scope of the established Information Security Management System comprises:

a) processes and activities and tasks carried out in the ERBUD Group,

b) all information processed as part of the aforementioned processes and tasks, including:

- processed in traditional form (including information printed or recorded on paper),
- processed in electronic form (e.g., sent via e-mail or electronic devices, electronic media),
- verbalized,
- owned by the ERBUD Group or other entities, insofar as they have been transferred on the basis of applicable laws or contracts

c) assets supporting the processing of information as part of the activities and tasks carried out in the ERBUD Capital Group, including:

- employees (all employees of ERBUD Capital Group regardless of the basis of cooperation), trainees, interns, volunteers and other persons and external entities performing activities for and on behalf of ,
- ERBUD CG and/or who have access to the information assets of the ERBUD Capital Group's information assets),
- ERBUD CG's buildings and premises where information is or will be processed,
- equipment, including computer hardware, mobile devices and other data carriers used to store protected information, software and network infrastructure,
- technologies for acquiring, selecting, analysing, processing, managing and sharing information, which include both paper-based and electronic systems,
- organizational structure.

2. Owing to the special nature of classified information under current legislation, the protection of classified information and assets supporting its processing is subject to exclusion from the established Information Security Management System.

§ 4

Basic principles of information security

1. In order to secure information and the assets that support its processing, the following basic principles of information security are implemented in the ERBUD Capital Group:

a) the principle of „adequacy of safeguards" - the safeguards used must be adequate to the identified risks,

b) the principle of „secure processing" - processing of sensitive information should be carried out only in secure environments, i.e. in dedicated IT systems, on secured premises, etc.,

c) the principle of „secure cooperation with external entities" - documents governing cooperation with external entities (including the content of contracts and agreements) contain provisions on information security, including security clauses on confidentiality,

d) the „clean desk" rule - in order to eliminate the risk of information being accidentally or intentionally read, copied, destroyed or modified by unauthorized persons, when leaving the workplace, documents containing information other than information of a public nature should be removed from the desk top, placing them in designated secure office furniture: cabinets, drawers or safes,

e) the „clean screen" rule - for the time of absence, access to the computer should be effectively blocked and the computer should be turned off after work,

f) the principle of „segregation of duties and tasks" - duties and powers should be so separated that one person does not have full authority to perform tasks in their entirety,

g) the principle of „authorized access" - the use of ERBUD CG's information assets may be carried out only on the basis of formal authorizations to use selected assets,

h) the principle of „improving the Information Security Management System" - the information security management system is adapted to changing conditions based on the results of periodic monitoring and supervision,

i) the principle of „need-to-know knowledge" - the persons referred to in § 5 have knowledge of information assets to a limited extent, necessary to carry out the tasks assigned to them.

2. Additional safety rules may be specified in other documents included in the safety documentation.

3. The Employees of ERBUD Capital Group, trainees, interns, volunteers and other persons and external entities performing activities for and on behalf of ERBUD Capital and/or having access to ERBUD Capital Group's information assets are required to comply with ERBUD Capital Group's applicable security rules.

§ 5

Roles and responsibilities in information security

1. Responsibility for information security shall be borne by all ERBUD Capital Group employees, trainees, interns, volunteers and other aforementioned persons and entities covered by the scope of the established Information Security Management System.

2. The responsibility is to comply with the requirements of generally applicable law, the provisions of this document and other requirements indicated in the security documentation, in particular, to:

a) implement the assigned information security related tasks;

b) protection of outsourced information and securing the assets supporting its processing,

c) not to give access to information to unauthorized persons,

d) keeping secret protected information and ways of securing it,

e) reporting suspicions/any irregularities noticed that may affect information security.

3. ERBUD Capital Group management is responsible for providing the resources necessary for the on-going operation, maintenance and continuous monitoring and improvement of the Information Security Management System.

4. In order to separate management and control functions from executive functions, roles and responsibilities within the established Information Security Management System have been established in two areas:

a) Roles and responsibilities in the area of administration are primarily related to the maintenance, on-going management and development of the Information Security Management System.

b) Roles and responsibilities in the security area are primarily related to the oversight, monitoring and continuous improvement of the Information Security Management System.

Information processed in the ERBUD Capital Group covered by the established Information Security Management System is classified in the following categories:

1) personal data (as defined in the regulations on the protection of personal data),

2) legally protected secrets (secrets established under the laws, the obligation to protect which arises from the laws),

3) secrets of the ERBUD Capital Group (information the disclosure of which could expose the ERBUD Capital Group to harm, as well as internal information made available on a „need-to-know" basis),

4) non-classified information (including information made available on a public information basis.