Information Security Policy of Reliable Deployment sp. z o.o.

1. General Provisions

1.1. This Information Security Policy of Reliable Deployment sp. z o.o. (hereinafter – the Policy) defines the system of principles for ensuring information security and represents a systematized presentation of the objectives and tasks of protection, the key principles of construction, and the organizational, technological, and procedural aspects of ensuring information security in Reliable Deployment sp. z o.o. (hereinafter – the Company).

1.2. Information security is the state of an information system in which unauthorized access, use, disclosure, distortion, modification, examination, recording, or destruction of information is impossible. Information Security implies a mechanism regulating the exchange of information and corresponding to such principles as confidentiality, availability, and integrity.

1.3. The Policy takes into account the current state and the near-term prospects of the development of information technologies in the Company, the objectives, tasks, and legal foundations of their operation, modes of functioning, and also contains a list of security threats to the objects and subjects of the Company's information relations.

1.4. The requirements of this Policy apply to all structural units of the Company.

1.5. The Policy is developed in accordance with the laws and regulatory legal acts of the Republic of Poland.

1.6. The Policy takes into account the requirements of Regulation (EU) 2022/2554 (DORA), which ensures digital operational resilience, security, and reliability of the Company's ICT processes and systems.

1.7. The Policy serves as the methodological basis for:

1) forming and adhering to a unified Policy in the field of ensuring information security within the Company;
2) organizing activities for identifying information subject to protection, justifying its level of confidentiality, and documenting it in the form of corresponding lists;
3) making managerial decisions and developing practical measures for implementing the information security policy;
4) developing a set of coordinated measures aimed at detecting, countering, and eliminating the consequences of various types of information security threats;
5) coordinating the activities of the Company's structural units when performing work related to the creation, development, and operation of information technologies in compliance with information security requirements;
6) developing proposals for improving the legal, regulatory, technical, and organizational support for information security within the Company.

1.8. The protection of information resources is carried out within the framework of the ISMS, which complies with:

– the requirements of the international information security standard ISO/IEC 27001:2022;

– the requirements of legislation, regulatory and contractual obligations of the Company in the field of information security;

– this Information Security Policy of the Company.

1.9. The scope of the Company's Information Security Management System (hereinafter – ISMS) is the successful provision, maintenance, and support of software development services (see the document "Statement of Applicability of the ISMS of Reliable Deployment sp. z o.o.").

1.10. The management of the Company, represented by the General Director, fully assumes responsibility for activities related to ensuring information security within the Company, declares its commitment to the above-stated goals and principles, and obligates all Company personnel to comply with them. The Company's employees bear personal responsibility for complying with the requirements of ISMS documents and are obligated to report all identified information security violations.

1.11. This ISMS construction Policy is subject to regular review at least once a year.

1.12. The Information Security Policy may be provided to interested parties upon their request.

1.13. The Policy is aimed at achieving the following main objectives:

1) protecting the integrity of information used and processed within the certification scope;
2) preserving the confidentiality of critical information resources;
3) ensuring the availability of information processed in the Company's information systems (hereinafter – IS);
4) ensuring the continuity of the main business processes functioning within the certification scope.

1.14. To achieve the specified objectives, the following tasks must be fulfilled:

1) active participation of the management in the Company's information security management;
2) increasing employees' awareness of risks associated with information resources;
3) clear distribution of responsibilities and duties of employees related to ensuring information security (see job descriptions);
4) restricting employees' access to the Company's hardware, software, and information resources;
5) recording user actions in system logs when using network resources;
6) controlling the correctness of user actions in systems by analyzing the contents of these logs;
7) protecting the functioning of IS from interference by unauthorized persons;
8) controlling the integrity of software tools used, the execution environment, and restoring it in case of violation, as well as protecting systems from the introduction of malicious code;
9) protecting restricted-distribution information and personal data from leakage through technical channels during its processing, storage, and transmission via communication channels;
10) ensuring authentication of IS users and resources;
11) timely detection of information security threats, as well as the causes and conditions contributing to damage;
12) creating conditions for minimizing and localizing damage caused by unlawful actions of individuals and legal entities;
13) applying disciplinary measures in case of violation of the Information Security Policy;
14) eliminating the consequences of information security violations;
15) developing and implementing rules and instructions for ensuring information security, as well as monitoring employees' compliance with relevant requirements;
16) implementing measures for assessing, managing, and minimizing information risks (see the documents "Methodology for the Analysis and Assessment of Information Security Risks of the Information System of Reliable Deployment sp. z o.o." and "Instruction on the Procedure of User Actions for Responding to Information Security Incidents and Non-standard (Crisis) Situations of the Information System of Reliable Deployment sp. z o.o.");
17) improving the ISMS.

2. Responsibility and Obligations of Management

2.1. Effective security requires accountability, comprehensive definition, and recognition of security-related duties. Management is responsible for all aspects of security management, including decision-making in risk management. Individual factors such as the type, form of incorporation, size, and structure of the Company will influence the level at which these duties are defined. Information security is an interdisciplinary matter that concerns all users within the Company. Proper definition and separation of accountability, specific official duties, and responsibilities ensures effective and competent performance of all important tasks.

2.2. Management takes direct part in resolving issues related to ensuring information security in accordance with the Company's (business) objectives, laws, and regulatory acts.

2.3. Management ensures the allocation of sufficient resources (financial, technical, and human) for the functioning and improvement of the Information Security Management System.

2.4. Management supports the required level of information security by implementing the ISMS and by allocating duties and responsibilities of personnel for its maintenance (see Job Descriptions).

2.5. Management:

1) formulates, reviews, and approves the Information Security Policy, as well as monitors the effectiveness of its implementation;
2) ensures clear governance and real support for information security initiatives;
3) provides resources for ensuring information security;
4) ensures coordination of information security control measures within the Company;
5) approves the roles and responsibilities of employees in the field of information security through job descriptions, orders, directives, etc.;
6) initiates ideas, plans, and programs to maintain information security awareness, determines the need for training of users and administrators in security methods and procedures, and defines duties related to the installation and maintenance of software and hardware;
7) clearly establishes the responsibility of department heads for various assets and security processes; the details of such responsibility are documented, and the levels of authority are clearly defined and documented;
8) enforces disciplinary measures in the event of Information Security Policy violations;
9) eliminates the consequences of information security violations;
10) promptly and mandatorily identifies and suppresses attempts to violate the established information security rules.

2.6. The control of user activities, of each security measure, and with respect to any protected asset is carried out on the basis of operational monitoring and logging tools and covers both unauthorized and authorized actions of users.

2.7. Management approves acceptable risk levels and risk tolerance levels that determine decision-making in the field of information security.

2.8. To ensure the timely consideration of changes in threats, regulatory requirements, and best practices, the Company maintains interaction with professional communities, industry groups, and associations in the field of cybersecurity.

2.9. Employees are informed of the measures of responsibility for the disclosure of information in accordance with their functional duties, as well as the measures of responsibility for possible violations.

2.10. The Information Security Policy may be provided to interested parties for review upon request.

2.11. The personnel servicing the information systems (hereinafter – infrastructure administrators), in case of violation of the requirements of the Information Security Policy, shall be held administratively or otherwise liable in accordance with applicable law. Responsibility is assigned to infrastructure administrators in accordance with their obligations as defined in the document "Infrastructure Administrator Guide." In particular, infrastructure administrators ensure the continuous functioning of the network and are responsible for implementing the technical measures required for the enforcement of the Information Security Policy.

3. Main Principles of Ensuring Information Security

3.1. The main principles of ensuring information security in the Company are:

1) compliance with legal requirements;
2) adherence to international and national information security standards in force within the country;

3) continuous and comprehensive analysis of the information environment in order to identify vulnerabilities of information assets;
4) identification of cause-and-effect relationships of potential problems and, based on this, building an accurate forecast of their development;
5) assessment of the degree of impact of identified problems;
6) integrated use of methods and means of protecting computer systems that cover all significant threat vectors and do not contain weak points at the intersections of individual components. Protection is ensured through physical, organizational, technological, and legal measures. At the same time, the measures taken to ensure information security shall not complicate the achievement of the Company's statutory objectives or increase the labor intensity of information processing technological procedures;
7) effective implementation of the adopted protective measures;
8) flexibility of protection means to ensure the Company's information security in the event of possible changes in external conditions and requirements over time;
9) improvement of information protection measures and tools based on continuity of organizational and technical solutions, analysis of IS functioning, taking into account changes in methods and means of information interception and impact on components, regulatory protection requirements, and experience gained by both domestic and foreign organizations in this field;
10) continuity of secure operation principles;
11) mandatory and timely detection and suppression of attempts to violate established information security rules;
12) clear definition of functional objectives and information security objectives in documents in order to avoid ambiguity in organizational structure, personnel roles, approved policies, and the inability to assess the adequacy of implemented security measures;
13) assignment of personal responsibility for ensuring the security of information and its processing system to each employee within the limits of their authority. According to this principle, the distribution of employees' rights and duties is structured in such a way that, in the event of any violation, the circle of responsible individuals is clearly known or minimized;
14) ensuring the availability of services and solutions for clients and counterparties within the timelines established by relevant agreements and/or other documents;
15) observability and the ability to assess the state of information security, where the effect of applied protective measures is clearly observable (transparent) and can be evaluated by a specialist with appropriate authority;
16) classification of processed information and determination of its level of importance in accordance with legislation;
17) ensuring the capability to measure protection effectiveness, including the presence of information security metrics and indicators that allow assessment of the effectiveness of measures and detection of deviations;
18) continuous improvement of the security management system based on incident analysis, internal audits, monitoring results, and changes in regulatory requirements.

4. Personnel Policy for Ensuring Information Security

4.1. The functions and responsibilities of personnel are clearly defined in job descriptions and communicated to candidates during the hiring process.

4.2. Employees sign the terms of the employment contract, which establish their responsibilities and the Company's responsibilities regarding information security.

4.3. Employees and representatives of third-party organizations who use the Company's information processing facilities sign an agreement in accordance with information security requirements in order to reduce risks of theft, fraud, misuse of equipment, and information security threats.

4.4. A non-disclosure agreement is signed by the employee, contractor, or third-party user before access to information processing facilities is granted.

4.5. Screening of all candidates for permanent employment is carried out in accordance with applicable labor legislation while ensuring the confidentiality of personal data. The following information provided by the candidate is subject to verification:

1) references from previous workplaces, if available;
2) the applicant's résumé;
3) documents regarding education and professional qualifications;
4) identity documents;
5) other information requiring clarification.

4.6. Information on all employees hired for permanent positions is collected and processed in accordance with applicable labor legislation.

4.7. Employees are familiarized with the requirements of this Policy and all documentation related to information security in order to increase awareness, provide information on incident response procedures, and prevent incidents. It is necessary to ensure the return of all assets (computer equipment, official documents, electronic media, etc.) used by employees upon termination of their employment contract, and in cases where an employee has used personal equipment, to ensure the transfer of information to the manager of the relevant department (responsible specialist) or the removal of information from the equipment using non-recoverable methods.

4.8. Access rights to information systems and resources are revoked upon termination of the employee's employment contract (dismissal) or are subject to review when their duties and functions change.

4.9. User accounts of employees whose work activities have ceased due to long-term business travel, leave (more than 60 days), or upon termination of their employment contract are blocked.

4.10. Information about employees and clients is collected and processed in accordance with GDPR, labor legislation, and the Company's internal data protection policies.

4.11. All employees are required to undergo regular information security training to prevent incidents and increase awareness.

5. External Information Exchange

5.1. External information exchange with consumers, suppliers, and other interested parties of the Company is carried out through the exchange of letters via courier services, postal mail, and/or via email, electronic document management systems where such method of information exchange is defined as permissible.

5.2. The exchange of confidential information is carried out using cryptographic data protection and electronic signatures, if this is required by legislation or internal requirements.

5.3. Information security in relationships with suppliers is ensured within the framework of contracts with suppliers, where information security requirements are described.

6. Information Security Incident Management

6.1. The Company implements a formalized process for managing information security incidents.

6.2. All employees are required to immediately report identified or suspicious incidents to the Information Security Officer.

6.3. The Information Security Officer documents incidents, conducts investigations, and ensures corrective actions.

6.4. The results of investigations are used to improve the ISMS.

6.5. Notifications to regulators are carried out in accordance with legislation and internal procedures.

7. Review of the Information Security Policy

7.1. The provisions of the Company's Information Security Policy require regular review and adjustment at least once a year according to the plan.

7.2. An unscheduled review of the Security Policy is conducted in the event of:

1) significant changes in the Company's information systems;
2) changes in legislation;
3) changes in the organizational structure;
4) information security incidents;
5) changes in the ICT structure affecting digital operational resilience;
6) the emergence of new DORA or ISO 27001 requirements;
7) significant changes in supplier-related risks.

7.3. When making changes, the following input data are taken into account:

1) results of the information security audit and previous audits;
2) recommendations of independent information security experts;
3) significant threats and vulnerabilities of the information system;
4) reports on information security incidents;
5) recommendations of government authorities;
6) feedback from interested parties;
7) results of independent reviews;
8) status of preventive and corrective actions;
9) results of previous management reviews;
10) performance and compliance with the Information Security Policy;
11) changes that may affect the Company's approach to information security management, including changes in organizational scope, business circumstances, resource availability, contractual/regulatory requirements, and the technical environment;
12) trends related to threats and vulnerabilities.

7.4. The review of the Policy is carried out by specialists responsible for its development and implementation and includes assessing possibilities for improving its provisions and the information security management process in accordance with changes.

7.5. The result of the management review of the Information Security Policy is the improvement of the organizational approach to information security management, controls and their objectives, allocation of resources and responsibilities, etc.

7.6. The review of the Information Security Policy is carried out in accordance with legislation.

7.7. This Policy is subject to mandatory review based on the results of information security risk analysis and assessment for the information system and is updated as necessary.

7.8. Responsibility for making amendments and additions to this Policy is assigned to the Technical Director.

7.9. The revised Information Security Policy is approved by the Company's General Director.

8. References to Internal ISMS Policies and Documents

8.1. This Policy is a top-level document and is implemented through internal regulations, policies, and procedures that establish detailed organizational and technical measures for ensuring information security, digital operational resilience, and compliance with the requirements of ISO/IEC 27001:2022 and Regulation (EU) 2022/2554 (DORA).

8.2. The internal ISMS documents cover the following areas:

8.2.1. **ISMS Management and Organizational Procedures.** Documents regulating information security management, risk analysis and assessment, internal audits, management of nonconformities, changes, business continuity and disaster recovery, as well as general organizational measures.

8.2.2. **Asset Management and Technical Security.** Documents regulating identification, classification, and accounting of IT assets, access management, software usage, backup, network device management, and operational requirements.

8.2.3. **Documents on Access Management, Authentication, and IT Operations.** Documents establishing rules for remote work, use of IT resources, authentication, secure development, antivirus protection, and operation of user devices.

8.2.4. **Documents on Incident Management and Digital Operational Resilience.** Documents regulating the procedure for incident management, personnel actions during incidents, business continuity, disaster recovery, and support of critical or important functions.

8.2.5. **Documents on Cryptographic Protection and Data Protection.** Documents establishing the procedure for the use of cryptographic means, personal data protection, and confidentiality requirements.

8.2.6. **Documents on Supplier and External Service Management.** Documents defining requirements for working with ICT suppliers, third-party ICT risks, the use of cloud services, and secure information exchange.

9. Regulatory References

9.1. Ustawa o krajowym systemie cyberbezpieczeństwa (National Cybersecurity System Act).

9.2. Cybercrime Directive. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.

9.3. NIS Directive. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

9.4. ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements.

9.5. DORA — Digital Operational Resilience Act. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

9.6. GDPR — General Data Protection Regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.