Version valid from:12.08.2025

INFORMATION SECURITY POLICY

1. PURPOSE

1.1. This Information Security Policy of UAB "Crowdpear" (hereinafter - Policy) establishes the framework for protecting information and communication technology assets of Crowdpear UAB (hereinafter - Company). The purpose of the Policy is to implement, maintain and continuously improve information security within the Company. This policy serves as the cornerstone document that defines the Company's approach to information security management and provides the basis for all information security procedures and standards.

2. SCOPE

2.1. This Policy applies to the management and use of all of the Company's information and communications technology assets (hereinafter - ICT Assets), regardless of the location or format of the assets, including but not limited to all information systems, applications, infrastructure, business processes and physical premises related to the processing, storage and transmission of information. All employees, contractors, consultants, temporary workers and third party entities who have access to or responsibility for the Company's ICT assets must comply with the Policy.

3. GENERAL PROVISIONS

3.1. The Policy considers the current state and future prospects of information technology development within the Company, the objectives and tasks for their operation, operating modes, and includes a list of security threats to the objects and subjects of the Company's information relationships.

3.2. All terms and abbreviations used in this Policy are specified in the *'Terminology Guide for DORA and ISO 27001 Compliance by Crowdpear UAB'*.

3.3. The requirements of this Policy apply to all structural divisions of the Company.

3.4. The Policy serves as the methodological basis for:

1) Establishing and maintaining a unified policy for ensuring information security within the Company.
2) Organizing the identification of information subject to protection, substantiating its confidentiality level, and documenting it in appropriate lists.
3) Making managerial decisions and developing practical measures to implement the information security policy.
4) Developing a set of coordinated measures aimed at identifying, countering, and eliminating the consequences of various types of information security threats.
5) Coordinating the activities of the Company's structural units when developing, improving, and operating information technologies while ensuring compliance with information security requirements.
6) Preparing proposals for improving the legal, regulatory, technical, and organizational frameworks for ensuring information security within the Company.

3.5. The protection of information resources is carried out within the framework of the Information Security Management System (ISMS) that complies with:

- The requirements of the international information security standard ISO/IEC 27001:2022.
- The requirements of DORA (Digital Operational Resilience Act) Regulation (EU) 2022/2554, ensuring the resilience, security, and integrity of ICT systems and processes.
- The requirements of legislation, regulatory, and contractual obligations of the Company regarding information security.
- This *Policy* of the Company.

3.6. The scope of the Company's ISMS includes the successful provision, support, and maintenance of software development services (see the document "*Statement of Applicability*").

3.7. Director of the Company is responsible for ensuring information security within the Company. Employees must be properly familiarized with the ISMS documents and comply with the requirements set out therein.

3.8. This Policy is subject to regular review at least once every two years.

3.9. The Policy aims to achieve the following key objectives:

1) Protecting the integrity of information used and processed;
2) Maintaining the confidentiality of critical information, as defined in the *ICT Asset Management Policy*.

3) Ensuring the availability of information processed in the Company's information systems.
4) Guaranteeing the continuity of key business processes operating.

3.10. To achieve these objectives, the following tasks must be addressed:
1) Ensuring active management involvement in the Company's Information Security management.
2) Raising employee awareness of risks associated with information resources.
3) Clearly assigning responsibilities and duties to employees for ensuring Information Security.
4) Implementing access control for employees to the Company's hardware, software, and information resources.
5) Logging user activities in system journals when using network resources.
6) Protecting the Information Security functioning process from external interference.
7) Controlling the integrity of software tools and their execution environment, restoring it in case of disruption, and protecting systems from malicious code introduction.
8) Protecting restricted information and personal data from leakage through technical channels during processing, storage, and transmission via communication channels.
9) Ensuring user authentication for Information Security and resources.
10) Timely identification of Information Security threats, as well as causes and conditions contributing to damage.
11) Creating conditions for minimizing and localizing damage caused by unauthorized actions of individuals or organizations.
12) Applying the measures provided in the legislation or local acts in case of Information Security Policy violations.
13) Eliminating the consequences of Information Security violations.
14) Developing and implementing rules and instructions for ensuring Information Security, as well as monitoring compliance by Company employees.
15) Implementing measures for assessing, managing, and minimizing information risks (see documents: “*ICT Risk Assessment Methodology*"", “*Incident Response Plan*", “*Personal Data Security Breach Management Policy*”).
16) Continuously improving the ISMS.

4. RESPONSIBILITIES AND OBLIGATIONS

4.1. Management is directly involved in addressing issues related to Information Security in accordance with the Company's (business) objectives, laws, and regulations.

4.2. Management supports the established Information Security level by implementing the ISMS and by assigning responsibilities and duties to personnel for its maintenance.

4.3. Information Security Officer:
1) Formulates, reviews, and prepares the Information Security Policy, as well as monitors its implementation effectiveness.
2) Ensures clear governance and active support for Information Security initiatives.
3) Ensures adequate resources are allocated to the information security program.
4) Coordinates Information Security control measures across the Company.
5) Approves employee roles and responsibilities related to Information Security through job descriptions, order projects, etc.
6) Approves of the organization's risk appetite and tolerance levels related to information security.
7) Initiates plans, and programs to raise Information Security awareness, defines the need for user and administrator training in security methods and procedures, and specifies responsibilities for installing and maintaining software and hardware.
8) Determines the need for internal or external specialist consultations on Information Security issues and overseas the implementation of recommendations Company-wide.
9) Clearly establishes the responsibility of unit managers for various assets and security processes. The details of these responsibilities are documented, and authority levels are clearly defined and documented (see Material Responsibility Agreement).
10) Initiate investigations into breaches of information security policies.
11) Eliminates the consequences of Information Security breaches.
12) Promptly identifies and prevents attempts to violate established Information Security rules.

4.4. To stay informed about evolving cybersecurity threats, regulatory developments, and industry best practices, the Company maintains active engagement with relevant professional communities, industry groups, and cybersecurity associations. The Information Security Officer is responsible for overseeing such interactions and integrating key insights and recommendations into the Information Security Management System (ISMS).

4.5. The control of user activities, each security measure, and any protection object is carried out using operational control and logging tools (see the document "*Access Control Policy").* This control encompasses both unauthorized and authorized user actions.

4.6. Employees are informed about their responsibilities for protecting information in accordance with their job functions, as well as the consequences for potential violations. The Information Security Officer is responsible for providing this information and ensuring that employees are properly introduced to security requirements relevant to their roles.

4.7. Infrastructure administrators are subject to administrative or other liabilities for violating the Information security policy, as prescribed by applicable law. Responsibilities of infrastructure administrators are defined in the "*Infrastructure Administrator Guidelines*" Specifically, infrastructure administrators ensure the continuous operation of the network and are responsible for implementing the technical measures necessary to enforce the Information security policy.

5. CORE PRINCIPLES OF ENSURING INFORMATION SECURITY

5.1. The main principles of ensuring Information Security in the Company are as follows:

1) Compliance with legal requirements – adhering to applicable laws and regulations.
2) Alignment with international and national standards – ensuring compliance with Information Security standards effective in the country.
3) Continuous analysis of the information environment – identifying vulnerabilities in ICT assets.
4) Identifying cause-and-effect relationships – understanding potential problems and predicting their development accurately.
5) Assessing the impact of identified issues.
6) Comprehensive use of protection methods – employing physical, organizational, technological, and legal measures to secure computer systems, covering all significant threat channels without weaknesses at component junctions. Protective measures should not hinder statutory goals or increase the complexity of information processing.
7) Effective implementation of protective measures.
8) Flexibility of protection measures – adapting Information Security measures to changes in external conditions and requirements over time.
9) Continuous improvement of Information Security measures – leveraging organizational and technical advancements, analyzing Information Security performance, incorporating updated methods of information interception and protection, adhering to regulatory requirements, and adopting best practices from domestic and international organizations.
10) Continuity of secure operations – maintaining uninterrupted adherence to Information Security principles.
11) Timely identification and prevention of violations – proactively detecting and addressing breaches of established Information Security rules.
12) Clear definition of Information Security objectives – avoiding ambiguity in the organizational structure, staff roles, policies, and the evaluation of protective measures' adequacy by documenting functional and security goals.
13) Accountability for Information Security – assigning personal responsibility for IS and information processing systems to each employee within their authority. The distribution of rights and responsibilities ensures that in the event of a violation, the responsible party is clearly identified.
14) Service availability – ensuring services and systems are accessible to clients and partners within the timeframes stipulated in agreements, contracts, or other documents.
15) Observability and measurability of Information Security – providing transparency and allowing the effectiveness of protective measures to be assessed by authorized specialists.
16) Information classification – categorizing processed information and determining its importance level in accordance with legislation.

6. PERSONNEL POLICY FOR ENSURING INFORMATION SECURITY

6.1. Employee roles and responsibilities are clearly defined in the internal documents of the Company..

6.2. Employees sign employment contracts that outline basic responsibilities regarding Information Security. More specific Information Security responsibilities are defined in internal policies and regulations, with which employees must be introduced by the Information Security Officer.

6.3. Employees and representatives of third-party organizations using the Company's information processing tools sign agreements in compliance with Information Security requirements to mitigate risks of theft, fraud, misuse of equipment, and information security threats.

6.4. A non-disclosure agreement (NDA) is signed by employees, contractors, or external users before access to information processing tools is granted.

6.5. Background checks for all candidates for permanent employment are conducted in accordance with applicable laws, ensuring confidentiality of personal data. The following information provided by candidates is subject to verification:

1) References from previous employers, if available and if candidate agreed.

2) The candidate’s CV.
3) Education and professional qualification documents.
4) Identification documents.
5) Other information requiring clarification.

6.6. Information on all employees hired for permanent positions is collected and processed in compliance with GDPR, laws, and the Company’s internal policies and regulations regarding data collection, storage, usage, and protection, as outlined in the relevant Crowdpear UAB documentation.

6.7. Employees are informed of the requirements of this Policy and all Information Security related documentation by the Information Security Specialist to raise awareness, educate them about incident response procedures, and prevent potential breaches. Measures are in place to ensure the return of all ICT assets (e.g., computer equipment, official documents, electronic media) used by employees upon termination of their employment. In cases where personal equipment is used, employees must either transfer information to the head of the respective department (or a responsible specialist) or give it for Information Security Officer to delete it using methods that prevent recovery (see the document “*ICT Asset Management Policy*” and “*Access Control Policy*”). The process of information deletion must be verified and documented through a formal agreement.

6.8. Access rights to information systems and resources are revoked upon termination of an employee’s employment contract or reviewed when their duties or functions change.

6.9. Employee accounts are deactivated upon termination of employment due to extended business trips, leave (over 60 days), or the end of their employment contract.

7. EXTERNAL INFORMATION EXCHANGE

7.1. External information exchange with customers, suppliers, and other stakeholders of the organization is conducted through courier services, postal mail, and/or via email and electronic document management systems where these methods are deemed acceptable for information exchange by the Information Security Officer in accordance with the Company's Information Security Policy and regulatory requirements.

7.2. Information about security in supplier relationships is addressed within supplier contracts. These contracts specify Information Security requirements to mitigate risks associated with supplier access to the Company's ICT assets, including processing, storage, transmission, and interaction processes, as well as the provision of IT infrastructure components. They also outline measures to address Information Security risks related to information and communication technology services and the product supply chain.

8. INFORMATION SECURITY POLICY STATEMENTS

8.1. Risk Management

8.1.1. The Company shall implement and maintain a comprehensive risk management framework that identifies, assesses, and treats information security risks in alignment with business objectives and stakeholder requirements.

8.1.2. Risk assessments shall be conducted at planned intervals, at least annually, and whenever significant changes to the business environment, technology infrastructure, or threat landscape occur.

8.1.3. The risk assessment methodology shall consider both threats and vulnerabilities, evaluate potential impacts to confidentiality, integrity, authenticity and availability of information, and document the rationale for risk treatment decisions.

8.1.4. Risk treatment plans shall be developed and implemented based on the organization's defined risk acceptance criteria, with regular monitoring and reporting of risk treatment effectiveness to relevant stakeholders.

8.2. Access Control Management

8.2.1. The Company shall implement and maintain a comprehensive access control framework based on the principles of least privilege and need-to-know.

8.2.2. All access to information systems and data shall be controlled through formal user registration and deregistration procedures.

8.2.3. Access rights shall be granted only after documented approval from both the resource owner and the information security team.

8.2.4. Multi-factor authentication shall be mandatory for all remote access and privileged account access.

8.2.5. Regular access reviews shall be conducted at least quarterly, with immediate revocation of access rights upon termination or role change.

8.2.6. The Company shall maintain audit logs of all access control changes, with automated alerts for suspicious access attempts or unauthorized privilege escalations.

8.2.7. Password policies shall enforce strong authentication requirements including minimum length, complexity, and regular password changes, with technical controls preventing password reuse.

8.3. ICT Asset Management and Classification

8.3.1. The Company shall maintain a comprehensive inventory of all ICT assets, including both physical and logical assets, with clearly assigned ownership and defined security responsibilities, as outlined in the *ICT Asset Management Policy*. The Information Security Officer is responsible for overseeing ICT asset classification and security compliance, while the IT Support maintains inventory records and ensures lifecycle management.

8.3.2. All ICT assets shall be classified according to their sensitivity, criticality, and legal requirements using the Company's defined classification scheme. ICT asset owners shall be responsible for ensuring appropriate handling procedures are implemented based on the asset's classification level.

8.3.3. The asset inventory shall be reviewed and updated at least once a year, with formal reconciliation processes to identify and address any discrepancies. Media handling procedures shall be implemented to protect against unauthorized disclosure, modification, or destruction throughout the ICT asset lifecycle, including secure storage, transmission, and disposal methods.

8.4. Information Security Incident Management

8.4.1. The Company shall implement and maintain an information security incident management process to ensure a consistent and effective approach to the management of information security incidents.

8.4.2. All employees and contractors shall be required to report any observed or suspected security incidents immediately through defined reporting channels.

8.4.3. Lessons learned from security incidents shall be documented and used to improve security controls and incident response procedures.

8.4.4.The Company ensures structured communication with relevant regulatory and law enforcement bodies. The Information Security Officer, or other appointed representatives are responsible for responding to official requests, regulatory audits, and notifications related to security incidents in accordance with applicable laws.

8.5. Cryptography and Key Management

8.5.1. The Company shall implement and maintain cryptographic controls to protect the confidentiality, integrity, and authenticity of information throughout its lifecycle.

8.5.2. All sensitive data shall be encrypted both in transit and at rest using industry-standard encryption algorithms and protocols.

8.5.3. The Company shall maintain a formal key management policy covering the entire cryptographic key lifecycle, including generation, distribution, storage, use, archival, and destruction.

8.5.4. Regular assessments of cryptographic implementations shall be conducted to ensure alignment with current industry standards and best practices, with documented procedures for transitioning to stronger cryptographic controls when required.

8.6. Operations Security

8.6.1. The Company shall establish and maintain documented operating procedures for all information processing facilities to ensure correct and secure operations.

8.6.2. Change management procedures shall be implemented to control all changes to information processing facilities and systems, with appropriate testing, documentation, and approval requirements.

8.6.3. Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to operational systems. System and security monitoring controls shall be implemented to detect unauthorized information processing activities, with regular review and analysis of system logs.

8.6.4. Protection against malware shall be implemented through regular security awareness training for all users.

8.6.5. The Company shall assess, approve, and securely integrate new technologies in accordance with risk management, compliance, and security best practices before implementation. All new technologies must be evaluated for potential security risks, operational impact, and regulatory compliance requirements, including DORA and ISO 27001.

8.7. Supplier Relationships

8.7.1. The Company shall establish and maintain information security requirements for relationships with suppliers to mitigate risks associated with supplier access to organizational assets.

8.7.2. Formal contracts or agreements shall include specific security requirements, including incident reporting obligations, data protection requirements, and right-to-audit clauses, as outlined in the Third-Party Risk Management Policy. Any additional security clauses must align with Company policies and regulatory requirements.

8.7.3. Supplier service delivery shall be regularly monitored and reviewed, with formal assessments of security controls implemented by suppliers conducted at least annually.

8.7.4. Changes to supplier services shall be managed through formal change management procedures, with impact assessments conducted for significant changes.

8.8. Ownership of Intellectual Property

8.8.1. Any intellectual property, including but not limited to software, source code, technical documentation, designs, research data, business strategies, and patents, created, developed, or improved by employees, contractors, or third parties using Company resources, time, or within the scope of their professional duties shall be the sole property of Company, unless otherwise stated in a written agreement.

8.8.2. Employees, contractors, and third-party service providers are strictly prohibited from using, copying, modifying, or disclosing any intellectual property of the Company for personal use, external distribution, or unauthorized commercial purposes without explicit written approval from the Company's management. Upon termination of employment or contract, all intellectual property, including source files, documents, and access credentials, must be returned or deleted as instructed by the Company.

9. REVIEW OF THE INFORMATION SECURITY POLICY

9.1. This policy shall be reviewed:

1) At least once in two years
2) When significant organizational changes occur
3) After major security incidents
4) When new threats or vulnerabilities are identified
5) When regulatory requirements change
6) When technology changes impact security requirements.

9.2. The following inputs are considered when revising the Policy:

1) Information sustem audit results, including results from previous audits.
2) Recommendations from independent Information Security experts.
3) Significant threats and vulnerabilities in information systems.
4) Reports on Information Security incidents.
5) Recommendations from government authorities.
6) Feedback from stakeholders.
7) Results of independent reviews.
8) The status of preventive and corrective actions.
9) Results from previous management reviews.
10) Process performance and compliance with the *Information Security Policy*.
11) Changes affecting the Company's Information Security management approach, including organizational scope, business conditions, resource availability, contractual or regulatory requirements, and technical environments.
12) Trends in threats and vulnerabilities.
13) Reported Information Security incidents.
14) Recommendations from independent parties.

9.3. The Policy review is conducted by the Information Security Officer, who is responsible for its development and implementation, including an evaluation of potential improvements to the Policy provisions and Information Security management processes in line with changes.

9.4. The outcome of the review of the Information Security Policy includes the refinement of the organizational approach to Information Security management, adjustments to controls and their objectives, resource allocation, and assignment of responsibilities.

9.5. The Policy review is conducted in compliance with applicable legislation.

9.6. Responsibility for making changes and additions to this Policy lies with the Information Security Officer.

9.7. The revised *Information Security Policy* is approved by the Company's Director.

10. REGULATORY REQUIREMENTS

10.1. Law of the Republic of Lithuania on Legal Protection of Personal Data

10.2. Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (Text with EEA relevance)

10.3. 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 (hereinafter - DORA) (Text with EEA relevance)

10.4. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems (hereinafter - Cybercrime Directive).

10.5. 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 (hereinafter - NIS Directive).

10.6. 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 (hereinafter - GDPR General Data Protection Regulation).

10.7. Lietuvos Respublikos kibernetinio saugumo įstatymas Cybersecurity law of the Republic of Lithuania

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