KOVOPROJEKTA
ENGINEERS & CONTRACTORS

CYBERSECURITY POLICY

PURPOSE OF THE POLICY

The purpose of this policy is to establish principles and rules for the safe and effective use of digital technologies to protect data, ensure process continuity, and minimize cyber risks. This document also supports the ethical and responsible use of artificial intelligence within the company and ensures that all employees adhere to the principles and procedures of acceptable AI tool usage. In case of violations, the policy defines appropriate disciplinary measures as well as specific steps for impact mitigation, security restoration, and prevention of recurrence.

SCOPE OF APPLICATION

This policy applies to:

- All company employees regardless of job position, as well as external collaborators, contractors, and partners who access the company's digital technologies, data, or systems in the course of their activities.
- All digital resources, systems, and tools used in design, project management, communication, data sharing, and AI implementation – including company devices (PCs, mobile phones, servers), cloud services, communication tools, specialized software, and AI platforms.
- Any information not explicitly marked as the property of other parties and transmitted or stored within the company's IT resources (including emails, text and chat messages, and files).
- All systems, tools, or services including those equipped with generative AI (e.g., ChatGPT, Copilot, etc.) that generate textual, visual, or other content based on input data.

The principles are binding both when working on company premises and remotely (home office, business trips), and also apply to personal devices used under the BYOD (Bring Your Own Device) model if used for work purposes.

EXCEPTIONS TO THE POLICY

Exceptions to this policy may be granted only in justified cases:

- Based on written approval from the responsible authority (company management);
- To the extent necessary for operational efficiency, security testing, development, or specific project requirements;
- After risk assessment and evaluation of impacts on security, personal data protection, and legal compliance.

Each exception must be properly documented, including the reason, scope, validity period, and responsible person. Exceptions must not be considered as a precedent and must not compromise the integrity or security of company systems or data.

Exceptions classified as high-risk will be recorded in the company's risk register.

DEFINITIONS

For the purposes of this policy, the following definitions apply:

- **Digital technologies** – Any hardware or software tools, systems, or devices that enable data processing, storage, transmission, or sharing (e.g., computers, servers, mobile devices, cloud services, CAD/BIM tools, etc.).
- **Artificial Intelligence (AI)** – Technologies capable of performing tasks that typically require human intelligence, including machine learning, generative models, pattern recognition,

natural language analysis, and decision-making systems. This includes tools like ChatGPT, Copilot, and predictive design systems.
- **AI systems –** All software tools or services equipped with AI functionality, especially those that generate texts, images, designs, analyses, or decisions without human intervention.
- **Confidential information –** Any information whose unauthorized disclosure, loss, or misuse could harm the interests of the company or third parties, including personal data, trade secrets, technical documentation, project designs, financial data, client contacts, etc.
- **Acceptable use –** The use of digital technologies and AI tools in accordance with this policy, ethical and legal standards, and the strategic goals of the company.
- **BYOD (Bring Your Own Device) –** A model where employees use their own devices (e.g., laptop, mobile phone) for work tasks, which are also subject to this policy.
- **Phishing –** A social engineering technique where an attacker attempts to obtain confidential information (e.g., login credentials, financial data) fraudulently, usually via fake emails, websites, or messages**.**
- **Compromised account –** A user account that has been accessed by an unauthorized third party (e.g., hacker), often due to weak passwords, phishing attacks, or insufficient security.
- **Data anonymization** – The process of modifying data so that specific individuals can no longer be identified, even indirectly, thereby eliminating the obligation to protect such data under personal data protection laws (e.g., GDPR).
- **Secure communication –** Any exchange of information protected by encryption or other means to prevent unauthorized access or data leakage (e.g., use of VPN, encrypted emails, etc.).
- **Cybersecurity incident / Security incident –** Any event that compromises the confidentiality, integrity, or availability of systems and data, including unauthorized access attempts, malware distribution, or data loss.
- **Company data –** All information created, obtained, or stored in the course of company activities, regardless of format (text, image, drawing, audio) or medium (cloud, hard drive, paper document), which holds value for company operations or its clients.
- **Ethical use of AI –** Deployment and use of AI tools in a manner that respects human dignity, transparency, non-discrimination, privacy protection, and accountability for AI-generated outputs.
- **Roles and responsibilities –** Specific duties assigned to individual employees or roles within the company in relation to fulfilling the principles of this policy (e.g., IT administrator oversees system security, project manager ensures proper data sharing within projects, etc.).
- **Minimum access principle –** A principle whereby employees only have access to the data and systems necessary for performing their specific job duties.
- **Security measures –** A set of technical, organizational, and procedural steps aimed at protecting the company from cyber threats, data loss, misuse of tools, or operational disruption.
- **Publicly available AI systems –** Online AI tools operated by third parties and accessible to the general public without a contractual relationship with the company. Typically, full control over how input data is processed, stored, or used is not guaranteed.

ROLES AND RESPONSIBILITIES

All company employees are responsible for complying with this policy. Key roles and their responsibilities are defined as follows:

- **Company Management**
  Approves this policy, grants any exceptions, and ensures that the principles align with the overall company strategy.
- **IT Department / System Administrator**
  Ensures the secure operation of digital technologies, regular updates and system monitoring, manages access rights, and provides technical support.

- **Project Managers**
  Ensure that project documentation and team communication are conducted in a secure manner and that the use of digital technologies complies with this policy.
- **Security and Compliance Officer (if appointed)**
  Coordinates training, assesses risks, monitors compliance with the principles, and maintains a register of security incidents and exceptions.
- **Employees**
  Are required to act in accordance with this policy, complete training, and promptly report any security incidents or violations of the rules.

PRINCIPLES OF ACCEPTABLE USE OF DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE SYSTEMS

Employees are required to use digital technologies and artificial intelligence tools in accordance with the following principles:

1. Secure Login and Account Management

- Use strong and unique passwords.
- Do not log into company services from public or untrusted devices.
- Access details are personal and must not be shared.

2. Working with Data and Documents

- Work files may only be stored in approved storage locations.
- It is prohibited to send project documentation or other confidential information via public platforms or unsecured communication channels.
- Confidential information must be protected against misuse, unauthorized access, and loss.

3. Use of AI Tools

- AI tools may only be used for purposes aligned with assigned work and in accordance with this policy.
- It is prohibited to input sensitive or confidential company information into publicly available AI systems (e.g., without prior approval or protective measures).
- AI-generated outputs must always be verified – the employee is responsible for their accuracy and appropriateness.
- AI-generated content that is shared or published must be clearly marked as AI output (e.g., with a watermark or note in the text), especially when presented on behalf of the company.

4. Use of Devices and Applications

- Software installation may only be performed through approved sources and in cooperation with the IT department.
- Personal devices under the BYOD model must be secured and meet company requirements.
- Company devices must not be used for illegal, inappropriate, or unethical purposes.

5. Communication and Company Representation

- When using digital and AI tools to create texts, presentations, or messages, the company's reputation must not be harmed, false information must not be disclosed, and communication ethics must not be violated.
- It is prohibited to generate or distribute AI outputs that may be misleading, deceptive, or manipulative.

6. Training and Awareness / Raising Awareness

- Every employee is required to undergo regular training on IT security, acceptable AI usage, and data protection.
- Lack of knowledge of this policy's rules is not an excuse for violations.

7. Data Evaluation and Feedback

The company systematically evaluates data related to the use of digital technologies and AI systems for the purpose of:

- Monitoring compliance with this policy,
- Identifying security incidents and risky behavior,
- Improving the efficiency of tools and work processes,
- Ensuring responsible and ethical use of AI.

Evaluation is carried out in accordance with legal regulations, especially GDPR, with emphasis on employee privacy protection. Data is analyzed in aggregated and anonymized form if the nature of the analysis allows it.

Data Sources:

- Access and activity logs in systems,
- Metadata from AI tool usage (e.g., frequency, types of requests),
- Results of internal audits and training,
- Feedback from employees and users.

Feedback and Corrective Measures:

- Based on evaluations, training, changes in access rights, or technical measures may be proposed.
- Serious deviations from the policy are handled in accordance with disciplinary procedures.
- Employees may provide feedback on the functioning of systems and the policy.

Examples of Acceptable and Unacceptable Use:

Area	Acceptable behavior	Unacceptable behavior
Login and passwords	Using of strong passwords, lock the screen when leaving	Sharing passwords, writing them down on paper, leaving devices unattended
Working with AI	Using AI to generate proposals, automate reports after verifying outputs	Entering confidential information into public AI platforms, uncritically accepting outputs
Data storage	Saving to approved company storage with access control	Storing files on unencrypted flash drives, personal accounts, freely accessible storage
Communication	Using encrypted channels, representing the company in professional language	Sending documents via personal email, publishing AI output with the company logo without checking
Use of devices	Working on secure company (or approved) devices	Installing unapproved applications, connecting unverified USB devices
Ethics and law	Respecting copyright, human rights, and equality when using AI	Generating AI outputs that could be misleading, discriminatory, or inappropriate

KOVOPROJEKTA
ENGINEERS & CONTRACTORS

SECURITY INCIDENT AND POLICY VIOLATION MANAGEMENT

All company employees are required to actively cooperate in detecting and resolving security incidents and any violations of this policy. The goal is to minimize the impact on the company, clients, and partners and to prevent recurrence. The company considers the timely detection and responsible resolution of security incidents to be a key element in protecting its data, systems, and client trust. Every employee has a responsibility to report incidents in a timely manner and actively contribute to their resolution.

1. Reporting obligation / Incident reporting
An employee who notices a security incident (e.g., data leak), suspicious activity (e.g., suspicious behavior of an AI tool, phishing), or a policy violation is required to report this immediately to the responsible person (e.g., manager, IT administrator).

2. Incident assessment
Each reported incident is immediately recorded, analyzed, and classified according to type, severity, and potential impact. In serious cases, the incident may be handled by an ad hoc group composed of representatives from management, IT, and other relevant departments or external specialists. In the event of an impact on third parties (e.g., clients), timely and transparent communication is ensured.

3. Measures
Based on the evaluation of the incident, the following measures may be taken:

- temporary technical measures (e.g., access restrictions, isolation of equipment),
- restoration and securing of data or systems,
- updating of processes and procedures,
- individual corrective measures against responsible persons.

4. Disciplinary proceedings
Violation of this policy may be grounds for disciplinary proceedings, including a written warning, restriction of access rights, or, in serious cases, termination of employment in accordance with labor law regulations.

5. Recording and instruction
Each incident is documented in terms of causes, consequences, and measures taken. It is also recorded in the company's risk register if appropriate and adequate.
The company conducts regular incident analysis and uses the findings to strengthen prevention, raise awareness, and improve internal processes.

ETHICAL PRINCIPLES IN THE FIELD OF CYBER SECURITY

The company is committed to an ethical and responsible approach to cybersecurity. The goal is to ensure the trust of employees, partners, and clients and to promote a culture of digital responsibility.

1. Respect for privacy and confidentiality
Access to data, systems, and network resources must always be justified, proportionate, and transparent. Employees with access to confidential information are required to maintain the highest level of confidentiality and act in accordance with legal regulations and internal rules.

2. Responsible use of privileges
Enhanced privileges (e.g., administrator rights, access to source codes or audit logs) must not be abused or shared. Everyone must act only within the scope of their authority and always with regard to security and ethical implications.

3. Prevention of misuse and manipulation
It is prohibited to perform any activities that could jeopardize the security of systems, data, or persons - including misuse of access, circumvention of technical measures, or manipulation of artificial intelligence outputs.

4. Transparency and awareness
In the event of a threat, incident, or vulnerability being detected, employees are required to act immediately and inform the relevant person in charge. Concealing or downplaying security risks is considered serious misconduct.

5. Promoting a fair and secure digital environment
Employees actively participate in creating a culture of cyber responsibility - they adhere to the principles of this policy, respect other users, and contribute to a secure, fair, and trustworthy corporate digital environment.

6. Ethical principles for the use of artificial intelligence AI

- -It must not be used in a way that would restrict freedom of choice, discriminate against individuals or groups, or otherwise violate human rights.
- -The company ensures that algorithms and models are not biased and do not lead to unfair treatment. The use of AI is subject to regular review in terms of equal access.
- -The company only implements verified AI systems that meet security, transparency, and risk management requirements.
- -The company takes into account the environmental impact of using AI (e.g. power consumption when training models) and prefers solutions with a lower ecological footprint.

FINAL PROVISIONS

This policy does not replace or supersede any other existing internal regulations.

1/10/2025