

Topchik N.V.

Information Security Policy

Version Control

Version	Date	Company	Description
1.0	2026.05.13	Topchik N.V.	Policy creation

Contents

1. General Provisions	4
2. Purpose and Objectives	4
3. Goals and Objectives of the Information Security	4
4. Main Directions of Information Security Provision	4
5. Use of Information Protection Measures	5
6. Personal Data Protection	5
7. Information Security Threats	5
8. Principles of Information Security Provision	6
9. Information Security Risk Management	6
10. Personnel Management Processes	6
11. Access Management	7
12. Secure Software Development	7
13. Security Testing	7
14. Information Security Incidents	8
15. Information Classification	8
16. Collaboration with Third Parties	9
17. Responsibility	9

1. General Provisions

1.1. The Company acknowledges the value of information provided to it by business clients, employees, founders, counterparties, and other stakeholders, and applies all reasonable measures to protect such information. Information security and cybersecurity form an essential part of the Company's operations and are necessary for preserving client and partner confidence.

Information security is intended to maintain the confidentiality, integrity, and availability of information. Cybersecurity is a part of information security focused on developing and applying measures that protect systems, services, networks, and applications against cyber-attacks.

1.2. This Policy sets out the Company's goals and objectives for information security and serves as the basis for all related internal processes, procedures, rules, and documents.

2. Purpose and Objectives

2.1. This Policy is the primary document establishing the principles and approaches used to protect the business processes and information assets of Topchik N.V. (hereinafter - the Company). It also confirms the commitment of the Company's Management to support information security principles and processes.

2.2. Compliance with this Policy is mandatory for all employees and for any individuals who work with the Company's information under contractual obligations.

3. Goals and Objectives of the Information Security

3.1. The Company regards the protection of information assets used in the business processes of its divisions as a strategic objective. This includes the protection of information and/or personal data of business clients, partners, employees, and any legal or natural persons that have legal relations or other forms of interaction with the Company. Protecting business client data and ensuring the secure provision of the Company's B2B services and platforms are among the Company's core principles.

3.2. This objective is achieved by:

- Ensuring the involvement of top management in the governance of information security processes.
- Performing information security risk assessments.
- Managing information security risks.
- Allocating the resources required for information security processes.
- Carrying out internal assessments of information security.
- Implementing applicable legal requirements for information protection.
- Maintaining compliance with relevant national and international standards.

4. Main Directions of Information Security Provision

The Company provides information security in accordance with legal requirements for information protection, applicable national and international standards, and through the following activities:

- Planning and implementing information security measures.
- Applying organizational security requirements and monitoring adherence to them.

- Implementing functional security requirements.
- Managing access and preventing unauthorized access.
- Preventing attacks and the infiltration of malicious software.
- Using cryptographic protection measures where necessary.
- Ensuring the resilience and reliability of information systems.

5. Use of Information Protection Measures

5.1. The Company applies appropriate information protection measures in line with legal and regulatory requirements.

5.2. The parameters and characteristics of the selected protection measures must correspond to the required security level.

6. Personal Data Protection

6.1. The Company gives special attention to the protection of personal data and privacy-related information of employees, representatives of business clients, partners, counterparties, and other relevant data subjects.

6.2. Information security must be taken into account when designing, implementing, or modifying systems and services that process personal data, so that applicable security requirements are met.

7. Information Security Threats

7.1. The Company protects information by:

- Applying legal, organizational, and technical measures to maintain confidentiality, integrity, and availability.
- Identifying potential threats and vulnerabilities, analyzing and assessing risks, and preventing incidents.

7.2. Threat sources include:

- Employee mistakes caused by insufficient knowledge or non-compliance with procedures.
- Technical and social negative factors, including malware, hacking, and fraud.
- Natural and man-made negative factors.

7.3. Common threats include:

- Information leakage.
- Unauthorized access.
- Malware.
- Hacker attacks.
- Denial of Service (DoS) attacks.
- Targeted attacks.
- Spam.
- Phishing.
- Spyware.
- Infrastructure failures.

7.4. Specific threats to systems include:

- Abnormal operating modes.

- Unauthorized access to operating environments.
- Remote unauthorized access.
- Substitution of trusted network objects.
- Routing of false information.
- Software and mathematical impacts.

7.5. If threats materialize, they may cause damage to the Company, including financial loss and reputational harm. Reducing the likelihood of risk realization requires the identification and remediation of vulnerabilities.

8. Principles of Information Security Provision

- Identification: uniquely distinguishing individuals or systems.
- Authorization: granting rights to perform specific actions.
- Authentication: confirming the authenticity of a user.
- Accountability: assigning individual responsibility for access to and handling of information.
- Business Necessity: providing access only where there is a business need.
- Least Privilege: limiting access rights to the minimum required.
- Segregation of Duties: requiring the involvement of more than one person for critical activities.
- Security Obligations: complying with applicable security requirements.
- Event Logging: recording user actions and security-related events.

9. Information Security Risk Management

9.1. The risk management process includes inventorying and classifying assets, identifying risks, analyzing and assessing them, and selecting appropriate risk treatment measures.

9.2. Asset categories include:

- Physical assets, including premises and equipment.
- Software assets.
- Service and system assets.
- Information assets.
- Personnel.

9.3. Risk treatment strategies include:

- Accepting the risk.
- Reducing the risk.
- Avoiding the risk.
- Transferring the risk.

10. Personnel Management Processes

10.1. In personnel-related processes, the Company's main objectives are:

- Recruiting qualified personnel.
- Verifying the reliability of employees.
- Informing personnel about information security requirements.
- Increasing security awareness.

11. Access Management

- 11.1. Access is granted on the basis of business necessity and the principle of least privilege.
- 11.2. Access to the Company's information, systems, services, and/or network must be managed with consideration of both business and security requirements.
- 11.3. The granting of access constitutes authorization to use the Company's information, systems, services, and/or network. It includes coordination with the initiator's direct supervisor and the asset owner, as well as verification that the requested access level corresponds to business needs and the requirements of this Policy.
- 11.4. Once a user receives access to a specific asset, the user may use that asset only for its intended purpose.
- 11.5. Access rights assigned to third-party service providers must be strictly controlled and promptly removed after the termination of the relevant contracts or agreements.

12. Secure Software Development

- 12.1. All software development must follow secure coding practices intended to prevent unauthorized manipulation of system components. Applications must be designed to protect databases and other critical assets from unintended or malicious programming activities initiated by users.
- 12.2. Only authorized personnel with the necessary access rights may perform system maintenance or application troubleshooting. Measures must be applied to ensure that servers are properly protected against unauthorized execution of mobile or external code, thereby preserving system integrity and reliability.
- 12.3. To preserve the security and integrity of software development processes throughout the full lifecycle, the following measures should be implemented, including but not limited to:
- Separating production, development, and testing environments where technically possible to prevent unauthorized connections.
 - Using controlled access mechanisms to production systems for development teams, ensuring that code changes are properly reviewed before deployment.
 - Applying rigorous verification procedures for software deployment to prevent test code from entering production environments.
 - Strictly prohibiting the use of raw production data in testing environments.

13. Security Testing

- 13.1. Regular technical security testing and vulnerability assessments should be conducted in a production environment to identify and address potential vulnerabilities. These assessments are performed by the Application Security Team.
- 13.2. Security testing and vulnerability assessments use a range of methods, including simulated attacks and vulnerability analyses, to identify both active threats and potential weaknesses in the Company's infrastructure.
- 13.3. Security assessments cover all aspects of the system, including network infrastructure, applications, and operating systems.

13.4. The Company uses both authenticated and unauthenticated testing methods to simulate different potential attack scenarios, including attempts to access systems at different privilege levels.

13.5. The results of these tests should be carefully reviewed and used by technical service owners and developers to strengthen security measures.

13.6. Testing procedures are aligned with industry standards and regulatory requirements to ensure that the Company meets the necessary security benchmarks and approaches.

14. Information Security Incidents

14.1. Violations are investigated and documented, and appropriate response measures are taken.

14.2. Incidents may be detected by employees or by automated systems.

14.3. Procedures for reporting, monitoring, and registering incidents are established.

14.4. Each incident is investigated, and the results of the investigation are recorded.

15. Information Classification

15.1. Certain types of information are more sensitive than others. Information classification determines how information must be handled. The Company uses four information levels:

- Public: information that may be freely disclosed to the public, or information intended for public release that does not create risk if accessed by anyone. Examples include press releases, marketing materials, and similar information.
- Internal: information intended only for internal use, or information not intended for public disclosure where unauthorized disclosure would not cause significant harm. Examples include company policies and procedures, aggregated data, and similar information.
- Confidential: sensitive information that requires restricted access, or information intended for a specific group of individuals within the Company where unauthorized access could harm the Company or individuals. Examples include employee records, internal project documentation, operational data, business client activity and service usage data, commercial data, compliance data, and regulatory data.
- Restricted: highly sensitive information that could cause severe damage if disclosed, or highly sensitive information that could have serious consequences for the Company or individuals if disclosed without authorization. Examples include financial data, such as profit and loss data, revenue and expense data, and budget statements, as well as sensitive client or partner information, including payment card data where applicable.

15.2. Classification criteria include:

- Legal and regulatory requirements: compliance with laws and regulations, including GDPR, PCI DSS, and other applicable requirements.
- Business impact: the potential effect on the business if the information is exposed or misused.
- Data owner input: input from the persons responsible for the information.

16. Collaboration with Third Parties

16.1. All contracts with third-party service providers involving access to, processing, communication, or management of the Company's systems or their components must include all relevant security requirements. These requirements include adherence to the Company's security policies, implementation of necessary safeguards, and compliance with applicable regulations.

16.2. To maintain an appropriate security level, the Company should periodically monitor and review services provided by third-party partners. This process may include evaluating performance against agreed metrics, assessing compliance with security protocols, and identifying potential risks or vulnerabilities.

16.3. Changes in the supply chain involving third-party service providers must be managed in a systematic manner. This includes maintaining and improving existing security policies, procedures, and controls in response to evolving threats and vulnerabilities.

16.4. The approach to third-party access management is described in the Access Management Policy.

17. Responsibility

17.1. The Company's Management is responsible for implementing and updating this Policy.

17.2. Management undertakes to take all relevant measures necessary to achieve the objectives of information security.