

Scores55 Tech B.V.
Information Security Policy

1. General Overview	3
2. Purpose and Scope	3
3. Information Security Objectives	3
4. Security Framework and Key Measures	4
5. Protection Measures	4
6. Personal Data Protection	4
7. Threat Management.....	4
8. Core Security Principles.....	6
9. Risk Management.....	7
10. Personnel Security	7
11. Access Control	7
12. Secure Development Practices	7
13. Security Testing.....	8
14. Incident Management.....	9
15. Information Classification.....	9
16. Third-Party Management	10
17. Responsibilities	10

1. General Overview

The Company recognizes that information is a critical business asset and is committed to ensuring its protection at all times. Information entrusted by customers, employees, partners, and other stakeholders must be handled securely and responsibly.

Information security is based on the principles of confidentiality, integrity, and availability. Cybersecurity forms an integral part of this framework and focuses on protecting systems, networks, and applications from digital threats.

This Policy establishes the foundation for the Company's information security framework and applies to all related processes, systems, and activities.

2. Purpose and Scope

The purpose of this Policy is to define the principles and requirements for protecting the Company's information assets and ensuring secure business operations.

This Policy applies to:

- all employees;
- contractors and consultants;
- third-party service providers with access to Company systems or data.

Compliance with this Policy is mandatory.

3. Information Security Objectives

The Company aims to protect all information assets, including personal data and operational data, against unauthorized access, disclosure, alteration, or destruction.

Key objectives include:

- ensuring continuous protection of information assets;
- integrating security into business processes;
- maintaining compliance with applicable laws and standards;
- supporting secure delivery of products and services.

These objectives are achieved through risk management, allocation of resources, internal controls, and continuous improvement.

4. Security Framework and Key Measures

The Company implements a structured approach to information security, aligned with applicable legal requirements and industry standards.

This includes:

- implementation of organizational and technical controls;
- monitoring compliance with internal policies;
- protection against cyber threats and malicious activities;
- ensuring system resilience and availability;
- use of encryption and other protective technologies where appropriate.

5. Protection Measures

Appropriate safeguards are implemented to protect information based on its sensitivity and associated risks.

Security controls are:

- proportionate to the level of risk;
- regularly reviewed and updated;
- aligned with regulatory and contractual requirements.

6. Personal Data Protection

The Company places particular importance on the protection of personal data.

All systems and processes that involve personal data must:

- incorporate security controls by design and by default;
- ensure compliance with applicable data protection regulations;
- prevent unauthorized access or misuse of personal information.

7. Threat Management

7.1 General Approach

The Company maintains a proactive approach to identifying, assessing, monitoring, and mitigating threats that may affect its information assets, systems, services, business processes, and stakeholders.

Threat management is intended to reduce the likelihood and impact of information security events and to support the confidentiality, integrity, and availability of Company information.

The Company implements appropriate organizational, technical, and procedural measures to prevent, detect, respond to, and recover from security threats.

7.2 Sources of Threats

Threats to information security may originate from internal or external sources, including but not limited to:

- human error, negligence, or lack of awareness;
- failure to follow internal policies or procedures;
- unauthorized or excessive access to systems or data;
- malicious actions by internal or external parties;
- cyberattacks, including phishing, malware, ransomware, and hacking;
- technical failures or misconfigurations;
- service interruptions or infrastructure failures;
- third-party or supply chain weaknesses;
- natural, environmental, or force majeure events.

7.3 Common Threat Categories

The Company considers, among others, the following threat categories:

- unauthorized access to systems, applications, or information;
- disclosure, leakage, alteration, or loss of information;
- malware infection or unauthorized code execution;
- phishing, social engineering, and credential compromise;
- denial-of-service or service disruption attacks;
- exploitation of technical vulnerabilities;
- misuse of privileged access rights;
- failure of critical systems, networks, or services;
- compromise of third-party services or integrations.

7.4 Threat Identification and Assessment

The Company identifies and evaluates threats through regular monitoring, internal reviews, risk assessments, vulnerability assessments, incident analysis, and input from relevant business and technical teams.

Threats are assessed based on their likelihood, potential impact, affected assets, and the effectiveness of existing controls.

Where a threat presents a material risk to the Company, appropriate mitigation actions shall be defined and implemented.

7.5 Preventive and Detective Measures

The Company applies preventive and detective controls to reduce exposure to threats. Such measures may include:

- access controls and authentication mechanisms;

- network and system monitoring;
- malware protection and endpoint security;
- secure configuration of systems and applications;
- vulnerability management and patching;
- logging and review of security events;
- employee awareness and training;
- backup and recovery measures;
- third-party risk controls.

7.6 Response and Continuous Improvement

Where a threat results in an actual or suspected security incident, the incident shall be managed in accordance with the Company's incident management procedures.

Lessons learned from incidents, testing, audits, and risk assessments shall be used to improve security controls and reduce the likelihood of recurrence.

8. Core Security Principles

The Company applies core information security principles to ensure that information assets are accessed, processed, stored, transmitted, and protected in a controlled and secure manner.

The Company applies the following core information security principles:

- Business Need: access to information and systems is granted only where there is a legitimate business requirement;
- Identification and Authentication: all users must be uniquely identified and their identity verified prior to access;
- Least Privilege: users are granted only the minimum level of access necessary to perform their duties;
- Authorization: access rights must be formally approved and regularly reviewed;
- Segregation of Duties: critical processes are divided to reduce the risk of error or misuse;
- Accountability: users are responsible for all actions performed under their credentials;
- Logging and Monitoring: relevant activities are recorded to ensure traceability and oversight;

Compliance: all users must adhere to the Company's information security requirements and policies.

9. Risk Management

Information security risks are managed through a structured process involving:

- identification of assets and risks;
- assessment of likelihood and impact;
- selection of appropriate mitigation measures.

Risk treatment options include:

- risk reduction;
- risk acceptance;
- risk avoidance;
- risk transfer.

10. Personnel Security

The Company ensures that personnel understand and comply with information security requirements.

This includes:

- hiring qualified and trustworthy individuals;
- conducting appropriate checks where necessary;
- providing ongoing security awareness training;
- ensuring employees understand their responsibilities.

11. Access Control

Access to systems and information is controlled and managed.

- access is granted based on role and business need;
- approvals are required prior to access provisioning;
- access rights are reviewed regularly;
- access is revoked promptly when no longer required;
- third-party access is strictly controlled.

12. Secure Development Practices

12.1. All software development activities must follow secure coding principles aimed at preventing unauthorized modification of system components.

12.2. Applications must be designed in a way that protects databases and other critical resources from unintended or malicious user actions.

12.3. Only authorized personnel with the required access rights may perform system maintenance or troubleshoot applications. Appropriate safeguards must

be in place to protect servers from unauthorized execution of external or mobile code, ensuring system integrity and stability.

12.4. To maintain security and integrity throughout the software development lifecycle, the following measures must be implemented, including but not limited to:

- Separation of development, testing, and production environments, where technically feasible, to prevent unauthorized interactions.
- Controlled access to production systems for development teams, ensuring that all code changes are reviewed and approved before deployment.
- Strict validation procedures during deployment to prevent test or unapproved code from being introduced into production
- Prohibition of using raw production data in testing environments.

13. Security Testing

13.1. Regular security testing and vulnerability assessments must be conducted in production environments to identify and remediate potential weaknesses. These activities are carried out by the Application Security Team.

13.2. Security testing includes a range of techniques, such as simulated attack scenarios and vulnerability scanning, to identify both existing threats and potential risks.

13.3. Assessments must cover all system components, including network infrastructure, applications, and operating systems.

13.4. Both authenticated and unauthenticated testing approaches are used to simulate different attack scenarios, including attempts to access systems with varying privilege levels.

13.5. The results of all testing activities must be reviewed and analyzed, and used by technical service owners and developers to strengthen security controls.

13.6. Testing processes must align with applicable regulatory requirements and generally accepted industry practices.

14. Incident Management

14.1. All security violations must be properly investigated, documented, and addressed with appropriate corrective actions.

14.2. Incidents may be identified either by employees or through automated monitoring systems.

14.3. Formal procedures must be established for incident detection, reporting, tracking, and logging.

14.4. Each incident must be investigated, and the findings must be documented for future reference.

15. Information Classification

The Company defines the following classification categories:

Public

Information intended for public disclosure or that may be freely shared without restriction.

Disclosure of such information does not pose any risk to the Company, its customers, or partners.

Examples may include:

- marketing materials
- publicly available website content
- press releases

Internal

Information intended for use within the Company only.

Unauthorized disclosure is not expected to cause significant harm but may be undesirable.

Examples may include:

- internal policies and procedures
- operational guidelines
- non-sensitive business communications

Confidential

Information that is sensitive and must be accessed only by authorized individuals on a need-to-know basis.

Unauthorized disclosure, modification, or loss may result in financial, legal, or reputational damage.

Examples may include:

- employee data
- customer data and player activity
- internal reports and analytics
- business strategies and operational data
- compliance-related information

Restricted

Highly sensitive information requiring the highest level of protection.

Unauthorized disclosure or compromise may result in severe financial loss, legal consequences, or significant reputational damage.

Examples may include:

- financial records and forecasts
- payment and cardholder data
- authentication credentials and encryption keys
- sensitive personal data
- critical system configurations.

16. Third-Party Management

The Company manages risks associated with third-party providers to ensure the security of its systems, data, and operations. This includes defining security requirements in contractual agreements, conducting risk assessments prior to engagement, monitoring third-party compliance and performance, and evaluating security impacts of any changes in third-party services. Access to Company systems by third parties must be strictly controlled and granted only as necessary.

17. Responsibilities

17.1. Management is responsible for implementing and maintaining this Policy.

17.2. All employees and third parties must comply with its requirements.

17.3. The Company is committed to continuously improving its information security practices.

Version Control

V. 1.0 – 2026.04.05 – Scores55 Tech B.V. - Policy creation