TRUST AND ASSURANCE STATEMENT

SEC-STMT-4

JULY 2026

INTRODUCTION

Playtech provides gaming technology and services to customers worldwide. The Information Security Department supports this mission by protecting the information, systems and assets entrusted to Playtech by employees, customers, suppliers and partners.

Playtech maintains a security programme designed to support trust, responsible business growth and the delivery of secure products and services. This Trust and Assurance Statement defines Playtech's commitment to securing the data, assets, and operational integrity of our global partners, customers, and stakeholders.

1 SECURITY FRAMEWORK AND GOVERNANCE

Playtech maintains a comprehensive Information Security Management System (ISMS) benchmarked against international standards, including ISO 27001 and PCI-DSS. Security practices are documented, regularly audited, and governed by a dedicated Global Information Security Team to ensure continuous compliance across all jurisdictions.

The Playtech ISMS includes security documentation, protective controls, organisational processes, audits, and security risk management principles.

Security documentation defines our approach to protecting information, systems and services. These documents set out security responsibilities, standards and requirements across key areas such as access management, network protection, vulnerability management, secure product development, supplier security, business continuity, and incident response. These documents are reviewed regularly and aligned with recognised security practices.

2 SECURITY CULTURE

Playtech's Information Security Department provides leadership and oversight for the security programme. Security responsibilities are organised across specialist areas including application security, cloud security, network security, offensive security, physical security, security governance, risk and compliance, security operations, security project management and system security. These teams support the development, operation, and improvement of the information security management system.

Clear responsibilities are defined and maintained for security implementation across the organisation. Business and operational units are required to implement the technologies, processes, and practices specified by the Information Security Department. Implementation is verified through internal and external assessments.

Secure workforce practices are implemented across the employment lifecycle. Recruitment practices support identity and background verification in accordance with applicable local requirements. Security obligations are included in employment arrangements, and security violations may be handled through disciplinary processes. Termination and offboarding activities follow defined tasks and timelines, including removal of accounts and access permissions.

The security awareness programme ensures that employees understand their information security responsibilities. Employees complete annual security awareness training and receive additional awareness activities through phishing campaigns, emerging threat communications, and regular security updates.

3 SECURE PRODUCT DEVELOPMENT

Playtech's secure software development lifecycle (SSDLC) embeds secure product development practices including requirements for processes and technologies designed to reduce the risk of introducing security weaknesses into products and services.

Developers receive additional secure development training designed to support their use of technologies, and additional training materials are available outside the formal training window.

Proactive security testing is performed on products and services. Playtech's internal security testing team conducts regular testing of products, records findings and tracks remediation in line with Playtech vulnerability management requirements.

4 OPERATIONAL AND INFRASTRUCTURE SECURITY

Playtech applies defence in depth and layered security protections to our networks, systems, and cloud environments. Systems and environments are monitored for vulnerabilities, and remediation must be performed in accordance with our vulnerability management requirements. Vulnerabilities identified through tools, testing and scanning are recorded, assessed, and managed

Secure system configuration practices protect systems against compromise. Systems are configured using security baselines, vendor guidance, and appropriate access controls. Protective technologies are deployed to protect corporate computers, servers, and other relevant devices. Devices are monitored for malicious activity and support the use of supported operating systems and current security applications.

Network security controls are implemented to reduce the risk of unauthorised access and attack. Access to production networks is restricted according to segregation of duties, least privilege and need-to-know principles.

Our Information Security Team maintains oversight of cloud environment configurations to ensure cloud services are adopted, implemented, and operated securely.

The Security Operations Centre coordinates Playtech's monitoring, detection, and incident response capabilities.

Business continuity and disaster recovery arrangements are in place to support resilience during disruptive events. Playtech supports flexible working arrangements, redundancy for offices and infrastructure where required, regular backups and disaster recovery planning for defined services and infrastructure.

5 PHYSICAL SECURITY

Physical security measures are implemented to protect facilities, assets, and data. Measures are applied according to sensitivity and criticality of facilities. Sensitive office areas are segregated where appropriate, and servers and communication equipment are kept in locked areas protected by appropriate monitoring and access controls.

6 DATA SECURITY

We protect our data through a series of processes and controls.

Asset management practices support the proper use, ownership, and protection of information and physical assets. Information and physical assets are classified, recorded, and assigned to accountable owners. Devices are controlled, managed and protected, and assets are returned or securely disposed of at the end of their use.

Access management controls and processes restrict access to sensitive information systems and assets based on organisational roles and business need.

We have established secure remote access measures employing layered controls, including secure connectivity, multi-factor authentication, managed devices, and restrictions on remote access use.

Encryption technologies are utilised to protect information in our devices, systems, files, websites, products, databases, and data transfers based on business and security requirements.

Supplier security practices ensure that suppliers demonstrate an appropriate commitment to information security. Suppliers are assessed during procurement and monitored throughout their relationship with Playtech. Where required, Playtech specifies security controls for safe use of supplier products or services, and suppliers with access to sensitive Playtech information are required to sign confidentiality agreements before access is granted.

The adoption of artificial intelligence technologies is tightly controlled. AI tools must be assessed and approved by the internal AI Governance Committee and Information Security team before use.

7 DATA PRIVACY

Data protection practices are designed to protect personal data belonging to employees, customers, partners and players. Playtech's Data Protection Team works with business units and product teams to improve processes and assess products against data protection obligations. The privacy function operates independently from Security and Product teams to support impartiality.