



Information Security Policy

SEC-1-SMG-POL-1

Code:	SEC-1-SMG-POL-1
Version:	3.0
Date of Version:	08.09.2025
Confidentiality Level	For Internal Use Only

Owned by	GRC Security
Last reviewed by	Director of Security GRC
Acknowledged By	Security Team Managers
Approved By	VP Security & IT

INTERNAL

The information presented herein is confidential information of Playtech Group and is also protected subject matter of copyrights owned by Playtech Group and of agreements between Playtech Group and its licensees and other parties. Copying, transmission and disclosure of such information can only be done within the strict scope of a governing Playtech Group agreement. In the absence of any specific agreement to the contrary, reverse engineering, decompilation and disassembly are prohibited in any event as to any software content. While all efforts have been made to ensure that the content of this document is accurate at the time of publication, the data upon which this document is based is subject to future change. Updated versions of this document will be released when necessary, resources permitting.

PREFACE

PURPOSE

The purpose of the Information Security Policy is to set out the corporate information security mission, objectives, and framework.

SCOPE

This policy applies to all Playtech personnel and legal entities (partners and businesses working alongside or under the Playtech corporate brand).

RESPONSIBILITIES

- Reviewing and updating the policy periodically: GRC Security Team
- Policy governance: GRC Security Team
- Review frequency and changes approval: As defined in this document

INTENDED AUDIENCE

All interested parties, stakeholders and Playtech employees and employees of Playtech's legal entities globally.

EXCEPTIONS TO THIS POLICY

- Exceptions or deviations to the requirements of this policy must be requested from the Security Department.
- Requests must be submitted via a ticket through the Helpdesk at: **Playtech Home > Playtech support | Jira ServiceDesk > Security > Issue Impact Acceptance**
- When submitting the request, please ensure that all relevant information is provided. A list of the required information is included in **SEC-1-SMG-PRD-1.2 Security Issue Impact Acceptance Process**, section 2.3.
- Exceptions to this policy will be approved on a case-by-case basis.
- More information about the exceptions process can be seen in: **SEC-1-SMG-PRD-1.2 Security Issue Impact Acceptance Process**.

CONTENTS

- 1 Introduction: Information Security at Playtech
 - 1.1 Information Security Objectives
 - 1.2 Basic Security Concepts
 - 1.3 Influencing Factors
- 2 Security Governance Framework
- 3 Security domains and policy statements
 - 3.1 Security Management and Governance
 - 3.2 People and Culture Security
 - 3.3 Asset Management
 - 3.4 Identity and Access Management
 - 3.5 Cloud Security
 - 3.6 Security Incident and Problem Management
 - 3.7 System Security
 - 3.8 Network Security
 - 3.9 Cross Domain Security
 - 3.10 Product and Application security
 - 3.11 Physical Security
 - 3.12 Business Continuity
 - 3.13 Supplier Security
 - 3.14 Security Compliance
 - 3.15 Offensive Security
- 4 Exceptions to Information Security Policies
- 5 Policy Enforcement
- Appendix A - Document Details
 - A.1 - Editorial Notes
 - A.2 - Change History

APPENDIX A - DOCUMENT DETAILS

A.1 - EDITORIAL NOTES

Repository	Playtech Home	Security Portal
Document Type	POL	Policy
Document Number	SEC-1-SMG-POL-1	
Valid From	08.09.2025	
Next Review Date	08.09.2026	

A.2 - CHANGE HISTORY

Date	Version	Updated By	Approved By	Description of Change
01.06.2012	1.0		CIO	Initial version
02.06.2013	1.1		CIO	Annual review
12.06.2014	1.2		CIO	Annual review
15.05.2015	1.3		CIO	Annual Review
19.09.2016	1.4		CSO	Align to business needs
30.06.2017	1.5		CSO	Amendments
08.06.2018	1.6		CSO	Annual review
03.06.2019	1.7		Senior ISM	Annual review
21.11.2019	1.8		CSO	Amendments
21.12.2020	1.9		CSO	New naming convention
30.12.2021	1.10		CSO	Annual review. Minor stylistic changes.
14.02.2023	2.0		CSO	New document format. Merged with Organization Security Policy

Date	Version	Updated By	Approved By	Description of Change
25.06.2024	2.0		CSO	Extension of validity to 31.12.2024 with no changes
08.09.2025	3.0		VP of Security and IT	Major update - Revision of content and structure