Information Security Directive

Document owner	VP, Group IT & Content Platform
Approval	CEO and CFO
Initially adopted	13 February 2020
Date last approved	13 January 2025
Date of next review/approval	Q4 2025
Applicability	Group

viaplay GROUP

Information Security Directive

1. Purpose statement and scope

The Viaplay Group Information Security Directive is a governance model that combines the organisation's specific information security prerequisites with the global standard ISO 27001:2017. As such, it represents an information security management system (ISMS) for Viaplay Group.

This ISMS seeks to preserve the confidentiality and integrity of information by applying an appropriate level of risk assessment. The basis for this assessment includes identified information or assets – whether defined by law, in agreements or by Viaplay Group – in addition to the consequences of an information security incident and suitable security controls to reduce risk.

Risk-related discussions and decisions should be integrated into existing risk management framework at Viaplay Group. The ISMS aims to provide a framework for knowledge-based decisions about information security risks and to ensure an acceptable level of risk for the company.

The information security field frequently overlaps with other fields. These include fields with common security goals, such as IT security, content protection and personal data protection. They also include fields with both common and separate security goals, such as human resources and finance.

Information security is everyone's responsibility. Everybody at Viaplay Group should strive to maintain a reasonable level of information security when handling information assets. Certain roles, particularly those involving the management of organisational areas, co-workers or systems, entail additional responsibilities.

This ISMS do not cover the information security attribute referred to as availability. It does not cover the domains of physical security (except physical security for user devices), environmental security, personal safety, or business continuity. It is not set out to be the security framework for production and content systems containing information assets.

This Group Directive applies to all employees of subsidiaries and entities in which Viaplay Group exercises decisive control, either directly or indirectly.

2. Steering documents, roles, and responsibilities

2.1 Steering documents

The steering documents relating to information and IT security at Viaplay Group are as follows:

- Asset Protection Policy: defines general information security principles and how they should be implemented by all users[1] at Viaplay Group.
- Information Security Directive: defines the framework of Viaplay Group's information security management system (ISMS) and the company's main information security objectives sorted by areas.
- Guidelines: present the specific requirements for fulfilling the information security objectives for a defined area.

These steering documents strive to fulfil defined parts of the requirements of ISO27001:2017 table A.1. Some of these requirements are not directly addressed in the second part of this Information Security Directive because they are covered i.) in Viaplay Group's Asset Protection Policy; ii.) in the first part of this Directive; or iii.) by the stated limitations in scope.

2.2 Roles and responsibilities

2.2.1 General

- Users at Viaplay Group should always work in a responsible manner and in accordance with the company's Asset Protection Policy.
- Managers of a domain, group, project or similar have a responsibility i.) to strive to fulfil information security requirements within their area of responsibility; ii.) to facilitate the development of metrics that increase transparency in relation to how information security requirements are fulfilled within their area of responsibility; and iii.) to establish procedures for responding to and learning from information security incidents.
- Managers with extended responsibilities have an individual or shared responsibility i.) to create the information security requirements in one or several guidelines; ii.) to make a regular assessment of any changes needed to these requirements; and iii.) to revise the requirements at least annually. The latter two responsibilities necessitate contact with authorities and special interest groups, in addition to knowledge of legislative, regulatory, and contractual requirements related to the information security areas relevant to the manager's role and responsibility. The decision that certain managers have an extended responsibility is initiated during a dialogue with and later decided by VP Group IT & Content Platformtogether with related Information Security functions.

[1] This Directive refers to any person with access to Viaplay Group's information systems as a "user." The term can include permanent Viaplay Group employees, consultants, contracted agencies, suppliers, customers and/or business partners.

- The VP Group IT & Content Platformhas the mandate and is responsible for developing and maintaining a framework and governance model for information security which is defined in the Viaplay Group's Asset Protection Policy and this Directive.

2.2.2 Incidents

- Viaplay Group's Information security function, and VP Group IT & Content Platformin case of high severity, should always be immediately informed of Information security incidents. Whether it is a discovery of a vulnerability or actual exploitations of vulnerabilities. This according to the main incident management process.
- Major Incidents are managed through the corporate Incident Process and framework for Risk Management. Incident Ownership and management should always follow the corporate process. Incident ownership is determined by type of incident and business area in which the incident was being identified.

2.2.3 Reviews

- Reviews are to be regularly held according to the Risk framework. Risks are identified, classified and mitigations, if so needed are implemented to eliminate vulnerabilities. Reviews within the Incident Process focus on securing continuity, aiming at timely, effective identification and action of exploits. All reviews relating to information security should be conducted by both the Information Owner concerned and the related Information Security function.

3. Information security objectives

In this ISMS, information security is divided into areas according to the ISO27001:2017 standard. The main objectives or requirements for each area are described below. Each area has a corresponding guideline document that sets out more detailed requirements.

The owners of each guideline document are responsible for developing and maintaining these requirements, which should consider Viaplay Group's regulatory and contractual responsibilities. Viaplay Group's VP Group IT & Content Platformand the different Businesses' Information security functions, are responsible for facilitating this work and for providing guidelines and templates to safeguard a coherent structure.

As part of the design of each guideline document, there should be an assessment to establish the right information classification level. Viaplay Group recognizes four levels of information value: unrestricted, restricted, confidential, and secret. Each value level has an associated security level. The information security requirements in this directive and in the following guidelines will determine the security requirements, hence the security level.

3.1 Human resources

3.1.1 Prior to employment

The objective is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are being considered. This includes screening and terms and conditions of employment.[2]

3.1.2 During employment

The objective is to ensure that employees and contractors are aware of and fulfil their information security responsibilities. This includes management responsibilities, information security awareness, education, training and disciplinary processes.[3]

3.1.3 Change or termination of employment

The objective is to protect the organisation's interests as part of the process of changing or terminating employment.[4]

3.2 Asset management

3.2.1 Responsibility for assets

The objective is to identify organisational assets and define appropriate protection responsibilities. This includes inventory of assets, ownership of assets, acceptable use of assets and return of assets.[5]

3.2.2 Information classification

The objective is to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation. This includes classification of information, labelling of information and handling of assets.[6]

3.2.3 Media handling

The objective is to prevent unauthorised disclosure, modification, removal or destruction of information stored on media. This includes management of removable media, disposal of media and physical media transfer.[7]

3.3 Access control

3.3.1 Business requirements of access control

The objective is to limit access to information, network services and networks.[8]

[2] ISO/IEC 27001:2017 Requirement 7.1.1 – 7.1.2
[3] ISO/IEC 27001:2017 Requirement 7.2.1 – 7.2.3
[4] ISO/IEC 27001:2017 Requirement 7.3.1
[5] ISO/IEC 27001:2017 Requirement 8.1.1 - 8.1.4
[6] ISO/IEC 27001:2017 Requirements 8.2.1 – 8.2.3
[7] ISO/IEC 27001:2017 Requirements 8.3.1 – 8.3.3
[8] ISO/IEC 27001:2017 Requirements 9.1.1 – 9.1.2, with limitations according to scope, especially physical security

3.3.2 User access management

The objective is to ensure authorised user access and to prevent unauthorised access to systems and services. This includes user registration and de-registration, user access provisioning, management of privileged access rights, management of secret user authentication information, and review, removal or adjustment of access rights.[9]

3.3.3 User responsibilities

The objective is to make users accountable for safeguarding their authentication information.[10]

3.3.4 System and application access control

The objective is to prevent unauthorised access to systems and applications. This includes information access restrictions, secure log-on procedures, password management systems, privileged utility programs and access control for program source code.[11]

3.3.5 Cryptography

The objective is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.[12]

3.4 Physical security

3.4.1 Secure working conditions related to equipment and information

The objective is to prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations. This includes equipment siting and protection, security of equipment and assets off-premises, secure disposal or reuse of equipment, unattended user equipment, clear screen, mobile devices, and distance work.[13]

3.5 Operations security

3.5.1 Operational procedures and responsibilities

The objective is to ensure correct and secure operation of information processing facilities. This includes documented operating procedures, change management, and separation of development, testing and operational environments.[14]

[9] ISO/IEC 27001:2017 Requirements 9.2.1 – 9.2.6
[10] ISO/IEC 27001:2017 Requirements 9.3.1
[11] ISO/IEC 27001:2017 Requirements 9.4.1 – 9.4.5
[12] ISO/IEC 27001:2017 Requirement 10.1.1 – 10.1.2
[13] ISO/IEC 27001/2017 Requirement 6.2.1 – 6.2.2, 11.2.1, with limitations according to scope, especially environmental security 11.2.6 – 11.2.9
[14] ISO/IEC 27001:2017 Requirement 12.1 – 12.1.2, 12.1.4, with limitations according to scope, especially availability

3.5.2 Protection from malware

The objective is to ensure that information and information processing facilities are protected against malware.[15]

3.5.3 Logging and monitoring

The objective is to record events and generate evidence. This includes event logging, protection of log information, administrator and operator logs, and clock synchronisation.[16]

3.5.4 Control of operational software

The objective is to ensure the integrity of operational systems.[17]

3.5.5 Technical vulnerability management

The objective is to prevent exploitation of technical vulnerabilities. This includes management of technical vulnerabilities and restrictions on software installation.[18]

3.5.6 Communications security

The objective is to ensure the protection of information in networks and supporting information processing facilities. This includes network controls, security of network services and segregation in networks.[19]

3.5.7 Information transfer

The objective is to maintain the security of information transferred within an organisation and to/from any external entity. This includes information transfer and procedures, agreements on information transfer, electronic messaging, and confidentiality or non-disclosure agreements.[20]

3.6 System acquisition, development, and maintenance

3.6.1 Security requirements of information systems

The objective is to ensure that information security is an integral part of information systems across the entire lifecycle, including requirements for information systems that provide services over public networks. This includes information security requirement analysis and specification, security application services on public networks and protecting application service transactions.[21]

[15] ISO/IEC 27001:2017 Requirement 12.2.1
[16] ISO/IEC 27001:2017 Requirement 12.4.1 – 12.4.4, with limitations according to scope, especially availability
[17] ISO/IEC 27001:2017 Requirement 12.5.1
[18] ISO/IEC 27001:2017 Requirements 12.6.1 – 12.6.2
[19] ISO/IEC 27001:2017 Requirements 13.1.1 – 13.1.3
[20] ISO/IEC 27001:2017 Requirements 13.2.1 – 13.2.4
[21] ISO/IEC 27001:2017 Requirements 14.1.1 – 14.1.3

3.6.2 Security in development and support processes

The objective is to ensure that information security is designed and implemented within the development lifecycle of information systems. This includes secure development steering documents, system change control procedures, technical review of applications after operating platform changes, restrictions on changes to software packages, secure system engineering principles, secure development environments for outsourced development, system security testing and system acceptance testing.[22]

3.6.3 Test data

The objective is to ensure the protection of data used for testing.[23]

3.7 Supplier relationships

3.7.1 Information security in supplier relationships

The objective is to ensure protection of the organisation's assets that are accessible by suppliers. This includes steering documents for supplier relationships and addressing security in supplier agreements and throughout the information and communication technology supply chain.[24]

3.7.2 Supplier service delivery management

The objective is to maintain an agreed level of information security and service delivery in line with supplier agreements. This includes monitoring and review of a supplier's services and managing changes to these services.[25]

4. Document history and change information

For more details of this Group Directive's document history and change information, see Appendix 1.

[22] ISO/IEC 27901:2017 Requirements 14.2.1 – 14.2.9
[23] ISO/IEC 27001:2017 Requirements 14.3.1
[24] ISO/IEC 27001:2017 Requirements 15.1.1 – 15.1.3
[25] ISO/IEC 27001:2017 Requirements 15.2.1 – 15.2.2

Appendix 1 – Document History and Change Information

Version	Revision Date	Change information
1	2020-02-13	Initial Group Directive.
2	2021-01-11	New Document Owner. Editorial changes. Major deletions and changes to content in Para. 2.2 on roles & responsibilities, including sub-sections 2.2.2. on incidents and 2.2.3. on reviews.
3	2022-09-12	No changes
4	2023-11-21	No changes
5	2024-10-08	Minor adjustments