

PLCY-SEC-T1 Information Security Policy



Definition

For the purposes of this policy, IGamingCloud N.V. shall hereinafter be referred to as GiG

Introduction

1.1	Purpose
	GiG's Information Security Policy is a top-level overarching policy within GiG's Information Security Management System ("ISMS"). GiG's ISMS contains a set of policies and procedures for systematically managing information security.
	The purpose of this policy is to: • demonstrate top management's direction and support for information security in accordance with the purpose of the organisation, and the requirements from the business strategy, regulations, legislations, contracts, and the current and projected information security threat environment, • define GiG's information security objectives, • ensure that information security objectives are based on business requirements, • define the various roles and responsibilities for information security within GiG, and • define high-level policy statements.
1.2	Conversational Summary
	This document outlines GiG's mission, and objectives with regards to Information Security, as well as the roles and responsibilities required to maintain GiG's ISMS.
Failure to comply with this document will be dealt with disciplinary action per company policy.	

Scope

2.1	Audience
	The requirements of this policy need to be followed by: • all employees and contractors of GiG Software PLC and its subsidiaries, regardless of their position, job role, location or relationship with the company.
2.2	Applicability
	This document applies to: • all information, irrespective of the way it exists, that is owned or processed by GiG. • all physical premises and assets owned and operated by GiG. • all employees and contractors of GiG regardless of their position, job role, location or relationship with the company. • all GiG Software PLC subsidiaries.

Organisational Roles and Responsibilities

3.1	Certain individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless they remain accountable and should determine that any delegated tasks have been correctly performed.
3.2	The following is a list of roles and responsibilities for information security within GiG:

		Top Management (CEO, COO etc) • Overall direction, support and commitment to information security in-line with the company's objectives; • Ensuring that the information security policy and security objectives are established, and are compatible with the strategic direction and purpose of the organisation; • Ensuring the integration of the information security management system requirements into the organisation's processes; • Ensuring that the resources needed for the ISMS are available; • Endorsing the importance of effective information security management and of conforming to the ISMS requirements; • Ensuring that the ISMS achieves its intended outcome(s); • Directing and supporting persons to contribute to the effectiveness of the ISMS; • Acceptance of information security risks which have a risk level higher than the defined acceptable level; • Promoting continual improvement; and • Supporting other relevant management roles to demonstrate leadership as it applies to their areas of responsibility. • Ensuring that the requirements laid out in ISO 27001 are abided by. • Be informed about the performance of the group's management systems.
	3.2.2	Management - Responsible for ensuring that all ISMS policies and procedures are adhered to within their respective business area, and to ensure that all employees understand their obligation to protect GiG's information assets, to comply with security policies and related procedures, and to report security events/ incidents when they occur.
	3.2.3	Employees and Contractors - All staff are required to acknowledge this policy, and to adhere to all ISMS policies and procedures that are relevant to their role (for more information refer to the audience matrix). Staff have an important role to play in considering security in their day-to-day operations and to report security events/ incidents when they occur. It is a requirement that all staff undergo annual security training to ensure continued awareness of their responsibilities for information security.

Information Security Objectives

	GiG's Information Security Management System Objectives are the following: 1. Achieve, and maintain ISO 27001 certification 2. Ensure that users are aware of, and compliant to Information Security documentation 3. Raise Information Security awareness company wide 4. Drive a risk aware culture company wide These objectives in turn feed into the overarching Information Security, as well as organisational objectives, as supported by the framework of policies, which include the following:
4.1	1. Confidential information must be accessed only by persons that require access, always following the principle of least privilege 2. Stability, security, and availability of our information must be kept consistent when affecting changes to GiG's systems 3. The integrity of our client information, as well as our business information, must be maintained at all times 4. To be the industry leading platform, and media provider delivering world class secure solutions to our iGaming partners and their customers 5. Compliance to Gaming Regulations and other legal requirements for our various licenses must always be in place, integrated within all our systems and business processes For audit purposes, a detailed information security objectives plan may be found in /wiki/spaces/GISO/pages/320012497 (restricted).

Policy Statements

	GiG shall follow a Plan, Do, Check, Act (PDCA) cycle approach for the management of information security within the business; aligned to the requirements of ISO/IEC27001:2022
5.1	The list of Information Security Policies below provide the framework by which we can maintain these principles. The framework will enable GiG personnel and other persons processing GiG information, to understand both the legal and ethical responsibilities concerning information, and empower them to use, store and distribute it in appropriate ways.
5.2	An Information Security Education, Training, and Awareness (S.E.T.A) programme shall be put in place to foster an information security culture within the organisation. Please refer to GiG Security, Education, Training and Awareness Framework for further details.

5.3	The tools provided to employees and contractors which are appropriate and necessary to fulfil their role, including access to computer systems, mobile devices, networks, software, databases, cloud services, physical premises, email and the internet, shall be used in line with the requirements of the Acceptable Use Policy .
5.4	All information created, stored or communicated on or by GiG's systems remains the exclusive property of the company, and shall be classified, labelled and handled in accordance with the Information Classification Policy. Information shall be classified, labelled, handled and appropriately protected according to its level of sensitivity/ confidentiality and importance to the organisation. Please refer to Information Classification Policy for further details.
5.5	Access to physical premises, systems, networks, and information shall be controlled within the organisation. Please refer to /wiki/spaces/GISO/pages/585499797 for further details.
5.6	GiG shall ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. Please refer to Cryptography Policy for further details.
5.7	GiG shall prevent unauthorised physical access, damage, theft, and interference to information, assets and information processing facilities. Please refer to Physical Access Policy for further details.
5.8	The transfer of GiG information both internally and externally shall be secured based on its classification. Please refer to Information Handling Procedure for further details.
5.9	Information security shall be designed and implemented within the development lifecycle of information systems. Please refer to the Application Security document for further details. In line with ensuring such objectives, GiG follows a vulnerability management framework which can be found in the Vulnerability Management Policy .
5.10	GiG shall ensure the protection of information assets that are accessible by third party suppliers. Please refer to Secure Supplier Relationship Management Policy for further details.
5.11	GiG shall ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. Please refer to Security Incident Management Procedure for further details.
5.12	GiG Employee assets (laptops, mobile phones) are closely monitored and managed by GiG's CorpIT team. This also includes the secure disposal of such assets. Kindly reach out to CorpIT for further details.
5.13	GiG strives to ensure that its network are well maintained and secure. Additionally, as part of the Vulnerability Management Policy , tests on internal networks are carried out to ensure an adequate level of security. Additional information can also be found in the Network Security Policy .

Policy Exceptions

6.1	Exceptions to the policy are deemed to be a business risk and hence need to be formally raised , reviewed and approved by GiG's C-level member.
6.2	Exceptions shall be time limited and in the exception request there shall be a plan for how and when to comply.
6.3	Exceptions will be handled on a case-by-case basis, and no exception is to serve as a precedent to approving similar requests in the future.
6.4	Violations of GiG's information security policies and procedures, as well as information security breaches* committed by employees or contractors must be reported to a Line Manager or infosec@gig.com as soon as possible and may result in disciplinary action, leading up to and including dismissal (according to the disciplinary policy found on the HR portal) - depending on certain factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. *An information security breach is defined as: Exposing sensitive GiG information to unauthorised access, use, disclosure or modification.

Document Control

7.1	All versions of this document shall be kept under strict control; all major changes shall be formally approved, recorded in the Version History table and communicated to the relevant individuals as identified in Section 2.1.		
7.2	This document shall be reviewed at least annually, or when major changes occur.		
7.3	The review and approval process shall be as follows: 1. Document Owner reviewing shall change the status of the document to UNDER REVIEW (both at the top of the document under the logo and in the document control table). Important that the document is not published until all changes are complete. 2. The Document Owner will then tag the approver (example: Nádia Cação) in the Version History Table (at the end of the document, in the column “Approved By”). 3. The Approver will review the changes made in the document and if approved, update the status to LIVE (both at the top of the document under the logo and in the document control table).		
<table border="1"> <tr> <td>Document Type</td><td>Policy - Tier 1</td></tr> </table>		Document Type	Policy - Tier 1
Document Type	Policy - Tier 1		

Owner	Nadia Cacao (Information Security GRC Analyst)
Approver	Michael Fenech (Head of Information Security)
Date First Published	05 Feb 2018
Date of Next Planned Review	05 Feb 2026
Classification	INTERNAL
Status	LIVECOMMUNICATED

Version	Date	High Level Description of Changes Name	Edited By	Approved By
1.0	05 Feb 2018	Initial release of document	Christian Bajada (Head Of IT Security)	Edgars Peics (CTO)
1.1	10 Jan 2019	Review of policy	Michael Fenech (Information Security Officer)	Diane Abela (Head of Information Security)
1.2	10 Jul 2019	Minor changes due to centralisation of policies	Marlon Vassallo (Information Security Officer)	Diane Abela (Head of Information Security)
1.3	10 Feb 2020	Annual Review	Joswe Muscat (Information Risk Officer)	N/A
2.0	26 Feb 2021	Annual Review & Major Changes	Joswe Muscat (Information Security GRC Team Lead)	Diane Abela (Director of Information Security)
3.0	11 Jun 2021	Major Change: Revamp of Policy as part of the Revamp Initiative	Jonathan Bezzina Gatt (Information Security GRC Analyst) & Joswe Muscat (Information Security GRC TL)	Former user (Deleted) (Director of Information Security)
3.1	03 Aug 2021	Minor change: update to 4.1	Joswe Muscat (Information Security GRC TL)	N/A
3.2	10 Aug 2021	Minor change: insertion of clause 1.2	Jonathan Bezzina Gatt (Information Security GRC Analyst)	N/A

3.3	07 Feb 2022	Annual Review & Minor change: update embedded link in 4.1	Joswe Muscat (Information Security Manager GRC)	N/A
3.4	11 Apr 2022	Minor change: changes to document control table	Jonathan Bezzina Gatt (Information Security GRC Analyst)	N/A
3.5	15 Feb 2023	Annual Review & Minor Changes	Jonathan Bezzina Gatt (Information Security GRC Analyst)	N/A
4.0	17 May 2023	Major Changes: Updated Information Security Objectives	Jonathan Bezzina Gatt (Information Security GRC Analyst)	Michael Fenech
4.1	01 Feb 2024	Annual Review	Jonathan Bezzina Gatt (Information Security GRC Analyst)	N/A
4.2	08 May 2024	Minor changes	Nadia Cacao (Junior Information Security GRC Analyst)	N/A
4.3	04 Dec 2024	Minor changes	Nadia Cacao (Information Security GRC Analyst)	N/A
4.4	09 Apr 2025	Annual Review	Nadia Cacao (Information Security GRC Analyst)	N/A