

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

Policy

Of Information Security

CURACAO, 2025

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

Revision history

Version	Date	Author(s)	Comment
1.0.	30.08.2024	L. Gyurjyan	Initial version
1.1.	28.08.2025	L. Gyurjyan	Periodic review

CONTENTS

1.	Policy's purpose and scope.....	3
2.	Terms, definitions, acronyms.....	3
3.	Policy description	4
4.	Policy review	12
5.	Related documents, annexes.....	12

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

1. Policy's purpose and scope

The purpose of this policy is to define the Digitain Curaçao B.V. (hereinafter referred to as Company) goals and main development directions in the field of Information Security.

The scope of the company's ISMS includes offering B2B services to key partner companies in the fields of fast games and online casino games.

In addition, the scope of the Company's information security management system covers the information security of all business processes in the Company. The scope includes all structural units making part of the Company's structure, employees, all information assets and cooperation with third parties and other stakeholders.

2. Terms, definitions, acronyms

The definition of Information Security in this policy includes the compliance, access, availability, confidentiality and integrity of physical and information assets.

Compliance - means that management, all employees, contract-based workers, third-party employees, etc. must be informed of their Information Security related obligations (which are included, for example, in contracts or NDA agreements), maintain information security, report the observed violations and act according to the requirements of the ISMS.

CIA – Confidentiality, Integrity, Availability – three main components (pillars) of Information security.

Availability - means that information and related assets are available to authorized persons as necessary. The Company must be able to detect and promptly respond to information security incidents (such as malware attacks or other breaches) that threaten the availability of assets, systems, information.

Confidentiality - means that information is accessible only to authorized persons, thus preventing intentional or accidental unauthorized access to systems (networks, websites, information systems, etc.).

Integrity - means ensuring the accuracy and integrity of information and data processing methods, preventing intentional or accidental, partial or total destruction or unauthorized modification of physical & electronic information assets. The Company has plans in place to handle potential information security incidents, as well as a data backup process.

Physical assets include network equipment, computer equipment, cables, telephone systems, etc.

Information assets can be printed or handwritten, sent by mail, spoken verbally or stored electronically on websites, intranet, backup copies, digital or other magnetic media, as well as transmitted electronically.

ISMS stands for information security management system, which consists of an information security management policy, manual and a set of other documents developed according to the ISO/IEC 27001:2022 standard.

An information security breach is an incident, weakness or event that causes or may cause a violation of the availability, confidentiality, or integrity of the Company's information assets.

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

3. Policy description

Digitain Curaçao B.V. (hereinafter referred to as the Company) operates a business in the field of software development, buying and reselling software programs and also rendering all possible services related hereto.

The Company ensures the confidentiality, integrity and availability of hard-copy and electronic information with the aim of maintaining competition, cash flow, profitability. The Company's activities are carried out in accordance with the relevant legal, regulatory and contractual requirements, in particular, in accordance with the legislation of Curaçao, civil and criminal codes, GDPR, the Labor Code, this IS policy.

The external and internal goals and objectives of the implementation of the Company's ISMS are:

- To have a continuously developing information security management system,
- To ensure confidentiality, availability and integrity of information,
- To have in place a comprehensive and complete package of IS regulatory documents,
- To comply with the requirements of ISO 27001 and other applicable standards,
- To prevent leakage of information,
- To comply with international and Curaçao laws,
- To be able to ensure business continuity in emergency/force majeure situations,
- To ensure effective risk management,
- To ensure the confidentiality of personal data made available to the Company,
- To have a secure network infrastructure,
- To ensure proper performance of IS functions,
- To maintain steady and secure relationship with stakeholders, including suppliers and partners,
- To ensure proper handling of information security incidents,
- To ensure efficiency of systems and data backup and recovery processes, etc.

The list of Company's main stakeholders and their expectations regarding information security are summarized below:

- a. CEO (internal)
 - Undertake comprehensive measures to ensure the confidentiality of Company's sensitive information.
 - Regularly present information on the current state of the ISMS, assessment of potential risks and necessary measures for their mitigation.
 - Undertake comprehensive measures to protect the company's assets from possible cybercrimes.
- b. Employees (internal)

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

- Obtain the necessary knowledge and training to recognize security risks and take effective countermeasures against them.
- Enjoy a safe and secure working environment.
- c. Partners (external)
 - Have confidence in the security procedures and technical means used by the Company.
 - Ensure confidentiality and integrity of sensitive information and personal data entrusted to the Company.
 - Ensure the rights of the customers and/or their employees and players under GDPR.
 - Be timely notified of the information security incidents, take measures for their immediate resolution and elimination of consequences.
- d. Suppliers (external)
 - Be sure that the security of the supplied software products will not be compromised due to the lack of proper security measures in the Company.
 - Ensure confidentiality and integrity of sensitive information and personal data entrusted to the Company.
 - Ensure the rights of the supplier and/or its employees under GDPR.
 - Get prompt notifications of information security incidents.
- e. Consultants (external)
 - Have accesses needed to provide the relevant services.
 - Ensure the confidentiality of sensitive and personal information made available to the Company during the provision of services.
- f. Regulatory bodies (external)
 - Ensuring compliance with IS requirements

Company's risk assessment and risk management plan define the principles and rules of their management, define the measures necessary to deal with risks and the responsible structural units.

The Information Security function of the Company organizes training for all employees no less than once a year, during which employees are presented with the requirements of safe use of information.

Also, ongoing trainings are organized for newly recruited employees, during which a brief description of the procedures and the main concepts and principles of information security, as well as information regarding the involvement of employees in the processes of ISMS implementation are presented.

All employees of the Company must take part in education/training in IS-related matter and pass an appropriate test to confirm the proper adoption of the acquired knowledge.

The information security function is subject to continuous, periodic review and improvement. The Company's management has a strong input and supports the implementation, maintenance, evaluation, development and periodic review of the ISMS by conducting regular management reviews.

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

The IS management system and its implementation is also subject to review by an independent reviewer at the initiative of the Company's management. The results of the independent review are recorded, maintained and communicated to the Company's management.

In case of violation of information security requirements, the employees may be subject to disciplinary and administrative penalties, depending on the consequences resulting from the violation of the information security, up to the termination of the employment contract.

The person in charge for Information Security is the owner of this document and is responsible for the implementation of this Policy.

The current version of the Information security policy is available to all employees of the Company and does not contain sensitive information.

4. Information Classification

Digitain will classify its information as follows:

- **Strictly confidential:** Information, breach of confidentiality, integrity or availability of which leads to severe consequences for the Company and the functions, staff, partners or customers thereof.
- **Confidential:** Information, breach of confidentiality, integrity or availability of which leads to medium level consequences for the Company and the functions, staff, partners or customers thereof.
- **For internal use:** Information, breach of confidentiality, integrity or availability of which leads to low level consequences for the Company. Access to this information is restricted to company's employees only.
- **Public:** Information which is published on the Company's websites, social media pages, mass media, advertising and informative material, as well as other information intended for the public at large. Unrestricted information has no internal or external restrictions.

Digitain' information shall be protected according to the results of the classification during the whole information life cycle, i.e. from creation /registration through destruction / disposal of the information.

The Company has designed special handling rules for each classification level (detailed in Appendix 1), covering access provision, storage, transfer, sanitization and labelling of information with special care to specific areas, like Intellectual Property Rights and Personally Identifiable Information.

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

5. Network Security Policy

The use of networks is an essential part of the day-to-day business of Digitain. Networks not only connect many of the components of business processes together internally, but they also link the organisation with its suppliers, customers, stakeholders and the outside world.

The company's networks have evolved over a period of time to become the circulatory system of the company, transporting information to where it needs to go and enabling business to be carried out effectively.

But the fact that so much information runs through our networks makes them a target for those who would try to steal that information and disrupt our business. Therefore, these networks need to be protected to ensure that the confidentiality, integrity and availability of our vital information is always assured.

The effective protection of our network requires that we adopt good practices in information security covering the design, implementation, operations and management of them and that we ensure that everyone involved follows these practices.

This policy sets out Digitain's rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure. Its intended audience is IT and information security management and support staff who will implement and maintain the organisation's defences.

As a cloud service provider (CSP), this policy also applies to the methods used to design and create the physical and virtual networks used to deliver service to our cloud customers.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Digitain's systems

5.1. Network security design

The design of networks is a complicated process requiring a good knowledge of network principles and technology. Each design is likely to be different, based on specific set of requirements that are established early in the process. This policy does not attempt to specify how individual networks should be designed and built but provides guidance for the standard building blocks that should be used.

5.2. Requirements

A network design must be based on a clear definition of requirements which should include the following security-relation factors:

- ☐ The classification of the information to be carried across the network and accessed through it
- ☐ A risk assessment of the potential threats to the network, taking into account any inherent vulnerabilities

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

- ☐ The level of trust between the different components or organisations that will be connected
- ☐ The hours of availability and degree of resilience required from the network
- ☐ The geographical spread of the network
- ☐ The security controls in place at locations from which the network will be accessed
- ☐ Security capabilities of existing computers or devices that will be used for access, etc.

Requirements must be documented and agreed before design work starts.

5.3. Defence in depth

A ‘defence in depth’ approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network. For example, network firewalls may be supplemented by host-based software firewalls on server and clients in order to provide several levels of firewall protection.

At key points in the network a ‘defence diversity’ approach must also be taken so that vulnerabilities are minimised. For example, this may involve using firewalls from different subject to it. This may be extended to the use of more than one network virus scanner at the perimeter for the same reason.

5.4. Network segregation

The principle be adopted that, where appropriate, a network will consist of a set of smaller networks segregated from each other based on either trust levels or organisational boundaries (or both).

For a large network this may be achieved using separate domains, particularly where separate organisations’ networks are being linked. An appropriate level of trust must be configured at the domain level and domain perimeters must be secured using a firewall where appropriate.

Within networks, Virtual Local Area Networks (VLANs) will be used to segregate organisational units.

In a cloud environment, it is important that requirements for segregating networks to achieve tenant isolation are defined and the cloud service provider’s ability to meet these requirements is verified.

5.5. Perimeter Security

At all perimeters between the internal networks and an external network (such as the internet) effective measures must be put in place to ensure that only authorised network traffic is permitted. For connections such as broadband at smaller locations a packet filtering firewall may suffice, depending on the results of a risk assessment.

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

Servers that are intended to be accessed from an external, insecure network (such as web servers) must be located in a Demilitarized Zone (DMZ) of the firewall in order to provide additional protection for the internal network.

5.6. Cloud networks

Where virtual infrastructure services are configured within a virtual private cloud, the same principles must be used as for the security of physical networks. These will include the use of network segmentation, firewall, access control lists and log monitoring.

5.7. Public networks

Where information is to be transferred over a public network, such as the internet, strong encryption via TLS 1.2+ must be used to ensure the confidentiality of the data transmitted.

Servers that will be accessed from devices on the public network will be located in the DMZ of the firewall.

5.8. Wireless networks

Wireless networks must be secured using WPA2+ encryption. WEP and WPA must not be used.

Wireless networks must be treated as insecure even if WPA2 is used as the encryption method and a firewall installed between the wireless network and the main LAN.

A guest wireless network may be provided to visitors. This must be physically separate from all internal networks (including internal wireless networks) and secured using a firewall.

Wireless access points must be configured to not broadcast their SSID and to not allow secure connection using WPS (Wi-Fi Protected Setup) via physical access to the access point itself.

Wireless access point admin logon passwords must always be changed from the default.

5.9. Physical security

Remote network equipment will be housed in secure cabinets which will always be locked. Only support staff will have access to the key to each cabinet.

Backbone and centralised network equipment will be housed in appropriate lockable cabinets or racks in a secure server room to whom only authorised support staff will have access (except for local facilities staff for reasons of health and safety).

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

Wireless access points located in public areas must be hidden from view where possible and must be placed in positions where access by the public is difficult e.g. in or near the ceiling. A lockable protective casing must be installed here an access point is located in an unprotected public area e.g. a car park.

5.10. Remote access

Where there is a requirement for remote access to the internal network the following controls will be used:

- ☐ A Virtual Private Network (VPN) will be used providing session encryption using TLS 1.2+
- ☐ Multifactor authentication at the client where appropriate
- ☐ Secure authentication using a RADIUS server
- ☐ Network access control (NAC) will be used to restrict access to remote clients that do not meet minimum requirements e.g. virus control.

Remote access must be granted on an 'as required' basis rather than for all users by default.

5.11. Network intrusion detection

A Network-based Intrusion Detection System (NIDS) must be installed at the network perimeter and at all key points within the network e.g. on critical servers.

5.12. Network hardware

Where possible a single supplier policy will be used for network hardware. An exception will be made where the use of multiple vendor hardware may increase the level of security provided e.g. in a dual network-based firewall configuration.

CAT 6 UTP will be used for network cabling unless specific circumstances (such as excessive interference) preclude its use. The network topography used will be Ethernet according to the IEEE 802.3 family of standards.

5.13. IP addressing

IPv4 will be used on internal networks. However new network devices purchased must support IPv6 in preparation for the future.

IP addresses and associated network information for desktop and laptop clients will be controlled using DHCP, internal DNS servers will be used.

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

5.14. Network protocols

The protocol used on all networks will be TCP/IP. UDP will be used where appropriate, but other OSI layer 4 network protocols should not be used.

5.15. Network Security management

Once networks have been designed and implemented based on a clear set of security requirements, there is an ongoing responsibility to manage and control the secure networking environment to protect the organisation's information in systems and applications.

5.16. Roles and responsibilities

Roles and Responsibilities for the management and control of networks must be clearly defined. In order to provide effective segregation of duties, the operation of networks is managed separately from the operations of the rest of the infrastructure such as servers and applications. This segregation of duties is detailed in the following table.

Management role	Team	Main responsibilities
Network manager	Network team	- Design and implementation of new and changed networks - Installation and removal of networking equipment - Configuration of networking equipment - Third line incident management
Network operations manager	Network team	- Network availability monitoring - Network intrusion monitoring - Second line incident management - Configuration backups - Patching and updates - Setup and management of remote access users
Computer operations manager	System engineers' team, Monitoring team	- Server and application backups - Job scheduling - Infrastructure monitoring - First line incident management
Information Security team		- Defining and monitoring baseline security configurations for infrastructure elements.

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

5.17. Logging and monitoring

Logging levels on network devices must be configured, logs must be pushed to SIEM platform, monitored on a regular basis and stored for at least 12 months.

Firewall logs will be monitored for signs of excessive port scanning which may be a precursor to a remote attack. Where installed, a Network-based Intrusion Detection System must be configured to alert the Network Operations team of this activity.

Network monitoring for availability may be achieved using appropriate SNMP-based network management tool (Zabbix) and recovery actions automated where possible.

Alerts from the Network Access Control (NAC) system must be addressed immediately to ensure that clients that do not meet minimum security requirements are only allowed access to a quarantined subset of systems on the network.

5.18. Network changes

All changes to network devices will be subject to the change management process and appropriate risk assessment, planning and back-out methods out in place. Configuration records must be updated whenever such changes are carried out so that a current and accurate picture of the network is always maintained.

5.19. Network security incidents

Network events which are deemed to be security incidents must be recorded and managed according to the company's incident response procedures.

6. Incident Response Plan

The Company has established an Incident Response Plan to ensure timely and effective response to information security incidents. Employees must report suspected security incidents immediately to their supervisor or the Information Security Officer. The response plan includes identification, containment, eradication, recovery, and lessons learned

7. Policy review

All ISMS-related policies and procedures are subject to review in the event of changes in the ISMS systems / processes, but not less than once a year.

8. Related documents, annexes

PLACE FOR LOGO	POLICY OF INFORMATION SECURITY	Code: PLC-001
		Version: 1.1

Annex 1. Information Handling Rules