

PROPRIETARY

Information Security
Information Security Policy
ISMS_PL_01
Release 1.0

Document Information

Company	JarvisDelivery B.V.
Division:	Information Security
Title:	Information Security Policy
No.:	ISMS_PL_01
File Name:	ISMS_PL_01_Information Security Policy
Release:	1.0
Date:	01.09.2025
Review Date:	01.09.2025
Author:	Information Security Manager
Agreed:	Chief Executive Officer
Status:	Approved

This copy of the document is controlled only if it is open through the internal portal of company

History of changes

Date	Release	Description	Author	Approver
01.09.2025	1.0	Initial development of the document.	Information Security Manager	Chief Executive Officer

1. Introduction

1.1.Objectives and Goals

JarvisDelivery B.V. (hereinafter - the Company, JarvisDelivery) develops, implements, maintains and supports an iGaming platform designed to provide the end users with the different types of Sports Betting, Egaming Betting, Casino Games, Slots, Live Casino, Live Bingo, Games of Skill and Chance, and Loot Boxes in accordance with SOA v1.0 dated 01/09/2025. Rapid growth in the targeted markets with continued information processing, exchange of information, required interconnected business environments, usage of service providers and high dependency on Information Technology contains a variety of continuity threats and vulnerabilities. This could involve an increasing reliance on information systems, an increasing use of external networks, rapid changes in technology, computer-based fraud, information theft, targeted and non-targeted hacking, and careless handling of information throughout all stages of internal processing.

In accordance with mandated organizational security requirements set forth and approved by management, JarvisDelivery has established and implemented Information Security Management System (ISMS) in order to document its best information security practices, ensure that critical and vital company information assets are readily available to authorized users. The Information Security Management System of JarvisDelivery meets the requirements of the international standard ISO/IEC 27001:2022.

This policy is designed to provide JarvisDelivery with a documented and formalized information security policy in accordance with Requirement 5.2 of the ISO/IEC 27001:2022 standard. Additionally, this policy also serves as the organisation's primary, enterprise-wide information security manual that defines JarvisDelivery security team activities and clarifies how the team is using best practices and international standards.

This comprehensive policy document is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on an annual basis for ensuring its adequacy and relevancy regarding JarvisDelivery needs and goals.

The security that can be achieved through technical means is limited and must be supported by appropriate management, business processes and procedures.

JarvisDelivery defines Information security as the preservation of the confidentiality, integrity and availability of information and information systems (digital and non-digital).

- **Confidentiality:** ensuring that the information is accessible only to those persons that have the authority to deal it;
- **Integrity:** safeguarding the accuracy, completeness and timeliness of information and processing methods;
- **Availability:** ensuring that the authorized users have access to the information and associated assets on time and when necessary. The availability, integrity and confidentiality of information are essential in maintaining our competitive edge, our cash flow, profitability, legal compliance and respected company image.

JarvisDelivery defines its objectives as following:

1. System Availability/down time;
2. Minimizing bugs, i.e. tracking incidents that require code fixes; and
3. Code reviews.

The above-mentioned objectives are measured according to the relevant monitoring activities and reported based on the requirements of *ISMS_PR_01_Annual Information Security and Management Review Procedure*.

1.2.ISMS Scope

The Information Security Management System at JarvisDelivery applies to the provision of a full cycle of maintaining and deploying of JarvisDelivery software code & infrastructure with related supporting activities.

1.3.Governance

The responsibility of managing the Policy is assigned to the Information Security Manager of the JarvisDelivery. The developed Policy is submitted to the Chief Executive Officer for final approval. The Chief Executive Officer will be annually informed about subjects concerning the Policy.

2. Policy

Keeping crucial information exclusively for JarvisDelivery is mostly a matter of attitude and behavior, besides technical countermeasures with regard to IT and/or physical environments.

The strategic vision of JarvisDelivery is to become increasingly integrated with all its systems. The need to protect information assets becomes more demanding and challenging in an integrated and dynamic business environment

JarvisDelivery is aiming to create a flexible structure whereby information security becomes an integral part of the daily processes (business core activities) and behavior. To achieve this structure, business process engineering and staff (awareness) training will require high priority next to JarvisDelivery's minimum-security baseline enforcement.

The international standards – ISO/IEC 27001:2022 - Information technology -- Security techniques -- Information security management systems – Requirements and ISO/IEC 27002:2022 -- Code of Practice for Information Security Management has been chosen as a guide to implement ISMS within JarvisDelivery.

JarvisDelivery Information Security Policy is the umbrella policy, determines the roadmap, and provides the senior guidance for managing information security within JarvisDelivery.

JarvisDelivery Information Security Policy also provides management direction and support for information security in accordance with business requirements and relevant laws and regulations.

2.1.Organisation of Information Security

JarvisDelivery should build a structure for the organisation of information security, define and distribute related roles and responsibilities to manage, discuss, and approve items and issues concerning information security.

The Chief Executive Officer is responsible for Information Risks across JarvisDelivery with one employee having specific accountability for Information Risk Management, supported by the Information Security Manager.

A risk management framework and organisation of information security shall be established to manage Information Security Coordination within JarvisDelivery.

Related Document(s):

ISMS_GL_02_Information Security and Data Protection Governance Regulations

2.2.Information Security Risk Management

JarvisDelivery shall identify, evaluate and prioritize the threats of information security risks.

JarvisDelivery shall pursue to create a minimum-security baseline, where all business lines need to comply with the set minimum baseline.

Desirably, JarvisDelivery's Information Security Policy should be mainly based on detection/spot, rather than limiting and prohibiting, in order to control the information risks.

The application of protection measures is based on the risks associated with the information assets and processes and the importance of those assets to JarvisDelivery's processes and objectives.

To identify the risk level, periodic risk assessments shall be scheduled to minimize those risks that are determined to pose an unacceptable level of risk (Risk Treatment) for JarvisDelivery.

Related Documents:

ISMS_PR_03_Risk Assessment and Treatment Procedure

2.3.Human Resources Security

2.3.1.Roles and Responsibilities related to Information Security

JarvisDelivery shall define and document the security roles and responsibilities of JarvisDelivery employees, contractors and third-party users in their job descriptions including Information Asset Valuation and Incident Reporting.

When defining the security responsibilities of the employees, segregation of duties principle shall be considered and applied where possible to prevent misuse or abuse of JarvisDelivery resources and systems as depending on one individual.

2.3.2.Screening

Where legally applicable, all the employees and contractors of JarvisDelivery who have applied for a job or will be hired for a job that requires privileged access rights to critical systems or to process confidential JarvisDelivery data shall be checked for screening controls (this includes also temporary personnel and third-party personnel).

2.3.3.Information Security Training and Awareness

All employees and contractors, and third-party users shall receive appropriate security awareness training, education and regular updates in organisational policies and procedures as it pertains to their job function.

2.3.4.Disciplinary Process

A well-defined disciplinary process shall be in place to activate in case of noncompliance with JarvisDelivery policies and procedures.

Related Documents:

ISMS_PL_06_Human Resources Security Policy

2.4.Information Asset Management

JarvisDelivery shall provide and maintain appropriate protection of organisational information assets by managing controls over the information asset inventory and related ownership assignments to assets and proper classification and labelling of the information resides on these assets.

Related Documents:

ISMS_PR_05_Information Assets and Media Handling Procedure

ISMS_PL_08_Acceptable Use Policy

2.5.Access Control

JarvisDelivery shall take both logical and physical access control where information-processing activities are performed, and facilities are located. The access control rights shall be assigned according to "need-to-know" principle and these rights shall be periodically reviewed. Principles for accessing network resources shall be obtained and applied.

JarvisDelivery will maintain a solution to monitor and report malicious network activity. Review logs for unusual activity or anomalies and ensure that an annual penetration test is carried out by third party specialists.

All users shall be informed and trained to prevent unauthorised access and information leakage.

Third party access to JarvisDelivery systems and teleworking of employees shall be limited and controlled.

Related Documents:

ISMS_PL_02_Access Control Policy

2.6.Cryptography

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information JarvisDelivery takes appropriate cryptographic controls across the organisation, including AWS Encryption SDK requirements and the general principles under which business information must be protected to achieve information security objectives:

- confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
- integrity/authenticity: using digital signature or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information;
- non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;
- authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transaction with system users, entities and resources.

Related Documents:

ISMS_PL_04_Cryptography Policy

2.7.Physical and Environmental Security

To prevent unauthorised physical access, damage, and interference to the organisation's assets and information, JarvisDelivery takes the appropriate controls according to the classification level of data located and processed within the Company.

Protection of the assets is necessary to reduce the risk of unauthorised access to information and to protect information assets against loss or damage.

Related Documents:

ISMS_PL_10_Physical and Environmental Security Policy

2.8.Operations Security

JarvisDelivery shall create necessary procedures for appropriate and secure use of information processing systems and shall ensure proper capacity planning to prevent interruptions of information processing facilities.

Changes to the organisation, business processes, information processing facilities and systems that affect information security must be controlled. JarvisDelivery shall create the necessary procedures to ensure satisfactory control of all changes.

The Security Monitoring System shall be in place to detect unauthorised activities and collected logs shall be properly correlated and investigated with alarm functionalities.

JarvisDelivery shall ensure that the detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures are in place.

Backup copies of information, software and system images must be taken and tested regularly in accordance with an agreed backup policy.

Related Documents:

ISMS_PL_03_Change Management Policy

ISMS_PL_05_Cyber Security Policy

ISMS_PL_07_Information Backup Policy

2.9. Communications Security

JarvisDelivery computer networks shall be secured, and information shall be backed up properly to increase the availability of the information and ensure the protection of information in networks and their supporting information processing facilities.

JarvisDelivery shall identify and include in network services agreements security mechanisms, service levels and management requirements of all network services whether these services are provided in-house or outsourced.

Related Documents:

ISMS_PL_11_Network Security Policy

2.10. Information Systems Acquisition, Development and Maintenance

JarvisDelivery should consider defining the security requirements in the analysis phase for developing or acquiring software and should establish system acceptance criteria for the information systems and applications.

JarvisDelivery shall maintain the security of application system software and information. Project and support environments (test, development and production) shall be strictly controlled. Change Management and Configuration Management process shall be used for proper management of new versions and upgrades of software used.

The information involved in electronic commerce passing over the network shall be protected from fraudulent activity, contract dispute, and any unauthorised access or modification.

Related Documents

ISMS_GL_03_Secure Development Guideline

2.11. Supplier relationship

JarvisDelivery shall agree with the supplier and document information security requirements for mitigation of the risks associated with the supplier's access to the organisation's assets. All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for JarvisDelivery's information.

To maintain an agreed level of information security and service delivery in line with supplier agreements, JarvisDelivery shall regularly monitor review and audit supplier service delivery.

Related Documents

ISMS_GL_04_Third Parties Security Principles Guideline

2.12. Information Security Incident Management

JarvisDelivery shall establish a framework for managing security incidents with effective and efficient incident response and should provide ways for all employees and contractors to report security incidents and weaknesses. The reported incidents shall be recorded and responded to and lessons learned shall be examined.

Related Documents

ISMS_PL_09_Information Security Incident Management Policy

2.13. Business Continuity Planning

JarvisDelivery shall create and manage the framework that addresses the continuity of JarvisDelivery business processes.

This framework shall enable a plan that provides proper protection and timely recovery against disruptions of critical services. This plan shall be periodically tested and maintained according to changes.

Related Documents

BCMS_PLN_01_Business Continuity Plan

2.14. Compliance

JarvisDelivery shall have due diligence approximation and consider all relevant Curacao legislative, statutory, regulatory, contractual requirements and organisational approach to meet the requirements.

All JarvisDelivery employees shall act according to relevant Curacao laws, regulations, intellectual property rights, license agreements and the policies/procedures applicable within JarvisDelivery. They shall also be responsible for protecting company information and processing information according to confidentiality levels.

JarvisDelivery operations are bound by the requirements of the relevant Curacao laws and regulations, that are mentioned in the *ISMS_GL_01_Information Security Context, Requirements and Scope Manual*.

3. Policy Enforcement

It is the responsibility of all employees and contractors of JarvisDelivery to comply with the information security policies of JarvisDelivery and to ensure timely implementation.

Unruly acts that result from gross negligence are classified as serious security incidents. The following categories are defined as serious violations, if they fall under one or more of the following categories:

- if behavior or act results in: use of corporate information and assets for illegal purposes;
- if behavior or act results in: unauthorised access to information;
- if behavior or act results in: unauthorised modification of information;
- if behavior or act results in: harming the reputation of JarvisDelivery;
- if behavior or act results in: harming people and bringing JarvisDelivery owners at risk;
- if behavior or act results in: jeopardizing the security of employees, business partners, customers and JarvisDelivery assets;
- If behavior or act results in: consciously exposing JarvisDelivery to an actual or potential loss or loss of opportunities as a result of the security of data or business information being placed at risk.

Failure to comply with or intentionally violating JarvisDelivery's information security policies and standards may result in measures being taken, but must not be limited to the following:

- Disciplinary measures, up to and including termination of employment or service agreements;
- Measures under labor and/or civil law;
- Recovery of damages.

Any knowledge of a security breach must be reported immediately to the Information Security Manager, using designated communication channels.

4. Deviation from the Policy

Deviation from JarvisDelivery policies, standards and baselines are only allowed under exceptional circumstances whereby the contractor and/or employee is unable to comply with the requirements of the policy or with a segment of the policy.

Possible unique circumstances are identified as follows:

- Local legal and regulatory requirements;
- Limitation and/or circumstances due to geographical location;
- Product availability;
- Other specific condition(s), (which is/are not mentioned under this list).

In all events/cases where the contractor and/or employee is unable to comply with JarvisDelivery security policy, this contractor and/or employee is required to report this to the Information Security Manager.