

RoyceRose N.V.

Zuikertuintjeweg Z/N (Zuikertuin Tower), Curaçao

RoyceRose N.V.

Information Security Policy

Date: 4th February 2026

Version: 1.0

Status: Original

Classification: Sensitive

Distribution: All staff, contractors and managed service providers

Document Owner: Mr. Chun Fan Hsiao (CTO)

RoyceRose N.V.

Zuikertuintjeweg Z/N (Zuikertuin Tower), Curaçao

Version History

Version	Creation Date	Author/Prepared By	Change reason/ Comments
1.0	2026	Original	Original

Table of Contents

Version History	2
1. Information Security Policy	5
1.1.1 Scope	5
1.1.2 Applicability	6
1.1.3 Enforcement	6
1.1.4 Objectives	6
1.1.5 Exceptions	6
1.2 Security risk assessment	7
1.3 Access controls	7
1.3.1 Enforcement and Exceptions	8
1.3.2 User Management	8
1.3.3 Joiners, Movers and Leavers	8
1.3.4 Restricted Physical Access & Controls	9
1.3.5 Visitor Access	9
1.3.6 Remote Access for Users	9
1.3.6.1 Remote Work Security	9
1.3.7 Session Time-Out	10
1.3.8 Password Management	10
1.3.9 Training and Awareness	10
1.3.10 Device and Equipment Management	10
1.3.11 Usage of Personal Devices	11
1.3.12 Remote Data Wipe	11
1.4 Disposal	11
1.5 Safeguarding of Applications	12
1.5.1 Application Security	12
1.6 Safeguarding of equipment	12
1.7 Network Security, Remote Access and Endpoint Protection	13

1.7.1 Multi-Factor Authentication (MFA)	13
1.7.2 Patch Management and Software Updates	13
1.7.3 Least Privilege Access Model	13
1.7.4 Remote Access Monitoring and Intrusion Detection	13
1.7.5 Endpoint and Malware Protection	13
1.7.6 Email Use	14
1.8 Information Asset Management	14
1.9 Retention	14
1.10 Backup	14
1.11 Information Classification	14
1.12 Document Review and Approval	15

1. Information Security Policy

Introduction

RoyceRose N.V. (“RoyceRose” or “the Company”) is licensed by the Curaçao Gaming Control Board (GCB) under the National Ordinance for Games of Chance (LOK) to provide gaming-related services in a business-to-business (B2B) capacity.

This Information Security Policy sets out the minimum information security controls applicable to the Company’s operations and information assets. The Policy is designed to meet applicable Curaçao regulatory requirements and to support a risk-based and proportionate approach to information security, taking into account the Company’s B2B operating model and the nature of its services.

Scope and Objectives

1.1.1 Scope

This Policy establishes the framework for protecting the confidentiality, integrity, and availability of the Company’s information assets in accordance with applicable laws and regulatory requirements in Curaçao.

It applies to all employees, directors, contractors, and relevant third parties who access, process, or manage Company information as part of the Company’s B2B gaming supply activities. Failure to adequately safeguard information assets may result in unauthorised access, use, disclosure, alteration, or loss of information and may expose the Company to regulatory, contractual, operational, and reputational risks.

This Policy applies to all information in the possession or control of RoyceRose N.V., regardless of the form in which it is held. It covers all systems, services, and assets that support the Company’s licensed operations under its Curaçao B2B gaming licence, including but not limited to:

- Cloud-based gaming and related systems, in both production and non-production environments.
- Corporate IT services, including email, collaboration tools, document storage, and identity and access management systems.
- Software development environments, source code repositories, and deployment pipelines.

- End-user devices (laptops, desktops, and mobile devices) issued, managed, or expressly approved by the Company.
- Third-party services and integrations where Company information is accessed, processed, transmitted, or stored.

1.1.2 Applicability

This policy applies to:

- All RoyceRose N.V. employees, regardless of role or location.
- Contractors, consultants, and temporary staff engaged by RoyceRose N.V..
- Third-party suppliers and service providers who access RoyceRose N.V. systems, networks, or data in connection with its licensed activities under the Curaçao gaming regulatory framework.

1.1.3 Enforcement

Compliance with this Policy is mandatory. Any actual or suspected breach of this Policy shall be reviewed and addressed in accordance with the Company's internal procedures and applicable Curaçao laws, licence conditions, and directives issued by the Curaçao Gaming Control Board.

Where appropriate, breaches may result in disciplinary action, contractual remedies, or other corrective measures proportionate to the nature and severity of the incident.

1.1.4 Objectives

The objective of this Policy is to protect the Company's information and systems from unauthorised access, loss, or misuse by applying reasonable and proportionate security controls.

The Company manages information security risks by identifying relevant threats and vulnerabilities and applying controls to maintain:

- Confidentiality – information is accessed only by authorised persons.
- Integrity – information is accurate and protected from unauthorised change.
- Availability – systems and data are available to authorised users when needed.

1.1.5 Exceptions

Exceptions to this Policy may be approved by the Chief Technology Officer (CTO) or an authorised delegate where required for business or operational reasons.

All exceptions should be appropriately recorded, limited in scope, and reviewed as appropriate. Records of approved exceptions shall be retained by the Company and provided to the Curaçao Gaming Control Board or other competent authorities upon lawful request.

1.2 Security risk assessment

RoyceRose N.V. identifies and manages information security risks in order to protect its information assets and systems.

Security risks are assessed by considering the likelihood and potential impact of threats affecting the Company's information, systems, and services. Risk assessments are performed when necessary, including where material changes occur to systems, infrastructure, third-party arrangements, or business operations.

Identified risks are recorded and monitored, and appropriate actions are taken to reduce risks to an acceptable level. The Chief Technology Officer (CTO) is responsible for overseeing information security risk management and for escalating material risks to senior management where appropriate. Information security risks and related mitigation measures are maintained as part of the Company's internal records.

1.3 Access controls

Access to the Company's information systems is granted strictly on a need-to-know basis and in accordance with the principle of least privilege. Access is provided only to individuals who have a valid contractual relationship with the Company and who are subject to appropriate confidentiality obligations.

User access rights are assigned based on role and responsibilities and are updated or removed when roles change or when access is no longer required. Administrative or privileged access is restricted to authorised personnel and granted only where necessary for operational purposes.

Access requests must be approved by appropriate management. Accounts that are no longer required, inactive, or associated with former personnel are disabled or removed without undue delay. User access approvals and removals are documented and performed in a timely manner.

Policies and procedures supporting access control and user management are maintained internally and reviewed as needed to remain appropriate for the Company's operations and Curaçao regulatory expectations.

1.3.1 Enforcement and Exceptions

Compliance with access control requirements is mandatory. Any breach or attempt to bypass access controls may result in disciplinary or contractual action.

Exceptions may be approved by the Chief Technology Officer (CTO) or an authorised delegate where justified by business needs. Approved exceptions must be documented, limited in scope, and reviewed as appropriate.

1.3.2 User Management

All access to Company information, resources, and services as well as physical access shall be restricted and controlled in accordance with the principle of least privilege and applicable Curaçao regulatory requirements.

Access to system documentation, software applications, logs, personal data, business-sensitive information, and intellectual property ("IP") shall be granted strictly on a need-to-know and need-to-use basis, taking into account risk assessments and applicable laws and regulations.

User access rights shall be assigned based on defined roles and responsibilities and shall be subject to formal approval, periodic review, and timely revocation through an access control process. Access shall be limited to those systems, networks, and services that are necessary for the performance of the user's authorised duties.

All employees, contractors, and third-party service providers shall be required to enter into appropriate contractual arrangements, including confidentiality and data protection obligations, prior to being granted access to Company information or systems. Where access is provided to personnel of third-party organisations, such access shall be governed by written agreements signed by the relevant legal representatives, and additional non-disclosure or data processing agreements may be required as appropriate.

1.3.3 Joiners, Movers and Leavers

Access rights for users are granted based on business need and the principle of least privilege.

Where a user's role, responsibilities, or engagement status changes, access rights are reviewed and adjusted accordingly. Access that is no longer required is revoked in a timely manner.

When a user's employment or engagement with the Company ends, access to Company systems and information is revoked promptly in accordance with internal procedures. Any reactivation of access requires appropriate authorisation.

1.3.4 Restricted Physical Access & Controls

Where the Company operates or utilises physical premises, reasonable measures are applied to restrict unauthorised physical access to areas where Company information or systems may be accessed.

Physical access to any server hosting facilities, data centres, or third-party co-location environments used by the Company is restricted and managed by the relevant service providers in accordance with their security controls and contractual arrangements.

Access to Company premises, where applicable, is limited to authorised personnel and visitors, and reasonable steps are taken to prevent unauthorised access. Employees are expected to remain vigilant and to report suspicious activity where identified.

1.3.5 Visitor Access

Where the Company operates or utilises physical premises, visitor access is managed in a manner intended to prevent unauthorised access to Company information or systems. Reasonable measures are applied to supervise visitors where access to sensitive areas may occur.

1.3.6 Remote Access for Users

The Company operates a remote-working model. Remote access to Company systems is restricted to authorised users and is protected by appropriate security controls, such as secure remote access mechanisms and multi-factor authentication, where applicable.

Remote access is granted based on business need and revoked when no longer required. Reasonable measures are applied to ensure that remote access does not expose Company information or systems to undue risk.

1.3.6.1 Remote Work Security

Where work is performed outside controlled office environments, users are expected to take reasonable steps to protect Company information from unauthorised access, loss, or disclosure.

Company-issued or approved devices are intended for use only by the authorised user, and access credentials must not be shared.

1.3.7 Session Time-Out

Reasonable session management controls are applied to Company systems to reduce the risk of unauthorised access due to inactivity, taking into account system capabilities and security risk.

1.3.8 Password Management

Appropriate authentication controls are applied to protect access to Company systems and information. Users are required to use strong, unique credentials and must protect authentication information from unauthorised disclosure.

Where applicable, additional controls such as multi-factor authentication are used to enhance security. Password and access management practices are implemented in a manner proportionate to system risk and operational requirements.

1.3.9 Training and Awareness

RoyceRose N.V. promotes information security awareness among its employees and contractors to support the secure handling of Company information.

Information security awareness measures may be provided as part of onboarding and on an ongoing basis, taking into account the Company's operations, risk profile, and Curaçao regulatory expectations. Awareness topics may include general information security responsibilities, common cyber threats, and good security practices relevant to the Company's activities.

Where appropriate, additional awareness activities may be implemented to reinforce secure behaviour.

1.3.10 Device and Equipment Management

Company-issued or approved devices may be used to access Company systems and information. Users are expected to take reasonable steps to protect devices from loss, theft, damage, or unauthorised access.

Where portable or removable devices are used, appropriate safeguards are applied based on risk. Users are required to promptly report lost, stolen, or compromised devices so that appropriate protective measures can be taken.

1.3.11 Usage of Personal Devices

Limited access to Company systems or information may be permitted using personal devices where authorised. Such access may be restricted or revoked where security risks are identified or where continued use is no longer appropriate.

1.3.12 Remote Data Wipe

Where access to Company information is permitted using Company-owned or personal devices, reasonable measures may be applied to protect Company information in the event of loss, theft, or suspected compromise of a device.

Users are required to promptly notify the Company where a device used to access Company information is lost, stolen, or reasonably suspected to be compromised. Following such notification, appropriate protective actions may be taken to reduce the risk of unauthorised access to Company information, taking into account technical feasibility and proportionality.

1.4 Disposal

The disposal of electronic records, storage media, and information-processing equipment may present information security risks if not handled appropriately. RoyceRose N.V. applies reasonable and proportionate measures to ensure that Company Information is not inadvertently disclosed, lost, or misused during disposal, reuse, or transfer of media and equipment.

This Policy applies to Company-owned or Company-approved fixed and removable storage media and equipment, including electronic storage devices, endpoints, and any future storage technologies used by the Company.

Responsibility for the disposal of media and equipment is assigned to authorised personnel. Disposal methods are selected based on a risk-based assessment, taking into account the sensitivity of the information and the intended disposition of the media or equipment.

Prior to reuse, redeployment, donation, sale, or disposal, reasonable steps are taken to ensure that Company Information, credentials, and residual data are securely removed or rendered inaccessible. Where sanitisation methods are assessed as insufficient due to the condition or nature of the media, physical destruction may be used as an alternative.

Disposal activities are performed in accordance with recognised information security good practices and applicable regulatory expectations. Where third-party disposal services are used, the Company ensures that such services are appropriate to the sensitivity of the information involved.

Records relating to disposal activities are maintained to an extent appropriate to the Company's operations and risk profile.

1.5 Safeguarding of Applications

1.5.1 Application Security

Application security is considered as part of the Company's software development and maintenance activities. Applications developed, maintained, or materially modified by the Company are designed and implemented with appropriate consideration for the confidentiality, integrity, and availability of information.

Security considerations are taken into account during the design and development of applications, particularly where applications support business-critical functions or process sensitive information. Relevant security risks are identified and addressed in a manner proportionate to the nature and use of the application prior to deployment.

Changes to core application functionality are subject to appropriate review before release. Application changes with potential security implications may be reviewed and approved by authorised personnel.

Reasonable testing may be performed to identify common security weaknesses prior to deployment, taking into account the application's risk profile. Developers are expected to maintain awareness of common application security risks relevant to their role.

Test or development functionality is not intended to be enabled in production environments. Access to management or administrative interfaces is restricted and protected by appropriate access controls.

Third-party libraries, frameworks, and components used within Company applications are considered as part of application security and are reviewed where appropriate. Applications supporting critical business functions may be subject to additional security review based on risk and operational requirements.

1.6 Safeguarding of equipment

The Company's core systems are hosted using cloud-based infrastructure provided by third-party service providers. Physical security of the underlying cloud infrastructure is managed by the relevant service providers in accordance with their security controls and contractual arrangements.

The Company is responsible for the secure configuration, access control, and use of its systems and data within the cloud environment, in line with its operating model and risk profile.

1.7 Network Security, Remote Access and Endpoint Protection

The Company operates a remote-working model. Remote access to Company systems is restricted to authorised users and protected by appropriate network security controls, such as secure remote access technologies.

Network access is configured in accordance with the principle of least privilege. Reasonable monitoring may be applied to detect unauthorised access or security issues, taking into account proportionality and operational requirements.

1.7.1 Multi-Factor Authentication (MFA)

Multi-factor authentication is applied to systems processing sensitive or business-critical information, where appropriate. Equivalent authentication solutions may be used to provide an adequate level of security.

1.7.2 Patch Management and Software Updates

Reasonable measures are taken to keep systems and software up to date with relevant security patches, taking into account the criticality of vulnerabilities and operational risk.

1.7.3 Least Privilege Access Model

The principle of least privilege is applied across Company systems and repositories. Access rights are granted based on role and business need and adjusted where responsibilities change. Elevated access is restricted to authorised users.

1.7.4 Remote Access Monitoring and Intrusion Detection

Appropriate monitoring and detection measures may be applied to identify and reduce the risk of unauthorised access, particularly in relation to remote access. Where suspicious activity is identified, reasonable technical or procedural controls may be applied to limit further access and reduce security risk.

1.7.5 Endpoint and Malware Protection

Appropriate measures are applied to protect Company-issued or approved devices from malware and other common security threats. Endpoint protection solutions may be used where appropriate and kept up to date in line with system requirements. Users are expected not to intentionally introduce malicious code and to promptly report suspected security issues.

1.7.6 Email Use

The Company's corporate email system is provided for business purposes. Limited personal use is permitted provided it does not interfere with business operations or security. Users are expected to exercise due care when sending emails and to report suspicious or potentially malicious messages.

1.8 Information Asset Management

Company information assets are managed in a manner intended to reduce the risk of unauthorised access, loss, or disclosure. Users are expected to handle Company information responsibly and in accordance with applicable security requirements.

1.9 Retention

Company Information is retained in accordance with applicable legal, regulatory, and business requirements, and in line with the Company's Information Retention Policy.

Information is not retained for longer than reasonably necessary for its intended purpose, unless a legitimate legal or operational reason exists. Access to retained information is restricted to authorised persons.

1.10 Backup

Appropriate backup measures are implemented to support the availability and recoverability of systems and data supporting the Company's licensed activities.

Backups are performed and stored in a secure manner, taking into account the criticality of systems and information. Backup practices are implemented proportionately and in line with operational and risk considerations.

1.11 Information Classification

Company Information has varying degrees of sensitivity and criticality. The higher the value of the Company Information and the higher the sensitivity, the greater the security required. Company Information must first be valued. Once a value has been given, a classification can be established and a corresponding security level can be identified and implemented.

When determining the value and classification of Company Information, the following factors shall be taken into consideration.

- the level of sensitivity and confidentiality of the information;
- the potential impact on the Company in the event of unauthorised disclosure, alteration, or loss;
- potential financial, operational, legal, and regulatory implications, including obligations under applicable Curaçao laws and regulatory requirements;
- the business need for sharing, restricting, or retaining access to the information.

The Company has defined the following information classifications:

- Confidential: Company Information classified as Confidential must be highly secured and remain private. If disclosed, Confidential Company Information would significantly impact the business.
- Sensitive: Company Information marked as Sensitive should be adequately secured. Sensitive information can be shared internally but not externally.
- Public: Company Information which can be shared externally.

All employees, contractors, and third parties with access to Company Information are required to handle, store, transmit, and dispose of information in accordance with its assigned classification and the applicable Curaçao information security, data protection, and retention policies.

1.12 Document Review and Approval

This Policy is reviewed periodically and updated where necessary to ensure it remains appropriate for the Company's operations, risk profile, and applicable Curaçao regulatory expectations.

Any material updates to this Policy are subject to management review and approval in accordance with the Company's internal governance arrangements.

Compliance with this Policy is monitored through management oversight and appropriate internal controls. Where material issues are identified, reasonable corrective actions may be taken, proportionate to the nature and impact of the issue.