

Miranda Path B.V.

Information Technology Policy

Version 1.0



Internal

DOCUMENT CONTROL

Version Number	Date	Author	Details and Reasons for Change
1.0			Version 1 of the document to create a new policy.

1. Purpose

The purpose of this IT Policy is to ensure the **secure, reliable, and compliant** operation of Miranda Path's IT systems and services, including business-critical gaming platforms. This policy establishes guidelines for IT operations, data protection, access control, and disaster recovery, in line with regulatory requirements in Curaçao.

2. Scope

This policy applies to:

- All employees, contractors, and third-party vendors (including outsourced IT support) accessing company IT systems.
- All hardware, software, networks, and data owned or operated by Miranda Path.
- All business-critical gaming services, including B2B platforms, APIs, databases, and supporting infrastructure.

3. IT Governance

- The IT Department (and its designated outsourced support partners) is responsible for implementing, maintaining, and monitoring this policy.
- Compliance with Curaçao eGaming regulatory requirements is mandatory.
- Regular audits of IT systems and processes will be conducted to ensure security and compliance.

4. Information Security and Classification

To manage information risk effectively, all company data must be classified and handled according to its sensitivity.

4.1. Information Classification

All information and data assets shall be assigned one of the following classification levels, dictating the required level of protection:

Classification	Definition	Examples
Public	Information approved for general public disclosure.	Marketing materials, public website content.
Internal	Information for staff and internal business use only. Disclosure would not cause material harm.	Internal memos, general procedures.
Restricted	Information that is sensitive and proprietary. Unauthorized disclosure could result in moderate business risk or minor regulatory non-compliance.	Internal IT documentation, audit reports, employee performance reviews.
Confidential	Information that is highly sensitive. Unauthorized disclosure would result in severe financial loss, legal liability, or major regulatory non-compliance (e.g., player data, financial reports).	Player records, payment data, proprietary source code, license keys.

4.2. Handling Classified Information

- Access controls must be strictly enforced based on the principle of **least privilege** and the data's classification level.
- Data classified as **Confidential** must be encrypted both in transit and at rest.

5. Access Control

- User accounts must be unique and protected with strong passwords and multi-factor authentication (MFA) where possible.
- Access to sensitive data, gaming platforms, and administrative functions must follow the principle of least privilege.
- Terminated employees or contractors must have system access revoked immediately.

5.1. Password Complexity Requirements

Passwords shall conform to the following rules:

1. **Minimum Length:** Shall be at least **8 characters** long.

2. **Uniqueness:** Shall not contain part of the user's name or account name.
3. **Character Set:** Shall contain characters from at least **three** of the following four categories:
 - English uppercase letters (A-Z)
 - English lowercase letters (a-z)
 - Numerical digits (0-9)
 - Special characters (e.g., \$!#%)

6. User Management Policy

This section defines the lifecycle management of user accounts to ensure only authorized personnel have access to IT resources.

- **Provisioning:** All user access must be formally requested and authorized by the respective department head or management before account creation. Access must be granted based on the **Principle of Least Privilege**.
- **Review:** User access rights must be formally reviewed by management at least quarterly to confirm continued business necessity.
- **Termination:** Upon an employee's or contractor's termination, all accounts, physical access, and credentials (including tokens) must be disabled and revoked immediately, verified by the IT department/Outsourced IT Provider.
- **Service Accounts:** Shared or generic accounts are strictly prohibited, except for documented and approved service accounts. Service account credentials must be managed via a secured vault and reviewed monthly.

7. Data Protection

- All personal and financial data must be stored securely and encrypted in transit and at rest.
- Backups must be performed daily, stored in secure, geographically separated locations, and tested regularly.
- Data retention and disposal must comply with regulatory and contractual requirements.

8. System Security

- Antivirus, firewall, and intrusion detection systems must be deployed and regularly updated.
 - Security patches for software and hardware must be applied in a timely manner.
 - Vulnerability assessments and penetration tests must be conducted at least **annually** by an independent third party.
-

9. Asset Management System

Miranda Path shall maintain a comprehensive inventory of all IT assets to support security, maintenance, and accountability.

- **Inventory:** A definitive inventory of all hardware (servers, endpoints, networking equipment) and software assets (licenses, proprietary applications) must be maintained and updated within 24 hours of any change.
- **Asset Tracking:** All assets shall be tagged and tracked from acquisition through disposal.
- **Ownership:** Each asset must have a designated owner responsible for its security and proper use.
- **Configuration Baseline:** All operational systems must adhere to a documented and approved security configuration baseline (e.g., standard OS hardening, minimum ports open).
- **Disposal:** Assets containing data must undergo secure data sanitization (e.g., physical destruction or documented secure wiping) before disposal or repurposing.

10. Incident Management

- All IT security incidents must be reported immediately to the IT Department.
- A formal incident response plan must be maintained, including investigation, containment, mitigation, and reporting.
- Serious incidents must be reported to Curaçao eGaming as required by regulations.

11. Disaster Recovery (DR) and Business Continuity

11.1. Objective

To ensure continuity of business operations and minimize downtime in the event of a disaster, cyber-attack, or system failure.

11.2. Disaster Recovery Plan

- **Critical Systems:** Identify and prioritize all critical gaming platforms, databases, and services.
- **Backup Procedures:** Daily backups stored offsite and tested for restoration.
- **Recovery Time Objective (RTO):** Critical systems must be restored within 2 hours of an outage.
- **Recovery Point Objective (RPO):** Data loss must not exceed 15 minutes in the event of a disaster.
- **Disaster Scenarios:** Plan must cover cyber-attacks, hardware failure, natural disasters, and data corruption.
- **Roles and Responsibilities:** Assign a DR coordinator and team responsible for executing the plan.
- **Testing:** Conduct DR drills at least **twice per year** to validate readiness and update procedures.

11.3. Communication Plan

- Notify stakeholders, customers, and regulatory authorities in accordance with legal obligations.
- Maintain up-to-date contact information for all key personnel and vendors.

12. Third-Party Management

- All third-party vendors (including outsourced IT support) must comply with security and compliance requirements outlined in this policy.
- **Service Level Agreements (SLAs)** must include provisions for uptime, security, data ownership, liability, and disaster recovery support.
- **Security Vetting:** Annual security due diligence (e.g., review of security certifications, audit reports) must be performed on all critical third-party vendors.

13. Security Awareness and Behaviour

Miranda Path B.V. recognises that its people are the first line of defence against security threats. This section sets out the standards of behaviour expected of all personnel, and the specific policies governing the use of company systems, communications, and devices.

13.1. Acceptable Use Policy

All personnel are granted access to company IT systems solely for legitimate business purposes. The following rules apply to all use of company IT resources, including hardware, software, networks, and data:

- IT systems and resources must be used primarily for authorised business activities. Incidental personal use is permitted provided it is minimal, does not interfere with work, and complies with this policy.
- Personnel must not access, download, store, or distribute material that is illegal, offensive, discriminatory, defamatory, or in breach of copyright or other intellectual property rights.
- Accessing, modifying, or attempting to circumvent security controls, firewalls, or access restrictions is strictly prohibited.
- Installing unauthorised software, applications, or browser extensions on company devices is prohibited. All software installations must be approved by the IT Department.
- Personnel must not share their login credentials, access tokens, or passwords with any other individual under any circumstances.
- Company data must not be transferred to personal cloud storage, personal email accounts, or other unauthorised external services without explicit management approval.
- Any suspected security incident, unusual system behaviour, or potential policy breach must be reported immediately to the IT Department.

13.2. Email and Communications Use Policy

Company email and communication platforms (including instant messaging and collaboration tools) are provided for business use. The following rules govern their use:

- Company email accounts must not be used to send, forward, or receive material that is offensive, unlawful, harassing, or in breach of this policy.
- Personnel must exercise caution when opening email attachments or clicking links, particularly from unknown or unexpected senders. Suspected phishing emails must be reported to the IT Department immediately and must not be acted upon.
- Confidential or Restricted information must not be transmitted via unencrypted email. Where such information must be shared externally, approved secure file transfer methods must be used.
- Mass email communications or bulk messaging to external recipients must be authorised by management and must comply with applicable anti-spam legislation.
- Personnel must not attempt to mask or misrepresent their identity in electronic communications.
- Company email and communication systems may be monitored by the IT Department in accordance with applicable law and for the purposes of security, compliance, and investigation of policy breaches.

13.3. Personal and Mobile Devices Policy

The use of personal devices ("Bring Your Own Device" or BYOD) and company-issued mobile devices to access company systems or data is subject to the following requirements:

- Any personal device used to access company systems must be registered with and approved by the IT Department prior to use.
- All devices (company-issued and personal) used to access company data must have up-to-date operating system patches, antivirus software, and screen lock enabled with a PIN or biometric authentication.
- Confidential company data must not be stored locally on personal devices. Access should be via approved secure remote access methods only.
- Lost or stolen devices that have been used to access company systems must be reported to the IT Department immediately. The company reserves the right to remotely wipe company data from any registered device.
- Personnel must not connect personal devices to the company's internal network (wired or Wi-Fi) without prior IT Department approval.
- Upon leaving the company, all company data must be removed from personal devices, and company-issued devices must be returned to the IT Department.

14. Training

Miranda Path B.V. is committed to ensuring that all personnel have the knowledge and skills necessary to protect company information and systems. Security awareness training is a mandatory requirement for all staff.

- All new employees and contractors must complete an IT security induction as part of their onboarding process, prior to being granted access to company systems.
- All personnel must complete mandatory security awareness training at least annually. This training will cover topics including phishing awareness, password security, data handling, acceptable use, and incident reporting.

- Personnel with elevated access rights or roles with specific security responsibilities (e.g., IT administrators, finance staff) must receive additional role-specific security training appropriate to their responsibilities.
- Training completion records must be maintained by the IT Department or HR and made available upon request for audit or regulatory review purposes.
- The IT Department will issue periodic security awareness communications (e.g., bulletins, alerts) to keep personnel informed of emerging threats and updated best practices.
- Management is responsible for ensuring that members of their team complete all required training within the specified timeframes.

15. Responsibilities, Rights and Duties of Personnel

All personnel have both rights and responsibilities in relation to information security. The following sets out the key obligations and entitlements applicable to employees, contractors, and third-party users.

15.1. Responsibilities of All Personnel

- Read, understand, and comply with this IT Policy and any related policies, standards, or guidelines issued by the IT Department.
- Use company IT systems and data responsibly, in accordance with the Acceptable Use Policy set out in Section 13.1.
- Protect login credentials and report any suspicion that an account has been compromised to the IT Department without delay.
- Complete all mandatory security awareness training within the required timeframes.
- Report actual or suspected security incidents, policy violations, or vulnerabilities promptly in accordance with Section 10.
- Take reasonable care to protect company assets, including hardware, data, and intellectual property, from loss, theft, or damage.

15.2. Responsibilities of Management

- Ensure that all members of their team are aware of and comply with this policy.
- Formally authorise and review access rights for their direct reports in accordance with Section 6.
- Promptly notify the IT Department of changes in personnel status (including role changes, leavers, and new starters) to enable timely provisioning or revocation of access.
- Lead by example in adhering to this policy and fostering a culture of security awareness within their teams.

15.3. Responsibilities of the IT Department

- Implement, maintain, and enforce this policy and associated technical controls.
- Provision, maintain, and revoke system access in accordance with approved requests and the User Management Policy in Section 6.
- Deliver or coordinate the delivery of security awareness training as required by Section 14.
- Monitor systems and networks for security threats, incidents, and policy violations, and respond in accordance with the Incident Management policy in Section 10.

- Maintain documentation of IT assets, configurations, access rights, incidents, and training records.

15.4. Rights of Personnel

- Personnel have the right to receive clear information about which IT systems and data they are authorised to access, and the purposes for which monitoring of company systems is carried out.
- Personnel have the right to raise concerns about potential security vulnerabilities or policy breaches without fear of retaliation, through the company's whistleblowing or incident reporting channels.
- Personnel have the right to receive appropriate training and support to enable them to fulfil their security responsibilities.
- Where monitoring of communications or devices is carried out, this will be undertaken in a proportionate, lawful manner and in accordance with applicable data protection legislation.

16. Policy Compliance

- Violations of this policy may result in disciplinary action, up to and including termination.
- Management is responsible for ensuring all personnel understand and adhere to the policy.

17. Policy Review

- This policy will be reviewed annually or after significant changes to business operations, IT infrastructure, or regulatory requirements.