

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. 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.
-

14. Policy Review

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