

Information Security Policy

Version Control:

Version No	Purpose/Change	Prepared by	Date Prepared	Approved by	Date Approved
1	Basic document		August 12, 2025	The Board of Directors	September 25 th , 2025

1. Introduction and Purpose

This Information Security Policy (the "Policy") establishes the framework for protecting information assets within Progress Path Co N.V., an online gambling company operating under a license from Curaçao, in compliance with applicable laws including the General Data Protection Regulation (GDPR), where relevant, and the National Ordinance for the Protection of Personal Data (NOPPD).

The purpose of this Policy is to:

- Ensure the **confidentiality, integrity, and availability** of all information assets.
- Protect against unauthorized access, use, disclosure, modification, or destruction of information.
- Comply with all applicable laws, regulations, and licensing requirements, including those specific to online gambling and data protection in Curaçao.
- Establish a culture of security awareness among all employees, contractors, and third parties.
- Maintain the trust and confidence of our customers, regulators, and business partners.

2. Scope

This Policy applies to all information assets, systems, networks, applications, and services owned or operated by Progress Path Co N.V., regardless of their physical location. It covers all employees, contractors, consultants, temporary staff, and any third parties who have access to Progress Path Co N.V.'s information systems or data.

3. Information Security Objectives

Our primary information security objectives are:

- **Confidentiality:** Ensuring that information is accessible only to those authorized to have access. This includes protecting sensitive customer data, financial information, game algorithms, and proprietary business data.
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods. This involves preventing unauthorized modification or corruption of data, including game outcomes and transaction records.
- **Availability:** Ensuring that authorized users have access to information and associated assets when required. This includes maintaining continuous operation of our gaming platforms and payment systems.
- **Compliance:** Adhering to all relevant legal, regulatory, and contractual obligations, especially those related to responsible gaming, anti-money laundering (AML), and data privacy (e.g., GDPR principles, if applicable to data subjects).

4. GDPR Principles

Progress Path Co N.V. adheres to the principles of data protection set out in Article 5 of the GDPR. Personal data shall be:

- **Lawful, fair, and transparent:** processed on a valid legal basis, fairly, and transparently communicated to the data subject.
- **Purpose-limited:** collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Minimized:** adequate, relevant, and limited to what is necessary.
- **Accurate:** kept up to date, with inaccuracies corrected or deleted without delay.
- **Storage-limited:** retained only as long as necessary for the purposes for which it was collected.
- **Secure:** processed in a manner ensuring confidentiality, integrity, and availability.
- **Accountable:** Progress Path Co N.V. is responsible for and able to demonstrate compliance with these principles.

5. Roles and Responsibilities

- **Board of Directors/Senior Management:** Overall responsibility for information security, approving the Information Security Policy, and allocating necessary resources.
- **Information Security Officer (ISO)/IT Manager:** Responsible for developing, implementing, maintaining, and overseeing the Information Security Management System (ISMS). This includes conducting risk assessments, managing incidents, and ensuring compliance.
- **All Employees and Contractors:** Required to understand and adhere to this Policy and related security procedures. They are responsible for protecting information assets they handle and reporting any suspected security incidents.
- **IT Department:** Responsible for implementing technical security controls, managing infrastructure, monitoring systems, and responding to security incidents.
- **Legal & Compliance Department:** Ensures compliance with all relevant laws and regulations, advises on data protection, and manages regulatory interactions.

6. Statutory Confidentiality

In accordance with Article 14.1 of the LOK, all employees, contractors, and management are under a statutory obligation to maintain the confidentiality of player and company information, except where disclosure is mandated by law or regulatory authority. Breach of this duty may lead to criminal sanctions in addition to disciplinary action.

7. Information Classification and Handling

Information assets will be classified based on their sensitivity and criticality to the business. Classification levels may include:

- **Public:** Information intended for general public consumption.
- **Internal:** Information for internal use only, not to be disclosed outside the company without explicit authorization.
- **Confidential:** Sensitive information requiring restricted access, such as customer data, financial records, and intellectual property.
- **Restricted/Highly Confidential:** Extremely sensitive information (e.g., encryption keys, critical system configurations, proprietary game logic) with very limited access.

Handling procedures will be defined for each classification level, including storage, transmission, retention, and disposal.

8. Access Control

- **Principle of Least Privilege:** Users will be granted only the minimum access rights necessary to perform their job functions.
- **Unique User IDs:** All users will have unique identification credentials.
- **Strong Passwords/Authentication:** Strong password policies will be enforced, requiring complexity, regular changes, and protection against unauthorized disclosure. Multi-factor authentication (MFA) will be implemented for all critical systems and remote access.
- **Regular Reviews:** User access rights will be reviewed periodically and revoked promptly upon role change or termination.

9. Network Security

- **Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS):** Implemented to control network traffic and detect/prevent malicious activity.
- **Network Segmentation:** Critical systems will be isolated within secure network segments.
- **Secure Configurations:** Network devices will be configured securely according to industry best practices.
- **Vulnerability Management:** Regular vulnerability scans and penetration tests will be conducted.

10. System and Application Security

- **Secure Development Lifecycle (SDLC):** Security considerations will be integrated into all phases of the software development lifecycle.
- **Regular Patching:** Operating systems, applications, and firmware will be regularly updated with security patches.
- **Hardening:** Systems will be hardened by disabling unnecessary services and features.
- **Logging and Monitoring:** Comprehensive logging will be enabled for all critical systems and applications, and logs will be regularly reviewed for suspicious activity.

11. System Certification

All gaming equipment, application software, and remote games of chance offered shall be tested and certified for information security and integrity by an independent laboratory approved by the CGA, prior to being made available to players. Regular re-certification shall be conducted in line with CGA requirements.

12. Data Protection and Privacy

Progress Path Co N.V. is committed to protecting the privacy and personal data of its customers in accordance with applicable data protection laws.

- **Data Minimization:** Only necessary customer data will be collected and processed.
- **Consent:** Where required, explicit consent will be obtained for data processing.
- **Lawful Basis:** Personal data shall only be processed where a valid legal basis applies under GDPR, including: consent, performance of a contract, compliance with a legal obligation (e.g., AML/LOK requirements), or legitimate interests pursued by the Company or a third party, provided these are not overridden by data subject rights.
- **Special Category Data:** Sensitive personal data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, or sexual orientation, shall only be processed under the conditions of GDPR Article 9, such as explicit consent, legal obligations, or for the establishment, exercise, or defense of legal claims.
- **Encryption:** Sensitive data, especially customer personal and financial information, will be encrypted both in transit and at rest.
- **Data Retention:** Progress Path Co N.V. shall retain player registration records, gaming transactions, financial data, and related communications for a minimum of 5 years from the date of the last transaction, in compliance with the LOK and AML regulations. After expiration, data will be securely deleted or anonymized unless required for ongoing investigations.

- **Customer Rights:** Progress Path Co N.V. shall maintain procedures to enable customers to exercise their data protection rights under GDPR, including the rights to:
 - Access their personal data,
 - Rectify inaccurate or incomplete data,
 - Request erasure of data ("right to be forgotten"),
 - Restrict processing under specific conditions,
 - Data portability (receive their data in a structured, machine-readable format),
 - Object to certain processing activities, including direct marketing,
 - Not be subject to automated decision-making or profiling without meaningful human involvement, unless legally permitted.

13. Data Hosting and CGA Access

Progress Path Co N.V. shall ensure that all critical digital records, including players' personal data, gaming transactions, and financial records, are stored on a Tier-IV certified data center located in Curaçao, and remain accessible to the Curaçao Gaming Authority (CGA) at all times for audit, inspection, or investigation purposes.

14. Incident Management

A formal **Information Security Incident Response Plan** will be maintained to ensure a timely and effective response to security incidents. This plan will include procedures for:

- **Identification:** Detecting security incidents.
- **Containment:** Limiting the impact of incidents.
- **Eradication:** Removing the cause of the incident.
- **Recovery:** Restoring affected systems and data.
- **Post-Incident Review:** Analyzing incidents to prevent future occurrences.
- **Notification:** Timely notification to relevant authorities (e.g., Curaçao Gaming Authority) and affected individuals, as required by law.

15. Incident Reporting

Any information security breach, gaming system failure, or fraud attempt that compromises the confidentiality, integrity, or availability of player information or gaming systems shall be reported to the CGA **within 24 hours of detection**, accompanied by an incident report including:

- nature and scope of the incident,
- affected systems and categories of data,
- mitigation steps taken,
- corrective and preventative actions planned.

In circumstances where GDPR applies, Progress Path Co N.V. shall notify the competent data protection authority of a personal data breach within 72 hours of becoming aware of it, and shall notify affected data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

16. Business Continuity and Disaster Recovery

- **Backup and Recovery:** Regular backups of critical data and systems will be performed and tested periodically.
- **Disaster Recovery Plan (DRP):** A DRP will be in place and regularly tested to ensure the ability to resume critical business operations in the event of a major disruption.
- **Business Continuity Plan (BCP):** A BCP will address how critical business functions will continue during and after an incident.

17. Employee Security Awareness and Training

- **Mandatory Training:** All employees will receive mandatory information security awareness training upon hiring and annually thereafter.
- **Ongoing Education:** Regular communications and updates will be provided to keep employees informed about emerging threats and security best practices.
- **Reporting:** Employees will be educated on how to identify and report security incidents or suspicious activities.

18. Third-Party Security

- **Vendor Due Diligence:** Thorough security assessments will be conducted on all third-party vendors and service providers who handle or have access to Progress Path Co N.V.'s information assets.
- **Contractual Agreements:** All third-party contracts will include clear security clauses and requirements.
- **Monitoring:** Third-party security performance will be regularly monitored.

19. Compliance and Audit

- **Internal Audits:** Regular internal audits will be conducted to assess compliance with this Policy, internal procedures, and regulatory requirements.
- **External Audits:** Progress Path Co N.V. will cooperate with external audits as required by regulators (e.g., Curaçao Gaming Authority) or other authorities.
- **Regulatory Compliance:** Continuous monitoring of changes in relevant laws, regulations, and licensing requirements to ensure ongoing compliance. This includes specific requirements for online gambling operators and general data protection principles.

20. Policy Review and Maintenance

This Policy will be reviewed at least annually, or more frequently if there are significant changes in business operations, technology, or regulatory requirements. The Information Security Officer (ISO) or equivalent will be responsible for initiating and coordinating these reviews.

21. Enforcement

Any violation of this Policy may result in disciplinary action, up to and including termination of employment or contract, and may also result in legal action.

Last update August 29, 2025

The Policy will be valid for a period up to its annual or required reviewing.

In witness whereof, Progress Path Co N.V. has caused this Policy to be duly executed this day of 25th day of September 2025



Herman Th. Oosten/Bryon J.A. Finies, Proxy-holder(s) of e-Management N.V. as
Director of Progress Path Co N.V.

