

INFORMATION SECURITY POLICY

for

CLUBHOUSE MEDIA N.V.

VERSION CONTROL

Title	Information Security Policy		
Description	How CHM protects the confidentiality, integrity and availability of the information and systems used to operate xolotto.com — the controls CHM applies, the obligations placed on the people who use those systems, and how security incidents are reported and handled.		
Date Created	December 2025		
Operative Date	August 2026		
Maintained By	Clubhouse Media		
Version Number	Modifications Made	Date Modified	Status
1.0	Initial draft. Not adopted and not filed.	Dec-2025	Superseded
2.0	Full redraft. Restructured into nine numbered sections with sub-clauses. Adds definitions and accountability; assigns information-security responsibility to the Compliance Officer and the Chief Technology Officer; states security controls as risk-based and proportionate to CHM's operations.	Aug-2026	Operative

Table of Contents

1 · Purpose, scope and application	3
2 · Definitions	3
3 · Accountability	3
4 · Acceptable use and access to CHM Systems.....	4
4.1 Acceptable use	4
4.2 Credentials and authentication	4
4.3 Access control	5
4.4 Data classification and handling	5
4.5 Devices	5
4.6 Software and downloads	5
5 · Security awareness	6
6 · Protection against external threats	6
6.1 Phishing and social engineering	6
6.2 Fraud and scam detection	6
6.3 Platform and network security	6
6.4 Secure software development	7
7 · Security incidents.....	7
7.1 Reporting	7
7.2 Response.....	7
7.3 Notification	7
8 · Regulatory compliance and assurance	7
9 · Review of this Policy.....	8

1 · Purpose, scope and application

This Policy sets out how **Clubhouse Media N.V. ("CHM")** protects the confidentiality, integrity and availability of the information and information systems used to operate xolotto.com.

This Policy states the security controls CHM applies, the obligations CHM places on the people who use its systems, and how CHM responds to security incidents. It addresses external threats, including phishing, fraud and attempts to gain unauthorised access to CHM Systems, and internal threats, including the mishandling, misuse or unauthorised disclosure of player data or operational data.

This Policy applies to:

- CHM Personnel, in respect of every CHM System they access or use;
- all data, systems, applications and network resources owned, managed or operated by CHM, or by any company within CHM's corporate group, that has direct or indirect access to CHM Systems; and
- CHM's service providers, and any other party granted access to CHM Systems, in respect of that access.

CHM applies security controls proportionate to the risks it faces, having regard to the nature and scale of its operations.

CHM is responsible for executing this Policy, under the supervision of the CHM Compliance Officer.

2 · Definitions

CGA — the Curaçao Gaming Authority.

CHM Personnel — the individuals who carry out CHM's operations, whether engaged directly by CHM or through CHM's service providers.

CHM Systems — the information systems, applications, networks, devices, accounts and data stores that CHM owns, manages or operates, or that are operated on CHM's behalf, for the purposes of CHM's licensed activities.

Service Provider Systems — the systems operated by CHM's service providers through which those providers deliver services to CHM, including the systems used for identity verification and for payment processing. Service Provider Systems are not CHM Systems; CHM's requirements in respect of them are set out at sections 3 and 4.4.

Security Incident — any event that compromises, or that may reasonably be expected to compromise, the confidentiality, integrity or availability of CHM Systems or of the data held in them, including unauthorised access to a system or account, the loss or unauthorised disclosure of data, malware, and the loss or compromise of a device.

3 · Accountability

The CHM Compliance Officer holds responsibility for information security, and is responsible for implementing and enforcing this Policy until such time as CHM appoints a person dedicated to information security.

The CHM Chief Technology Officer is responsible for the technical security controls set out in this Policy, including their implementation, operation and maintenance across CHM

Systems, and supports the holder of the information-security role in assessing and remediating Security Incidents.

CHM's management team is accountable for information security. Management makes available the resources required to give effect to this Policy, and is made aware of this Policy and of its implementation.

The holder of the information-security role reports to CHM's management team at least once every twelve months on the effectiveness of this Policy, and makes recommendations for any proposed operational or policy enhancement. That period runs from the date this Policy takes effect.

Every member of CHM Personnel is responsible for complying with this Policy, for protecting the CHM Systems and data to which they have access, and for reporting Security Incidents.

CHM's service providers, and any other party granted access to CHM Systems, are required to adhere to the security standards set out in their contractual terms with CHM.

CHM's obligations under this Policy apply however CHM's operations are delivered. Where CHM engages a service provider, CHM remains responsible for the performance of those obligations as if CHM had performed them directly.

4 · Acceptable use and access to CHM Systems

4.1 Acceptable use

CHM Systems and the access granted to them are provided for CHM's business purposes.

CHM Personnel must not use CHM Systems in a way that is unlawful, that circumvents a security control, or that exposes player data or operational data to unauthorised access.

4.2 Credentials and authentication

Access to CHM Systems is by an individual account where the system provides for one. Credentials for an individual account are not shared.

CHM operates shared functional accounts for certain operational functions, including shared mailboxes such as those used for payments and for compliance. A shared functional account is used only where a function, rather than an individual, is the appropriate holder. Access to a shared functional account is limited to the CHM Personnel whose role requires it, and is governed by section 4.3.

CHM Personnel access credentials for CHM Systems through a centralised password management system. Access within that system is granted by group according to role. Access is granted when a member of CHM Personnel begins working with CHM, and is withdrawn when their role changes or their engagement with CHM ends.

Strong, unique passwords are required for CHM Systems. Credentials are not disclosed beyond the CHM Personnel authorised to hold them, and are not reused across unrelated services.

Multi-factor authentication is applied to CHM Systems where it is available and proportionate to the risk associated with the system and to the access it grants.

4.3 Access control

Access to CHM Systems is granted on the principle of least privilege: a member of CHM Personnel is granted the access their role requires, and no more.

Access rights, including access to shared functional accounts, are reviewed periodically. Access is amended when a member of CHM Personnel changes role, and withdrawn when their engagement with CHM ends.

Access to a shared functional account is withdrawn by removing the member of CHM Personnel from the group that holds that account's credentials.

4.4 Data classification and handling

Information held in CHM Systems is handled according to its sensitivity. CHM distinguishes between confidential information, including player personal data, financial data and credentials; internal information; and information intended for publication.

Much of the most sensitive player information CHM relies on is held and processed in Service Provider Systems rather than within CHM Systems, in particular by the providers CHM engages for identity verification and for payment processing. CHM engages such providers on the basis that they apply security and data protection standards appropriate to that information, and that requirement is set out in their contractual terms with CHM.

Confidential player data and operational data held in CHM Systems is protected in transit and at rest by the encryption provided by CHM's platform and infrastructure providers.

Confidential information is disclosed only to those who require it for their role, or where CHM is required or permitted to disclose it by law or by its regulatory obligations.

4.5 Devices

CHM Personnel who access CHM Systems are required to:

- use a device that receives current security updates for its operating system and applications, and to apply those updates;
- maintain anti-malware protection appropriate to the device;
- secure the device against unauthorised use by screen lock, passcode or an equivalent control;
- not permit any other person to use the device while CHM Systems are accessible on it; and
- report the loss, theft or compromise of a device from which CHM Systems can be accessed as a Security Incident under section 7.

Where a device from which CHM Systems can be accessed is lost, stolen or compromised, the access held through that device is withdrawn under section 4.3.

4.6 Software and downloads

Software is installed on devices used to access CHM Systems, and third-party applications are granted access to CHM Systems, only where CHM has authorised it.

CHM Personnel must not install unauthorised software on a device used to access CHM Systems, and must not grant a third-party application access to a CHM account or data without authorisation.

5 · Security awareness

CHM Personnel are engaged on the basis of established, long-standing expertise in the technical and gaming domains in which they work.

CHM Personnel are made aware of the obligations set out in this Policy when they begin working with CHM, and confirm that they have read it.

Following each review of this Policy under section 9, CHM Personnel confirm that they have read the current version.

Security awareness at CHM is continuous rather than periodic. CHM Personnel are in daily contact through CHM's internal communication channels, and matters bearing on information security — including attempted phishing and social engineering, the handling of player data, and changes in the threat landscape — are communicated as they arise, and are raised and addressed at the time.

CHM maintains a record of the security matters communicated to CHM Personnel in this way.

Where the CHM Compliance Officer or the CHM Chief Technology Officer determines that formal training on a particular matter is warranted, CHM provides it.

6 · Protection against external threats

6.1 Phishing and social engineering

CHM's email and messaging services apply the filtering and threat-protection controls provided by CHM's service providers. Suspicious messages reported by CHM Personnel are investigated.

6.2 Fraud and scam detection

CHM monitors player activity and transactions for indications of fraud, using the monitoring and screening capabilities available in CHM's platform and in the systems of its payment and service providers.

Activity identified as anomalous is reviewed, and is escalated under CHM's anti-money laundering and counter-terrorist financing procedures where those procedures apply.

6.3 Platform and network security

The CHM platform is hosted on managed cloud infrastructure operated by a third-party provider. CHM applies the network and platform security controls available in that environment, directed at preventing unauthorised access to CHM Systems and at maintaining the availability of the platform.

Threats associated with the CHM website are monitored regularly through the security monitoring provided by that infrastructure.

CHM assesses the security of its platform and supporting infrastructure periodically, and remediates the weaknesses identified, prioritised by risk.

6.4 Secure software development

Changes to the CHM platform are reviewed and tested before deployment. Testing is carried out by the developer responsible for the change and by the business stakeholders for whom it is made.

Changes are, in all but exceptional cases, additionally subject to a formal quality assurance process, carried out by a dedicated quality assurance resource with established experience in the sector.

CHM records new features and deployment details, together with the quality assurance findings raised and the fixes applied, in its issue tracking and documentation systems.

7 · Security incidents

7.1 Reporting

A Security Incident, or a suspected Security Incident, is reported immediately to the CHM Compliance Officer and the CHM Chief Technology Officer.

Every member of CHM Personnel is required to report. No member of CHM Personnel is penalised for reporting in good faith an event that proves not to be a Security Incident.

7.2 Response

On receiving a report, the CHM Compliance Officer and the CHM Chief Technology Officer assess the incident together.

The CHM Chief Technology Officer leads the technical response: containment of the incident, remediation of its cause, and restoration of the affected systems and data.

The CHM Compliance Officer directs the response as a whole, determines what the incident requires of CHM under this Policy and under CHM's regulatory obligations, and decides any notification required under section 7.3.

CHM records each Security Incident, the assessment made, the action taken and the outcome.

The CHM Compliance Officer and the CHM Chief Technology Officer review Security Incidents together to identify the changes needed to reduce the risk of recurrence.

7.3 Notification

Where a Security Incident affects players or other external parties, CHM discloses it in accordance with its obligations under applicable law and its regulatory obligations, including its obligations to the CGA, and informs the parties affected. The CHM Compliance Officer determines what disclosure is required and makes it.

8 · Regulatory compliance and assurance

CHM complies with the requirements of the Curaçao Gaming Authority and with applicable data protection laws.

CHM reviews its compliance with this Policy periodically, and records the reviews carried out and the actions arising from them.

9 · Review of this Policy

This Policy is reviewed at least once every twelve months, and additionally on a material change to the threat landscape, to CHM's regulatory requirements, or to CHM's organisational structure or systems.

The CHM Compliance Officer owns the review.

Any material change to this Policy is reported to the CGA.