

Information Security Policy

BetU Curacao B.V.

Document Owner: Executive Leadership

Approved By: CEO - Peter Lawrence

Version: 1.0

Effective Date: 26 Feb 2026

Review Frequency: Annual or upon material infrastructure change

Version Number	Date Created	Author(s)
1.0	24/02/2026	Stephanie Johnstone & Liem Nguyen

Contents

1. Purpose	4
2. Scope	4
3. Governance and Responsibilities	5
3.1 Executive Leadership.....	5
3.2 Technology / Platform Leads	5
3.3 Managers	5
3.4 All Users	5
3.5 Security Governance Documentation	6
4. Risk Management	6
4.1 Identification of Security Risks	6
4.2 Risk Register	6
4.3 Technology Risk Review	7
4.4 Risk Review and Governance	7
5. Access Control.....	7
5.1 General Principles	7
5.2 AWS and Infrastructure Access	8
5.3 SaaS and Application Access	8
6. Identity, Authentication and Session Management.....	9
6.1 Corporate Identity	9
6.2 Application Authentication (Auth0)	9
7. Encryption and Data Protection	9
8. Data Classification and Handling.....	10
9. Data Storage, Retention and Backups	10
9.1 Storage.....	10
9.2 Retention.....	11
9.3 Backups	11
10. Secure Development and Change Management	11
11. Vulnerability Management and Security Testing	11
11.1 Patch Management	12
11.2 Vulnerability Tracking.....	12
11.3 Security Advisory Monitoring	12

11.4 Vulnerability Scanning (Planned Enhancement).....	13
11.5 Independent Security Testing (Planned Enhancement)	13
11.6 Remediation Prioritisation.....	13
11.7 Continuous Improvement	14
12. Logging, Monitoring and Audit.....	14
13. Business Continuity and Disaster Recovery	15
13.1 Infrastructure Resilience.....	15
13.2 Backups and Data Protection	15
13.3 Recovery Objectives	15
13.4 Recovery Procedures.....	16
13.5 Service Continuity and Player Fund Protection	16
13.6 Testing and Continuous Improvement.....	17
14. Third-Party Risk Management	17
15. Incident Response.....	17
15.1 Incident Response Procedure	18
15.2 Definition of Security Incident	18
15.3 Incident Reporting.....	18
15.4 Incident Register	19
15.5 Incident Classification	19
15.6 Incident Response Lifecycle.....	20
15.7 Escalation and Notifications	20
15.8 Post-Incident Review	20
16. Training and Awareness.....	21
17. Compliance and Exceptions.....	21
18. Review and Maintenance	21

1. Purpose

The purpose of this Information Security Policy is to ensure the confidentiality, integrity, and availability of Ubet's information systems and data, including player data and financial information.

This policy establishes the baseline security controls, governance framework, and operational standards designed to:

- Protect customer funds and data
 - Protect company information assets
 - Maintain platform integrity
 - Support compliance with applicable gaming and data protection requirements
-

2. Scope

This policy applies to:

- All employees, contractors, consultants, and authorised third parties
- All information assets (digital, paper, verbal)
- All production and non-production systems
- All cloud environments (including AWS)
- All SaaS platforms used to operate the business
- All end-user devices used for company business

In-scope systems include, but are not limited to:

- AWS infrastructure (EC2, RDS, S3, CloudWatch, IAM, etc.)
- Unified Data Platform
- Auth0 authentication services
- Microsoft 365
- VPN / secure access solutions
- Developer and operational tooling

3. Governance and Responsibilities

3.1 Executive Leadership

Executive Leadership:

- Approves this policy
- Ensures appropriate resourcing of security controls
- Oversees risk management and material security incidents

3.2 Technology / Platform Leads

Responsible for:

- Implementing technical security controls
- Maintaining secure AWS configuration
- Enforcing least privilege access
- Ensuring encryption standards are applied
- Maintaining system documentation
- Supporting audits and regulatory inquiries

3.3 Managers

Responsible for:

- Ensuring onboarding and offboarding processes are followed
- Ensuring timely removal or adjustment of access rights
- Escalating security concerns

3.4 All Users

All personnel must:

- Protect credentials and devices
- Use MFA where required
- Follow access policies
- Promptly report security incidents

3.5 Security Governance Documentation

Supporting security governance documentation, including operational procedures and registers, is maintained within the organisation's internal documentation and governance systems. This includes security incident registers, vulnerability tracking, and risk registers maintained within Jira, and operational security procedures maintained within Confluence.

4. Risk Management

Ubet maintains an information security risk management process to identify, assess, and manage risks that may affect systems, infrastructure, data, or gaming operations.

The objective of the risk management process is to ensure that security risks are identified in a timely manner, assessed based on their potential impact, and managed through appropriate mitigation or remediation measures.

4.1 Identification of Security Risks

Security risks may be identified through a variety of operational activities, including:

- Security incident investigations
- Vulnerability management processes
- Infrastructure and architecture reviews
- Monitoring of vendor security advisories
- Technology or system change reviews

Where potential risks are identified, they are documented and assessed to determine appropriate treatment actions.

4.2 Risk Register

Ubet maintains a centralised information security risk register within Jira to document and manage identified security risks.

The risk register records relevant details including:

- Description of the identified risk
- Impact and likelihood assessment

- Assigned risk owner
- Planned mitigation or treatment actions
- Risk status and review date

The risk register provides a structured mechanism for tracking risks and ensuring that mitigation activities are monitored until completion or formal acceptance.

4.3 Technology Risk Review

Security considerations are incorporated into the evaluation of new technologies, systems, and significant infrastructure changes.

Engineering and technology leadership review potential security risks associated with new systems or architectural changes prior to deployment, and identify mitigation measures where appropriate.

4.4 Risk Review and Governance

Information security risks are reviewed periodically by Technology Leadership to ensure that:

- Risks remain accurately assessed
- Mitigation actions are progressing as expected
- Emerging risks are identified and addressed

Risk reviews are conducted at least annually, or when significant changes to systems, infrastructure, or operations occur.

Material risks may be escalated to Executive Leadership for oversight and prioritisation of remediation actions.

5. Access Control

5.1 General Principles

Access to systems, applications, and information assets is managed according to the principles of role-based access control (RBAC), least privilege, and need-to-know.

Access is granted only to authorised individuals based on their job responsibilities and operational requirements. All users are assigned individual accounts, and the use of

shared or generic accounts is prohibited except where technically required and subject to additional monitoring and control.

Access rights are managed through defined onboarding and offboarding processes and include:

- Approval of access based on role and operational requirements
- Periodic review of access rights to ensure continued appropriateness
- Prompt revocation or adjustment of access when personnel change roles or leave the organisation

Authentication and access management controls are implemented across core infrastructure, SaaS platforms, and internal systems to protect sensitive data and production environments.

Operational security events, including security incidents and identified vulnerabilities, are centrally recorded and tracked within the organisation's Jira security governance registers to support investigation, remediation tracking, and security oversight.

5.2 AWS and Infrastructure Access

AWS access is managed through:

- Individual IAM identities
- Role-based access groups
- MFA enforcement
- Restricted production access

Database access (e.g., RDS):

- Is role-restricted
- Is limited to authorised personnel
- Is logged and auditable

Segregation of duties is enforced between development, testing, and production environments where practical.

5.3 SaaS and Application Access

Access to SaaS tools (e.g., Auth0, Microsoft 365) is:

- Provisioned individually
 - Role-restricted
 - Protected by MFA where supported
-

6. Identity, Authentication and Session Management

6.1 Corporate Identity

Microsoft 365 accounts serve as primary corporate identity.

Multi-Factor Authentication (MFA) is mandatory for:

- Microsoft 365
- AWS console access
- VPN access
- Other security-sensitive platforms where supported

6.2 Application Authentication (Auth0)

Customer authentication is handled via Auth0.

Security controls include:

- Token expiry enforcement
- Password policies
- Secure login and reset flows
- Protection against brute force attacks
- Monitoring of suspicious authentication events

Session management follows secure configuration standards.

7. Encryption and Data Protection

Ubet applies industry-standard encryption controls:

- Encryption in transit using TLS 1.2 or higher

- Encryption at rest using AWS-managed encryption (e.g., AES-256 via KMS)
- Encryption applied to databases, storage buckets, and backups where supported by platform capabilities.

Sensitive data includes:

- Player personal data (PII)
- KYC documentation
- Financial data
- Authentication credentials

Access to sensitive data is restricted and logged.

8. Data Classification and Handling

Information is classified as:

- Public
- Internal
- Confidential

Player data, financial data, and system credentials are classified as Confidential.

Confidential data:

- Must be encrypted at rest and in transit
 - Must only be accessible to authorised personnel
 - Must not be stored on unsecured devices
-

9. Data Storage, Retention and Backups

9.1 Storage

Production data is stored within secured AWS environments with:

- IAM-based access control
- Encryption
- Lifecycle management

9.2 Retention

Data retention is based on:

- Regulatory requirements
- Business and operational needs
- Contractual obligations

9.3 Backups

Backups:

- Are encrypted
- Inherit access controls
- Are stored within AWS
- Are protected against unauthorised access

Backup restoration capability is tested periodically.

10. Secure Development and Change Management

Security is integrated into development processes via:

- Security validation checklists
- Review of authentication flows
- Secure cookie and header configuration
- CSRF protections
- Controlled release processes

Changes to authentication or security-sensitive components require validation before deployment.

11. Vulnerability Management and Security Testing

Ubet maintains a vulnerability management process to identify, assess, and remediate security vulnerabilities that may affect systems, applications, or infrastructure.

The organisation combines platform security controls, engineering practices, and centralised tracking to manage technical vulnerabilities.

11.1 Patch Management

Systems and infrastructure components are maintained with security updates and patches as part of normal engineering and infrastructure management processes.

This includes:

- Applying security updates to operating systems and application dependencies
- Updating infrastructure components managed within AWS
- Applying vendor security patches as part of system maintenance cycles

Critical security updates are prioritised where identified.

11.2 Vulnerability Tracking

Ubet maintains a centralised vulnerability tracking register within Jira to record and manage identified vulnerabilities as part of the organisation's security risk management processes.

The vulnerability register records:

- Description of the vulnerability
- Severity classification
- Impact assessment
- Assigned owner
- Remediation actions
- Resolution status

Vulnerabilities remain tracked until remediation actions are completed and verified.

11.3 Security Advisory Monitoring

Technology and engineering teams monitor relevant vendor and platform security advisories to identify newly disclosed vulnerabilities affecting systems or software components.

This may include monitoring advisories from providers such as:

- AWS
- Auth0
- Software and infrastructure vendors
- Open-source dependency disclosures

Where relevant vulnerabilities are identified, remediation actions are tracked through the vulnerability register.

11.4 Vulnerability Scanning (Planned Enhancement)

Ubet intends to implement automated vulnerability scanning capabilities for systems and application dependencies.

Automated scanning will assist in identifying:

- Known software vulnerabilities
- Outdated or unsupported components
- Infrastructure misconfigurations

Findings will be reviewed by engineering leadership and tracked within the vulnerability register.

11.5 Independent Security Testing (Planned Enhancement)

Ubet intends to conduct periodic independent security testing, such as external penetration testing or equivalent security assessments, for public-facing systems.

The objective of these assessments is to:

- Identify potential security weaknesses
- Validate security controls
- Support continuous improvement of the organisation's security posture

Findings from such assessments will be documented and tracked through the vulnerability register until remediation is completed.

11.6 Remediation Prioritisation

Vulnerabilities are prioritised based on severity and potential business impact.

Typical remediation priorities include:

Critical

Immediate remediation or mitigation required.

High

Remediation scheduled as a priority engineering task.

Medium / Low

Remediation planned as part of normal development or maintenance cycles.

Technology leadership oversees remediation prioritisation and risk assessment.

11.7 Continuous Improvement

The vulnerability management process is periodically reviewed and improved to strengthen the organisation's security posture.

Improvements may include:

- Expanded automated scanning capabilities
- Enhanced monitoring of software dependencies
- Periodic independent security assessments

12. Logging, Monitoring and Audit

Security-relevant logging is enabled across:

- AWS services
- Auth0
- Unified Data Platform

Logs include:

- Authentication events
- Privileged access events
- Infrastructure configuration changes

Logs are retained in accordance with operational and regulatory requirements and are available to support security investigations and audits.

Security alerts provided by platforms (e.g., AWS, Auth0) are monitored and investigated where applicable.

13. Business Continuity and Disaster Recovery

Ubet is committed to maintaining the availability and integrity of its gaming platform and protecting player balances in the event of operational disruption.

13.1 Infrastructure Resilience

The production environment is hosted within AWS and is designed to support service continuity through:

- Redundant cloud infrastructure configurations (including multi-AZ deployments where applicable)
- Managed failover capabilities provided by AWS services
- Segregation of production and non-production environments

These measures are designed to minimise service disruption and reduce single points of failure.

13.2 Backups and Data Protection

Backups of critical systems and production data:

- Are encrypted at rest
- Inherit AWS-managed encryption controls
- Are protected through IAM-based access restrictions
- Are retained in accordance with operational and regulatory needs

Backup configurations are reviewed periodically to ensure recoverability of critical systems.

13.3 Recovery Objectives

Recovery objectives are defined for critical services, including:

- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)

These objectives are reviewed periodically by Technology Leadership to ensure alignment with business continuity requirements and protection of player balances.

13.4 Recovery Procedures

Ubet maintains operational knowledge and technical processes required to restore services following disruption, in alignment with the organisation's defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

A documented Disaster Recovery (DR) Procedure is maintained within the organisation's internal documentation platform (Confluence). The procedure defines the structured process for restoring systems and services in the event of major operational disruption.

The DR Procedure includes:

- Clearly defined recovery steps for critical systems
- Assigned recovery roles and responsibilities
- Escalation paths for major incidents
- Communication procedures during recovery events
- Validation and post-recovery verification steps

Engineering and Technology Leadership coordinate recovery activities in accordance with the documented DR Procedure and supporting operational documentation.

The procedure is reviewed periodically to ensure alignment with infrastructure changes and operational requirements.

13.5 Service Continuity and Player Fund Protection

System architecture and backup controls are designed to:

- Preserve integrity of player account balances
- Ensure transactional data durability
- Prevent data loss exceeding defined RPO thresholds

In the event of system disruption, priority is given to restoring:

1. Player authentication systems
2. Transactional integrity

3. Balance reconciliation systems
4. Core gaming services

Executive Leadership is notified in the event of material service disruption impacting player balances.

13.6 Testing and Continuous Improvement

Ubet intends to introduce periodic Disaster Recovery testing exercises to validate recovery procedures and infrastructure resilience.

Initial structured DR testing will be implemented within 6 months of policy approval.

Results of DR exercises will be reviewed by Technology Leadership and used to improve resilience.

14. Third-Party Risk Management

Third-party providers (e.g., AWS, Auth0, Microsoft 365) are selected based on:

- Industry reputation
- Security posture
- Availability of certifications or compliance attestations
- Ability to support required security controls

Contracts and service configurations are reviewed to ensure appropriate security safeguards.

Where appropriate, third-party providers may be assessed for security capabilities prior to adoption.

15. Incident Response

Ubet maintains a structured process for identifying, responding to, and resolving information security incidents that may impact systems, data, or player accounts.

The organisation maintains a documented Incident Response Procedure and a centralised incident register to ensure that incidents are managed consistently,

investigated appropriately, and recorded for audit and continuous improvement purposes.

15.1 Incident Response Procedure

Incident response activities are governed by the Incident Response Procedure, which is maintained in the organisation's internal documentation platform (Confluence) and is reviewed periodically by Technology Leadership.

The procedure defines:

- The lifecycle for responding to security incidents
- Roles and responsibilities during incident handling
- Incident classification and escalation processes
- Investigation and remediation procedures
- Documentation and post-incident review requirements

15.2 Definition of Security Incident

A security incident includes, but is not limited to:

- Unauthorised access to systems or data
- Compromise of player accounts
- Suspected or confirmed data breaches
- Malware or ransomware events
- Phishing or credential compromise
- Loss or theft of company devices
- Significant service disruption caused by malicious activity

15.3 Incident Reporting

All personnel are required to promptly report suspected security incidents to the Technology or Engineering leadership team.

Incidents may also be detected through automated monitoring alerts from systems such as:

- AWS infrastructure monitoring
- Authentication and access monitoring (e.g., Auth0)
- Application and infrastructure logging systems

Security awareness guidance provided during onboarding includes instructions for reporting potential incidents.

15.4 Incident Register

All security incidents are recorded in a centralised incident register maintained within Jira Service Management (Security & Incident Management project).

The register records:

- Date detected
- Severity classification
- Affected systems or services
- Impact assessment
- Containment and remediation actions
- Root cause analysis
- Notification decisions where applicable

The incident register provides an auditable record of incidents and supports internal review and regulatory oversight.

15.5 Incident Classification

Incidents are classified based on severity and potential impact:

Low

Minor operational issue with no exposure of sensitive data.

Medium

Operational disruption or potential exposure of internal systems or data.

High / Critical

Confirmed compromise of player accounts, exposure of sensitive data, significant service disruption, or incidents potentially requiring regulatory notification.

Severity classification determines escalation requirements and response prioritisation.

15.6 Incident Response Lifecycle

Security incidents follow a structured lifecycle including:

1. Identification and initial assessment
2. Investigation of the incident and affected systems
3. Containment of impacted systems or accounts
4. Remediation and recovery actions
5. Documentation and closure of the incident record

The lifecycle is implemented through the incident workflow within the Jira incident register.

15.7 Escalation and Notifications

High-severity incidents are escalated to Executive Leadership.

Where required by applicable laws, licensing conditions, or regulatory guidance:

- Regulators will be notified in a timely manner
- Affected customers may be informed if their data or accounts are materially impacted

External communications are coordinated by Executive Leadership.

15.8 Post-Incident Review

Significant incidents are subject to a post-incident review to:

- Document root cause analysis
- Identify corrective and preventative actions
- Improve security controls and operational procedures

Lessons learned from incidents are used to strengthen the organisation's security posture.

16. Training and Awareness

Security awareness is covered during onboarding.

Personnel with privileged access receive role-appropriate guidance on secure system usage.

17. Compliance and Exceptions

All personnel must comply with this policy.

Any exceptions must:

- Be documented
 - Be risk-assessed
 - Be approved by Technology Leadership
-

18. Review and Maintenance

This policy is reviewed at least annually or upon significant infrastructure or regulatory change.