

Information Security Policy.

1. Purpose & Scope

1.1 Purpose

The purpose of this Information Security Policy is to establish a comprehensive framework for protecting the confidentiality, integrity, and availability of all information processed, stored, or transmitted by **Seven Days B.V.**, including all operational brands under the Weeekly platform.

This policy ensures that all data, systems, digital assets, and supporting infrastructure are safeguarded against unauthorized access, misuse, loss, manipulation, or disruption.

The objectives of this policy are to:

- Maintain **secure and compliant operations** in accordance with the Curaçao Gaming Authority (CGA) standards, AML/CFT obligations, and global information security best practices.
- Protect **player data**, internal data, platform logic, financial records, and the integrity of cryptocurrency wallets.
- Define consistent security expectations for staff, contractors, and third-party partners to ensure a unified approach across all parties.
- Reduce risk arising from cybersecurity threats, operational failures, internal misuse, or external attacks.
- Support business continuity and secure, uninterrupted gaming operations across all Weeekly platforms.

1.2 Scope

This policy applies to **all information assets, systems, personnel, and third parties** engaged in the operation of:

Covered Platforms

1. **Weeekly**

- Weekly prize pool raffles
- Ticket-based entries
- Casino-style games utilising virtual **Weeekly Coins**
- User progression, coin wagering, bonus systems, tickets, and rewards

2. **Weeekly Rivals**

- Competitive gameplay mode based on casino-style wagering performance
- Casino-style games utilising virtual **Weeekly Coins**
- Leaderboards, and prize allocation mechanisms

3. **Traditional Online Casino Layer**

- Cryptocurrency deposits and withdrawals
- Real-money casino games
- Wallet security, payout logic, and user balance protection

1.3 Personnel and Operational Applicability

This policy applies to all individuals who access, manage, or process Weeekly information assets, including:

- **Employees**
- **Founders and executive team**
- **Contractors and consultants**

- **Customer support personnel**
- **Developers and engineers**
- **Compliance, AML, and risk teams**
- **Marketing and operations staff**

All personnel must comply with the controls, standards, and obligations defined within this document.

1.4 Third-Party Applicability

This policy also applies to all **external partners and service providers** that store, process, or access Weeekly systems or data, including but not limited to:

- **Game suppliers & aggregators**
- **Payment processors**
- **KYC/AML identity verification vendors**
- **Blockchain analysis and wallet screening tools**
- **Cloud hosting providers**
- **Security and monitoring services**

All third parties must adhere to Weeekly's minimum security standards, contractual requirements, and data-handling obligations.

1.5 Systems and Data Covered

This Information Security Policy covers **all systems** and **data types** used or generated by Weeekly platforms, including:

Systems

- Application servers
- Web and mobile platforms
- Admin consoles & back-office dashboards
- Player account management systems
- Payment and wallet infrastructure
- Logging, monitoring, and analytics systems
- Anti-fraud and AML monitoring tools
- Cloud hosting environments
- Third-party integrations

Data Types

- **Personally Identifiable Information (PII)**
(name, DOB, email, IP address, device identifiers)
- **Cryptocurrency data**
(wallet addresses, deposits, withdrawals, on-chain analysis)
- **Gaming data**
(bets, spins, coin usage, leaderboards, gameplay history)
- **Prize pool and raffle data**
- **Transaction data**
(Transfers, ticket purchases, game wagers)
- **Operational and internal business data**
- **Audit logs and security logs**

1.6 Enforcement

All individuals and third parties under the scope of this policy are required to comply with its standards.

Non-compliance may result in disciplinary action, account suspension, vendor termination, or regulatory reporting, depending on severity.

2. Information Security Objectives

The primary objective of this Information Security Policy is to establish, implement, and maintain a **robust security framework** that protects Weeekly's digital assets, gaming systems, player information, and financial infrastructure. The following objectives formalise the standards required to operate securely, responsibly, and in full alignment with the expectations of the Curaçao Gaming Authority (CGA).

2.1 CIA Triad: Core Security Principles

Weeekly adheres to the internationally recognised **Confidentiality, Integrity, and Availability (CIA)** model to guide all information security practices.

2.1.1 Confidentiality

Safeguard information from unauthorized access, disclosure, or misuse.

This includes ensuring:

- Player data and personal information remain protected at all times
- Access to internal systems is strictly controlled via authentication and role-based permissions
- Sensitive operational data (e.g., admin logs, wallet keys, game configuration) is limited to approved personnel

- Third-party integrations operate under strict data protection agreements
- Encryption is applied to data both in transit and at rest

2.1.2 Integrity

Ensure all data remains accurate, consistent, and unaltered except by authorized processes.

This includes:

- Preventing tampering, manipulation, or corruption of:
 - Game outcomes and randomization
 - Raffle ticket allocations
 - Prize pool calculations
 - Leaderboard logic in Weeekly Rivals
 - User balance and transaction records
- Detecting and blocking fraudulent or automated attempts to alter gameplay or results
- Maintaining verifiable audit logs of all system changes
- Implementing secure development, version control, and change management processes

2.1.3 Availability

Ensure systems, services, and data are accessible to authorized users when needed.

This includes:

- Maintaining stable uptime for:
 - Weeekly raffles
 - Casino-style coin games
 - Rivals competitive engines
 - Crypto-denominated casino operations (USDT; USDC where supported)
- Implementing redundant infrastructure, load balancing, and DDoS protection
- Ensuring reliable access to admin panels, AML tools, monitoring systems, and payment gateways
- Establishing robust incident response and business continuity procedures

2.2 Protection of Player Funds and Crypto Wallets

Weeekly is committed to protecting all assets related to real-money operations, including:

USDT/USDC Wallet Security

- Multi-signature wallet structures
- Secure storage and access controls for private keys
- Hot-wallet limitations and cold-wallet safeguarding
- Transaction velocity limits and anomaly detection
- Segregation of operational funds and player balances

Fraud & AML Protection

- Continuous monitoring using blockchain analytics (e.g., mixer detection, sanction exposure, wallet risk scoring)
- Automated flags for suspicious activity
- Tiered withdrawal thresholds and enhanced due diligence where required

This objective ensures players can trust the integrity of deposits, balances, withdrawals, and prize distributions.

2.3 Compliance With Curaçao Gaming Authority Requirements

Weeekly ensures full alignment with CGA information security expectations, including:

- Protection of player data and operational systems
- Proper internal controls around gaming logic and randomness
- Secure, transparent financial processes for USDT deposits and withdrawals
- Auditability of all transactions, game outcomes, and administrative actions
- Vendor oversight and secure integration with all third-party providers
- Policies that support AML/CFT compliance frameworks
- Timely incident reporting and cooperation with regulators

This objective ensures that Weeekly operates within a regulated, secure, and trustworthy environment consistent with Curaçao's licensing framework and international standards.

2.4 Continuous Improvement

Weeekly will regularly:

- Review and update this Information Security Policy
- Conduct internal audits and vulnerability assessments
- Monitor emerging cyber threats and industry trends
- Enhance security controls in alignment with global best practices (ISO 27001, NIST, etc.)
- Review third-party security practices and vendor compliance

This ensures long-term protection of the platform, users, digital assets, and operational stability.

3. Roles & Responsibilities

To ensure the effective implementation, monitoring, and enforcement of Weeekly's Information Security Policy, specific roles and responsibilities are assigned across the organization. These roles ensure clear accountability, proper segregation of duties, and consistent adherence to all security and regulatory requirements.

This section applies to all Weeekly platforms.

3.1 Information Security Officer (ISO)

The Information Security Officer is responsible for overseeing the development, implementation, and continuous improvement of Weeekly's security framework.

Key Responsibilities

- Develop, maintain, and enforce all information security policies and procedures
- Oversee security controls across infrastructure, applications, and data

- Monitor overall risk exposure and recommend improvements
- Coordinate vulnerability assessments, penetration testing, and system hardening
- Manage access controls, privileged accounts, and authentication standards
- Lead internal security reviews and compliance monitoring
- Ensure cryptographic key management meets industry standards
- Report security-related metrics, risks, and incidents to senior management
- Ensure staff receive ongoing security training and awareness sessions

3.2 Data Protection Officer (DPO) (*if applicable*)

A DPO is appointed if required by regulatory or contractual conditions (e.g., GDPR-aligned requests from EU players or partners).

Key Responsibilities

- Oversee the handling of player Personally Identifiable Information (PII) in full compliance with applicable data protection laws
- Monitor the collection, storage, processing, transfer, retention, and deletion of personal data throughout the data lifecycle
- Manage and respond to user data rights requests, including access, correction, deletion, and data portability where required
- Ensure privacy-by-design and privacy-by-default principles are embedded within all relevant systems, applications, and development processes
- Conduct Data Protection Impact Assessments (DPIAs) where processing activities present elevated privacy or security risks

- Liaise with regulators, supervisory authorities, and external agencies regarding data privacy obligations, inquiries, or breaches

3.3 Anti Money Laundering (AML) Compliance Officer

The AML Compliance Officer ensures Weeekly complies with AML/CFT obligations under Curaçao regulations and global standards.

Key Responsibilities

- Oversee identity verification, Know Your Customer (KYC), Enhanced Due Diligence (EDD), and source-of-funds and source-of-wealth processes
- Monitor transactional activity for suspicious behaviour using blockchain analytics tools and AML monitoring systems
- Review flagged accounts and determine required escalation, investigation, or enforcement actions
- Manage sanctions screening procedures, including IP checks, wallet address checks, and geographic restrictions
- Ensure all reporting obligations to competent authorities are fulfilled where required (e.g., suspicious activity reporting)
- Provide AML and Counter-Financing of Terrorism (CFT) training to relevant staff and business units
- Maintain comprehensive Anti-Money Laundering (AML) manuals, internal procedures, red-flag indicators, and risk matrices
- Collaborate with security, fraud, and engineering teams to detect and mitigate suspicious behaviour, account compromise, or wallet anomalies

3.4 Technical Leads (Developers, Infrastructure, and Security Engineers)

Technical leads oversee the design, development, deployment, and maintenance of all digital infrastructure across Weeekly platforms.

Key Responsibilities

- Implement secure coding practices and participate in formal code reviews throughout the development lifecycle
- Maintain server security, cloud configurations, network perimeter controls, and systems patching schedules
- Oversee Continuous Integration (CI)/Continuous Deployment/Delivery (CD) pipelines, ensuring strict access controls, code integrity checks, and secure deployment standards
- Support encryption practices, secure network architecture, and environment segregation (development, staging, production)
- Collaborate with the Information Security Officer during vulnerability assessments, penetration testing, and remediation planning
- Maintain version control governance, rollback strategies, deployment records, and change-management documentation
- Ensure gaming logic, Random Number Generator (RNG) systems, and prize allocation algorithms are tamper-resistant and independently verifiable
- Ensure platform uptime, service redundancy, backup integrity, and disaster-recovery readiness

3.5 Customer Support Leads

Customer Support Leads ensure player interactions are handled securely and in compliance with operational procedures.

Key Responsibilities

- Protect player data during interactions and troubleshooting

- Verify customer identity before sharing account information
- Escalate suspected fraud, AML concerns, or unusual player behaviour
- Maintain secure handling of support tickets, emails, and chat logs
- Follow internal procedures for password resets, account access, and disputes
- Ensure support teams understand and follow information security requirements

3.6 Vendor Oversight Lead

The Vendor Oversight Lead ensures that all third-party service providers meet Weeekly's security, compliance, and contractual obligations.

Key Responsibilities

- Conduct due diligence and risk assessments before onboarding vendors
- Maintain an updated vendor register with assigned risk categories
- Ensure third-party agreements include security, confidentiality, and data protection clauses
- Review vendor performance, security updates, and audit reports
- Monitor third-party access to Weeekly systems and revoke access when no longer required
- Coordinate with the ISO and AML officer for vendor-related compliance issues
- Ensure secure integration with game suppliers, KYC vendors, and payment processors

3.7 Incident Response Lead

The Incident Response Lead coordinates and manages Weeekly's response to security incidents.

Key Responsibilities

- Lead the incident response lifecycle: detection, containment, eradication, recovery, review
- Activate escalation protocols and inform senior management when required
- Coordinate cross-functional teams during security events
- Ensure evidence is collected, preserved, and logged appropriately
- Manage communication with regulators, partners, or affected users if necessary
- Maintain and update the Incident Response Plan
- Conduct post-incident reviews and ensure lessons learned are implemented

3.8 Documentation, Accountability & Auditing

Weeekly maintains clear documentation of responsibilities and audits to ensure accountability across all roles.

Requirements

- Each role must have written responsibilities within internal documentation
- All privileged actions (admin console changes, wallet operations, system configurations) must be logged and auditable
- Annual internal audits will be conducted to evaluate compliance with this policy
- Findings and corrective actions must be documented and tracked
- Evidence of training, access reviews, and compliance checks must be maintained

- Vendor audits and performance reviews must be stored securely

These controls ensure transparency, traceability, and regulatory compliance across the organization.

4. Asset Inventory & Classification

Weeekly maintains a structured and comprehensive inventory of all information assets to ensure appropriate protection based on sensitivity, regulatory obligations, and operational risk. Every asset—whether data, software, hardware, or third-party integration—is classified, monitored, and safeguarded according to this policy.

This classification framework supports risk management, access control enforcement, and security monitoring across all Weeekly platforms.

4.1 Asset Inventory Overview

A centralised **Information Asset Register (IAR)** will be maintained by the Information Security Officer (ISO).

The register includes:

- Asset type and description
- Owner or responsible department
- Sensitivity classification
- Storage location
- Applicable controls and encryption requirements
- Access rights and authorised users
- Third-party involvement (if any)

- Retention periods and backup requirements
- Change history and versioning (where applicable)

The Information Asset Register (IAR) ensures full traceability of all critical systems, data repositories, and technology components that support the operation and integrity of the entire Weeekly platform.

4.2 Asset Types

The following categories represent the core information assets of Weeekly. Each must be logged, maintained, and protected under defined classification rules:

4.2.1 Player Accounts & Personally Identifiable Information (PII)

- Names, email addresses, device fingerprints
- IP addresses, geographic data, time zones
- Verification documents (when collected for KYC)
- Login credentials and authentication information
- Player behavioural patterns and game history

4.2.2 Wallet Addresses & Blockchain Transaction Data

- Player deposit addresses
- Withdrawal addresses
- Internal hot and cold wallet addresses
- On-chain activity logs
- AML screening results (risk scores, sanction flags, mixer alerts)

4.2.3 Game Logic, Algorithms & RNG Systems

- Casino-style game configurations
- Internal game engines for Weeekly coin games
- Competitive logic for Rivals
- Randomisation calculations
- Prize algorithms and payout logic

4.2.4 Prize Pool Logic & Security Systems

- Ticket issuance calculations
- Prize pool balances and distribution logic
- Draw randomisation procedures
- Backend scripts controlling weekly draws
- Audit logs of prize pool changes

4.2.5 Backend Servers & Administrative Systems

- Admin consoles
- Customer support dashboards
- CRM and user account management tools
- Developer consoles and configuration environments
- IP allowlists and privileged access systems

4.2.6 Internal Communication Systems

- Email servers

- Slack/Teams/Discord channels
- Knowledge bases and internal documentation
- Support communications and ticketing tools

4.2.7 Third-Party Integrations

- Game provider APIs
- KYC/AML vendors
- Blockchain monitoring tools
- Payment processors and USDT gateways
- Analytics and behavioural risk systems

4.2.8 Crypto Custody Systems

- Hot wallet infrastructure
- Cold wallet storage
- Multisignature structures
- Wallet key management systems
- Withdrawal queue logic and automated risk screening

4.2.9 Monitoring Tools, Logs & AML Systems

- Server and application logs
- Transaction logs
- Security alerts and anomaly detection systems

- Chainalysis-type tools
- Behavioural analysis and fraud detection modules
- System health metrics, uptime monitors, performance dashboards

4.3 Data Classification Levels

To ensure security controls are proportional to sensitivity and risk, Weeekly defines four levels of data classification:

4.3.1 Public

Information intended for public distribution.

Examples:

- Marketing material
- Public FAQ
- Promotional content
- Terms & Conditions (public version)

Controls Required:

- No special access restrictions
- Integrity and availability protections maintained

4.3.2 Internal

Information intended for internal operational use but not harmful if disclosed.

Examples:

- Operational guidelines

- Low-sensitivity business analytics
- Non-sensitive internal communications

Controls Required:

- Access restricted to relevant staff
- Stored on secure internal platforms

4.3.3 Confidential

Information that could cause operational or reputational harm if exposed.

Examples:

- Player account details (PII)
- Staff information
- Support ticket data
- Non-public business strategies
- Game configuration settings

Controls Required:

- Encrypted storage and transmission
- Role-based access control (RBAC)
- Logging of access events

4.3.4 Highly Confidential

Information that could cause severe financial, regulatory, or security impact if exposed.

Examples:

- Cryptocurrency wallet private keys
- Admin panel credentials
- Hot wallet operational logic
- Source code for core game logic and RNG systems
- Prize pool scripts and draw mechanisms
- AML flags, risk scores, sanctions findings
- Internal audit trails and privileged action logs

Controls Required:

- Strict RBAC (minimum necessary access)
- Multi-factor authentication
- Hardware security modules or encrypted vault storage
- Continuous monitoring and access logging
- Segregation from general systems
- Limited internal distribution (need-to-know only)

4.4 Asset Ownership & Accountability

Each information asset must have an **assigned owner** responsible for:

- Ensuring correct classification
- Approving access requests
- Documenting changes

- Ensuring backups and retention comply with policy
- Coordinating with the ISO for periodic reviews

Ownership ensures clear accountability and traceability across all sensitive systems.

4.5 Review & Audit Requirements

- Asset inventories must be reviewed **at least annually**, or sooner following major platform changes.
- Highly Confidential assets must be reviewed **every quarter**.
- Logs and documentation must be accessible for inspection by the ISO, Compliance Officer, or regulatory authorities.
- Any asset lacking a documented owner or classification must be flagged for immediate review.

5. Access Control Policy

The Access Control Policy ensures that all Weeekly systems, data, and administrative environments are protected through strict authorization measures, consistent authentication processes, and continuous monitoring of privileged activity.

This framework prevents unauthorized access, internal misuse, and security breaches across all operational platforms.

This policy applies to all employees, contractors, developers, administrators, vendors, and any third party accessing Weeekly systems.

5.1 Access Control Principles

Weeekly follows industry-standard best practices for controlling system access.

5.1.1 Role-Based Access Control (RBAC)

All access rights must be assigned based on defined roles rather than individuals. Access must align with the responsibilities of each role.

Examples:

- Customer Support → ticketing system access only
- Developers → staging environment, code repositories
- Security/Technical Leads → production access with limited privileges
- AML Compliance → transaction dashboards, risk engines
- Finance/Admin → withdrawal approvals only

5.1.2 Minimum Privilege

Users must be granted only the **minimum level of access necessary** to perform their tasks.

No user should hold elevated permissions without documented justification.

This applies to:

- Backend consoles
- Wallet controls
- Prize pool systems
- Draw management
- Script execution

5.1.3 Need-to-Know Basis

Access to sensitive or confidential information must be restricted to individuals with a legitimate operational requirement.

Examples:

- Wallet addresses → AML and Finance teams
- Player documents → Compliance only
- Game logic → Technical leads only
- Admin logs → Security Officer and Compliance Officer only

If a user does not need data for daily work, they should not have access.

5.1.4 Multi-Factor Authentication (MFA)

MFA must be enabled for all privileged accounts, including:

- Admin panels
- Backend servers
- Wallet management tools
- Cloud consoles
- CRM dashboards
- Payment gateways
- Monitoring/alerting systems

MFA methods may include:

- Authenticator apps
- Hardware keys (preferred for crypto operations)
- SMS/email fallback only if necessary (lower security)

5.2 Administrative Access Rules

Access to critical gaming, financial, and operational systems is strictly limited and highly controlled.

5.2.1 Prize Pool Systems

Access restricted to:

- ISO
- Technical Lead (backend or system engineer)
- Finance/Admin (for oversight, not configuration)

Controls:

- Read/write access limited to authorized personnel
- Automated logs of all prize pool adjustments
- No manual script execution unless approved and logged

5.2.2 Crypto Wallet Systems

This includes:

- Hot wallet
- Cold wallet
- Multisig infrastructure
- Withdrawal queue logic

Access restricted to:

- AML Compliance Officer (monitoring only)
- Finance Lead
- Pre-approved senior management
- Technical Lead (system maintenance only, no transfer authority)

Controls:

- All wallet-related actions require MFA
- High-value withdrawals require multi-signature approval
- Automated anomaly detection must monitor unusual behavior

5.2.3 Transaction Processing Systems

Access restricted to:

- Finance team
- Compliance and AML team
- Security Officer
- Restricted technical staff with documented need

Controls:

- Force limits on manual adjustments
- All withdrawals above threshold require human approval
- Sanctions and AML checks must run automatically before transfer

- Transaction logs must be immutable and reviewable

5.2.4 Game Configuration Systems

This includes:

- Game provider configurations
- Internal game logic
- Prize algorithms and rulesets
- RNG-related components

Access restricted to:

- Technical leads
- ISO (for oversight)
- Developer team (staging only — never production unless approved)

Controls:

- All production changes must follow change management procedures
- No live-game parameter changes without documented authorization
- Audit logs must capture each modification

5.2.5 Backend Console & Admin Panels

This includes:

- Customer Relationship Management
- User management console
- Support dashboards
- Analytics dashboards
- Back-office monitoring tools

Access restricted by role-based permission groups:

- Support → limited view only
- Compliance → high-level financial/identity data
- Security → logs and system visibility
- Admin → highest privilege with strict need-to-know limitation

Controls:

- All privileged accounts must use Multi Factor Authentication (MFA)
- Session timeout enforced
- Automated alerts for unusual admin behavior

5.3 Privileged Action Monitoring & Auditability

All privileged actions must be:

Logged

- System configuration changes

- Wallet access attempts
- Withdrawal approvals
- Prize pool updates
- Admin panel access
- Suspended/locked account actions
- Login failures, password resets, MFA changes

Monitored

- Real-time monitoring through Security Information and Event Management (SIEM) tools
- Alerts for deviation from normal behavioural patterns
- Special attention to wallet-related activities

Auditable

- Logs must be tamper-resistant
- Retained according to data retention policy
- Accessible to ISO, Compliance Officer, and regulatory requests
- Reviewed quarterly (minimum)

Any suspicious privileged activity must trigger immediate investigation.

5.4 Access Review & Revocation

- Access rights must be reviewed **quarterly**, and upon role change or termination.

- Users leaving the organization must have all access removed within 24 hours.
- Vendor and contractor access must have **expiry dates** and limited permissions.
- Stale or unused accounts must be automatically disabled.

6. Authentication & Password Requirements

Strong authentication controls are essential to protecting Weeekly's systems, player data, crypto wallets, and administrative tools. This section defines mandatory requirements for all employees, contractors, vendors, and systems interacting with Weeekly platforms.

These rules apply to the entire Weeekly platform, and all administrative tools, backend systems, and third-party integrations.

6.1 Password Complexity Requirements

All passwords used to access Weeekly systems must comply with the following:

Minimum Standards

- Minimum length: **12 characters**
- Must contain:
 - Uppercase letters
 - Lowercase letters
 - Numbers
 - Special characters
- Must not contain easily guessable information:

- Names
- Dates
- Words related to Weeekly or the user's role
- Must be unique per system—**no password reuse allowed**

Password Storage Requirements

- All passwords must be hashed using industry-accepted algorithms such as:
 - **bcrypt, Argon2, or PBKDF2**
- No plaintext or reversible encryption storage is permitted.
- Password hints must not reveal information about the password structure.

Password Rotation

- Standard users: rotation required every **90 days**
- Privileged/admin users: rotation required every **60 days**
- Passwords must not repeat any of the last **5** previously used passwords
- Forced rotation triggered immediately if:
 - A breach is suspected
 - Account compromise is detected
 - Password sharing is identified

6.2 Multi-Factor Authentication (MFA) Requirements

MFA is mandatory for all staff and all privileged accounts.

MFA Requirement Applies To:

- Admin panels
- Prize pool systems
- Crypto wallet systems (hot and cold wallet access)
- Customer management and CRM dashboards
- Withdrawal processing systems
- Cloud hosting accounts (AWS, GCP, Azure, etc.)
- Git repositories and CI/CD pipelines
- Payment and KYC/AML tools
- Monitoring / SIEM platforms

Accepted MFA Methods

- Authenticator apps
- Hardware security keys (YubiKey or FIDO2 devices) — **preferred for wallet and production access**
- SMS or email MFA only permitted as backup when hardware/app MFA fails

MFA Enforcement

- MFA must be activated during onboarding
- Users cannot disable MFA without security approval
- Re-authentication required for:
 - High-risk actions

- Accessing Highly Confidential data
- Adjusting system configurations

6.3 Session Management & Timeout Rules

Session security is mandatory to protect against unauthorized access, hijacking, or shoulder surfing.

Session Timeout Rules

- Admin and privileged dashboards: Automatic logout after **10 minutes** of inactivity
- Customer support and CRM systems: Logout after **15 minutes** of inactivity
- Backend developer consoles: Logout after **10 minutes**
- Wallet and financial panels: **5 minutes** maximum inactivity

Forced Session Controls

- Sessions must expire automatically after **24 hours**, even if active
- Concurrent admin sessions are prohibited unless explicitly justified
- Re-authentication required when a session reaches a sensitive area

Session Encryption

- All sessions must use secure cookies with:
 - `httpOnly`
 - `Secure`

- `SameSite=strict`
- Tokens must expire immediately upon logout
- Session data must not be stored in local browsers beyond one session

6.4 Application Programming Interface (API) Key & Service Credential Security

API keys are considered sensitive authentication assets and must be protected accordingly.

Storage & Encryption

- API keys must be stored in secure vaults such as:
 - AWS Secrets Manager
 - HashiCorp Vault
 - GCP Secret Manager
- Keys must **never** be stored in:
 - Source code
 - Logs
 - Frontend applications
 - Emails or chat messages
- Encryption must meet Advanced Encryption Standard using a 256-bit key length (AES-256) or equivalent standards for at-rest storage.

API Key Rotation

- Mandatory rotation every **90 days**
- Immediate rotation required if:
 - A developer leaves the company
 - A breach or suspected compromise occurs
 - A key is exposed in logs, repositories, or communication channels

Access Control

- API key access must follow:
 - Role-based access control (RBAC)
 - Least privilege principle
 - Need-to-know justification
- Access logs must track:
 - Who accessed the key
 - When it was accessed
 - What it was used for

Restrictions

- API keys must be scoped to minimum privileges (read-only vs. write)
- Keys must be environment-specific:
 - Development
 - Staging

- Production
- Production keys must never be used in development environments

6.5 Account Lockout & Failed Login Attempts

To prevent brute-force attacks:

- After **5 failed login attempts**, the account is temporarily locked
- Admin accounts lock for **30 minutes** or require manual unlock by ISO
- Standard user accounts lock for **15 minutes**
- Lockout events must generate automatic alerts for monitoring

6.6 Credential Sharing & Prohibited Practices

The following are strictly prohibited:

- Sharing passwords between staff members
- Reusing passwords across systems
- Storing credentials in unsecured files, spreadsheets, or chat platforms
- Using personal accounts for work-related access
- Using outdated or weak authentication applications
- Hardcoding credentials into scripts or code repositories

Any violation will trigger an investigation and may result in disciplinary action.

6.7 Offboarding & Credential Deactivation

Upon employee departure or role change:

- All accounts must be revoked **within 24 hours**
- API keys associated with the user or team must be rotated
- Access to cloud, infrastructure, CRM, wallet systems, and support tools must be immediately terminated
- Logs must be reviewed to confirm there was no unauthorized activity prior to termination

7. Third-Party & Vendor Security

Weeekly relies on multiple third-party service providers—including game aggregators, KYC vendors, payment processors, cloud hosting platforms, and blockchain analytics tools—to operate securely and efficiently.

To ensure these partners meet Weeekly's information security, privacy, and regulatory requirements, the following controls and procedures apply to all vendors.

This section applies to all vendors that store, process, transmit, or have access to Weeekly data or systems.

7.1 Vendor Due Diligence

Before onboarding any third-party provider, Weeekly must conduct a structured risk assessment to verify the vendor's security posture and regulatory suitability.

Due Diligence Requirements

- Review the vendor's:
 - Information Security Policy

- Data Protection Policy
 - Incident Response processes
 - AML/CFT controls (if applicable)
 - Business Continuity and Disaster Recovery plans
- Assess certifications (if available):
 - ISO 27001
 - SOC 2
 - PCI DSS
 - GDPR compliance
- Review:
 - Company reputation
 - Regulatory track record
 - Litigation or breach history
 - Financial stability
- Validate that the vendor meets Curaçao Gaming Authority expectations for:
 - Player protection
 - Game integrity
 - Secure data handling
 - Anti-fraud and AML monitoring (if applicable)

Vendors cannot be approved without a completed due diligence assessment signed by the Vendor Oversight Lead, ISO, and Compliance Officer (if relevant).

7.2 Contractual Security Obligations

All vendor agreements must include legally binding clauses covering:

Mandatory Contractual Requirements

- Clear definitions of:
 - Security responsibilities
 - Access permissions
 - Restrictions on data use
- Data protection obligations (including PII and financial data)
- Requirement for secure data transmission (TLS 1.2/1.3)
- Encryption requirements for data at rest
- Notification obligations in the event of a data breach
- Requirement to comply with Weeekly's security policies
- Vendor liability and indemnification for security failures
- Prohibition on subcontracting without written approval
- Requirement for compliance with:
 - Curaçao Gaming Authority
 - Applicable AML/CFT standards
 - International data protection laws
- Mandatory participation in security audits or reviews requested by Weeekly

Contracts must be reviewed by legal counsel before execution.

7.3 Data Handling Agreements (DHA)

Vendors that process player data, financial data, or operational logs must enter into a Data Handling Agreement specifying:

- What data is collected
- Purpose of processing
- Storage location and retention period
- Security controls applied
- Data minimization requirements
- Restrictions on transferring data to third parties
- Procedures for data deletion or anonymization
- Requirements for handling user requests (access, deletion, correction)
- Secure disposal of data at end of contract

The DHA must be signed before any data exchange occurs.

7.4 Vendor Access Control Requirements

Vendor access to Weeekly systems must be strictly controlled and monitored.

Access Restrictions

- Vendors may only access systems necessary for their operational function
- Access must be:

- Role-based
 - Time-limited
 - Logged and monitored
 - Removed immediately when no longer required
- Vendor accounts must use:
 - MFA
 - Unique credentials (no shared logins)
 - Secure VPN or IP-allowlisted connections if required
- No vendor may access:
 - Prize pool logic
 - Crypto wallet systems
 - Player balances or internal AML tools
 - Highly Confidential data unless explicitly authorized

Remote Access

- Remote vendor access must be approved by ISO
- Sessions must be logged
- Actions must be monitored in real time for high-risk systems

7.5 Ongoing Monitoring & Performance Review

Weeekly must monitor all vendors continuously to ensure they maintain strong security practices over time.

Monitoring Requirements

- Review vendor security reports, SOC audits, or certifications annually
- Monitor vendor performance and reliability metrics
- Conduct annual vendor risk assessments
- Confirm vendors maintain:
 - Secure data storage
 - Encryption standards
 - Incident response readiness
 - Uptime commitments
- Evaluate real-world behaviour:
 - Promptness in resolving issues
 - Transparency
 - Response to incidents or service outages

Security Events

If a vendor experiences a breach:

- Vendor must notify Weeekly **immediately**
- Vendor must provide a written incident report
- Access to Weeekly systems may be suspended until risk is mitigated

- Internal review must be conducted to evaluate impact

7.6 Vendor Termination & Offboarding Procedures

When a vendor relationship ends or access is no longer required:

Termination Requirements

- All access credentials must be revoked immediately
- API keys must be regenerated
- VPN/IP allowlist rules must be removed
- All Weeekly data must be:
 - Returned securely, **or**
 - Destroyed with written proof
- Data disposal must comply with:
 - Data retention policies
 - AML/CFT record-keeping obligations
 - Regulatory reporting rules

Final Audit

A closing audit must be conducted to confirm:

- No residual access remains
- No data copies exist outside intended systems
- Vendor met contractual destruction or return requirements

The Vendor Oversight Lead, ISO, and Legal/Compliance must sign off on the completed offboarding checklist.

7.7 Prohibited Vendor Practices

Vendors may **not**:

- Store Weeekly production data on personal devices or unsecured servers
- Subcontract tasks without written approval
- Lower encryption standards or modify security controls without consultation
- Access Weeekly systems without MFA
- Share accounts among team members
- Retain data after contract termination
- Use Weeekly data for analytics, training, or any purpose beyond contractual obligations

Violation of any of these terms will result in suspension or termination of access.

8. Network & Infrastructure Security

Weeekly maintains a secure, resilient, and monitored infrastructure to protect platform integrity, ensure stable uptime, and safeguard all player and operational data. This section defines the technical controls, development standards, and security measures required across all systems that support the entire Weeekly platform.

These controls apply to all cloud environments, servers, APIs, backend consoles, third-party integrations, and network components.

8.1 Secure Coding Practices

Weeekly adopts secure software development lifecycle (SDLC) principles to prevent vulnerabilities in all platform components.

Requirements

- All developers must follow OWASP Top 10 and SEI CERT coding guidelines
- Code must undergo:
 - Peer review
 - Static application security testing (SAST)
 - Dynamic application security testing (DAST)
- Secrets, credentials, and API keys must **never** be stored in code repositories
- Use of environment variables and secure vaults is mandatory
- Dependencies must be monitored and updated regularly using dependency scanning tools
- Production code changes require:
 - Change management approval
 - Version control
 - Deployment logs
- High-risk components (e.g., RNG, prize pool algorithms, wallet interfaces) must undergo enhanced review

8.2 Firewalls & Network Protection

To defend the platform against unauthorized access and cyberattacks:

Firewall Controls

- Network firewalls must be configured to restrict inbound and outbound traffic based on least privilege
- IP allowlisting required for administrative access
- Database servers must not be directly exposed to the internet
- Regular firewall rule reviews must be conducted at least quarterly

Web Application Firewall (WAF)

A WAF must be deployed to protect Weeekly's web applications against:

- SQL injection
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- API abuse
- Known vulnerability exploits

WAF logs must integrate into central monitoring systems for real-time alerting.

8.3 Distributed Denial of Service (DDoS) Mitigation

Given Weeekly's global audience and operational model, scalable DDoS protection is mandatory.

Requirements

- Use of cloud-based DDoS mitigation services
- Automated rate limiting on API endpoints

- Traffic anomaly detection and auto-blocking mechanisms
- Redundant infrastructure to maintain availability during attacks

Mitigation tools must be monitored continuously, and response strategies documented within the Incident Response Plan.

8.4 Encryption Standards

Sensitive information must be protected by strong encryption whether in transit or at rest.

8.4.1 Data in Transit

- All data transmitted across public or internal networks must use:
 - **TLS 1.2** or **TLS 1.3**
- Certificates must be rotated prior to expiration
- Insecure protocols such as HTTP, FTP, and Telnet are strictly prohibited

8.4.2 Data at Rest

- All sensitive data must be encrypted using:
 - **AES-256** or stronger technologies
- Encryption must apply to:
 - Database storage
 - Backups
 - Logs containing PII
 - Hot wallet infrastructure

- API secrets and access tokens

8.4.3 Key Management

- Encryption keys must be stored in hardware security modules (HSMs) or approved cloud key management services
- Key rotation must occur every 12 months or upon suspected compromise
- Access to keys must follow role-based controls and require MFA

8.5 Environment Segmentation & Isolation

Weeekly maintains strict separation of environments to reduce risk, prevent accidental data leakage, and ensure smooth development operations.

8.5.1 Environment Definitions

- **Production:** Live player platform and operational systems
- **Staging:** Environment for pre-production testing
- **Development:** Code development and non-sensitive testing environment

Rules & Restrictions

- **Production access** is limited to approved senior technical staff
- **Staging and development environments must not contain any production data**
- Synthetic or anonymized test data must be used for all development/testing
- Network and database segregation must prevent lateral movement between environments

- CI/CD pipelines must enforce environment-specific credentials

8.6 Infrastructure Hardening

All systems must be hardened to reduce attack surfaces.

Requirements

- Disable unused ports, services, and default accounts
- Regular patching of:
 - Operating System (OS)
 - Databases
 - Application frameworks
 - Libraries and dependencies
- Enforce secure configurations for:
 - Web servers
 - Database servers
 - Containerized applications
- Use anti-malware and endpoint protection where applicable
- Store and update system configuration baselines

8.7 Logging & Monitoring of System Activity

Comprehensive logging and monitoring are essential to detect anomalies, investigate incidents, and maintain auditability.

Logging Requirements

Logs must be generated for:

- Login attempts (successful and failed)
- Privileged account actions
- Wallet operations
- Prize pool modifications
- Withdrawal processing
- API requests
- Firewall/WAF events
- Application errors and crashes
- System and infrastructure changes

Retention & Protection

- Logs must be tamper-proof and stored in secure locations
- Logs must be retained according to data retention policy and regulatory requirements
- Logs containing sensitive data must be encrypted

Real-Time Monitoring

- Logs must feed into a SIEM platform (Security Information & Event Management)
- Automated alerts must be triggered for:
 - Unusual admin actions

- Suspicious API behaviour
- DDoS indicators
- Wallet anomalies
- High-risk access attempts

Monitoring must be conducted 24/7 by security or automated systems.

8.8 Network Redundancy & High Availability

To ensure uninterrupted operation:

- Use load balancing and failover mechanisms
- Maintain redundant cloud regions or availability zones
- Implement automated backups and restoration testing
- Ensure database replication (real-time or near real-time)
- Maintain a minimum uptime Service Level Agreement (SLA) of 99.5% for core systems

8.9 Periodic Reviews & Penetration Testing

- Conduct internal and external penetration testing at least annually
- Run vulnerability scans monthly (or continuously via automated tools)
- Address identified vulnerabilities based on severity:
 - Critical: within 72 hours

- High: within 7 days
- Medium: within 30 days
- Low: at next scheduled update

Results must be documented and reviewed by the ISO and CTO.

9. Application & Game Security

Weeekly is committed to ensuring the security, fairness, and integrity of all gaming applications across the entire Weeekly platform.

This section outlines the controls required to prevent manipulation, maintain game fairness, and protect against cyber threats affecting application layers.

These controls apply to internally developed systems as well as third-party game providers.

9.1 RNG Integrity Protection

Random Number Generators (RNGs) must be secure, unbiased, and protected from tampering.

Requirements

- RNG implementations must be certified by an approved testing laboratory where applicable
- All third-party RNG systems must provide certification annually
- RNG configuration parameters must be:
 - Locked behind admin permission layers
 - Encrypted

- Logged when accessed
- No developer or staff may modify RNG behavior in the production environment
- Any manual override or emergency intervention must be logged and reviewed

For internal Weeekly token-based games, RNG data must be cryptographically secure and cannot be predictable or seed-manipulable.

9.2 Game Tampering & Manipulation Prevention

Weeekly must protect its applications—both internal and third-party—from malicious interference.

Core Protections

- Code obfuscation for client-side logic to prevent reverse engineering
- Server-authoritative game outcomes (client cannot decide outcomes)
- Checksums or signatures to validate data integrity
- Anti-automation measures to prevent botting or unfair play
- Input validation to block injection attacks (SQL, command, template, or code injection)
- Replay-attack protection using unique transaction identifiers
- Secure websocket and API communications
- Anti-multi-accounting checks
- Coin outcomes must be validated server-side
- Leaderboard calculations locked to backend computations

9.3 Reverse Engineering & Unauthorized Modification Protection

To protect intellectual property and prevent exploitation:

- Application binaries must be hardened against decompilation
- Sensitive application logic must remain server-side
- Disable debugging features in production builds
- Remove unused code paths before deployment
- Implement certificate pinning in mobile/web apps where relevant
- Prevent modification of client traffic using:
 - TLS enforcement
 - HSTS
 - Strict CORS policies

No production API must be accessible without authentication and authorization.

9.4 Secure API Integration

All integrations with third-party game providers, payment systems, or operational tools must adhere to strong API security requirements.

API Security Controls

- Encrypted communication via TLS 1.2/1.3
- IP allowlisting for inbound/outbound calls
- API key protection using secure vault storage
- Strict RBAC for access to API credentials
- Rate limiting to prevent abuse

- Signature verification for incoming provider callbacks

SoftGamings Integration Requirements

- Use Webhooks/API endpoints only through secure channels
- Validate provider payloads for authenticity and structure
- Monitor response anomalies and unexpected patterns
- Log all API requests and responses in tamper-resistant logs

9.5 Code Review & Development Controls

All application code must undergo structured review processes to reduce security risks.

Mandatory Code Review Requirements

- Peer review of all code before merge
- Security checkpoints during development
- Specialized review for critical systems (wallets, game logic, prizes)
- Use of automated scanning tools to detect vulnerabilities:
 - Static (SAST)
 - Dynamic (DAST)
 - Dependency vulnerability scanners

Developer Access Rules

- Developers may not access production databases or live data

- Sensitive configuration data must be masked during development
- Only senior engineers may approve production releases

9.6 CI/CD Pipeline Security

Continuous Integration and Continuous Deployment pipelines must be protected against compromise.

Controls

- MFA required for access to CI/CD tooling
- Separate pipelines for development, staging, and production
- No secrets stored in pipelines; all secrets must come from encrypted vaults
- Automated tests and scans must run before deployment
- Manual approval required for any production deployment
- Deployment logs must be retained and audited
- Pipeline tools must be monitored for:
 - Unauthorized job executions
 - Unexpected configuration changes
 - Credential access

Compromises in CI/CD are treated as critical incidents.

9.7 Penetration Testing & Vulnerability Assessments

Weeekly must proactively test its application security posture.

Penetration Testing Schedule

- **External penetration testing:** at least annually
- **Internal penetration testing:** annually or after major releases
- **API-specific pentests** for game logic, wallets, and prize pool systems
- **Mobile/web application pentests** if applicable

Vulnerability Scanning

- Automated scans must run:
 - Weekly for staging
 - Daily or continuously for production
- Critical vulnerabilities must be remediated within **72 hours**
- High vulnerabilities: within **7 days**
- Medium vulnerabilities: within **30 days**
- Low vulnerabilities: next planned cycle

Results must be logged, risk-scored, and reviewed by the ISO.

9.8 Anti-Fraud & Gameplay Integrity Measures

In accordance with new Curaçao regulations, Weeekly must deploy fraud detection and gameplay integrity mechanisms.

Anti-Fraud Controls

- Real-time monitoring for suspicious betting patterns

- Player behavior anomaly models (ML-based or rule-based)
- Detection of:
 - Multiple accounts from same identity
 - VPN or proxy abuse
 - Device fingerprint mismatches
 - Abnormal win patterns
 - Artificial inflation of performance in Rivals mode
- Transaction risk scoring
- Automated freezing of flagged accounts

Gameplay Integrity

- Regular audit of leaderboard fairness
- Verification of game outcomes via server-side logs
- Alerts for improbable outcomes or impossible win streaks
- Integrity checks on bonus exploitation and abuse patterns

These measures must integrate into Weeekly's AML/compliance framework.

9.9 Application Logging & Audit Trails

To ensure accountability, traceability, and incident readiness:

Logs Must Capture

- Every gameplay result

- All API requests/responses
- Admin interactions with game settings
- Prize pool actions
- Fraud alerts and anomaly detections
- Errors, warnings, and unexpected behaviors

Log Requirements

- Logs must be tamper-resistant
- Logs containing PII or financial data must be encrypted
- Retention period must meet regulatory requirements
- Logs must be accessible to ISO, Compliance Officer, and regulators

10. Crypto & Financial Security Controls

Weeekly implements strict crypto asset controls to ensure the security, integrity, and regulatory compliance of all transactions processed across its platforms. These controls protect player funds, prevent unauthorized transactions, and ensure compliance with Curaçao Gaming Authority requirements and global AML/CFT standards.

The following policies apply to the management of all digital assets associated with Weeekly, including deposits, withdrawals, prize distributions, wallet infrastructure, and internal fund movements.

10.1 Wallet Management

10.1.1 Hot & Cold Wallet Separation

To minimize exposure to theft or compromise:

- **Hot wallets** are used exclusively for real-time user transactions (e.g., withdrawals and automated processes).
- **Cold wallets** are used for long-term secure storage of the majority of funds.
- Hot wallets must only maintain the minimum float required for operational liquidity.
- Transfers between hot and cold wallets require strict authorization and are logged.

This reduces the risk of loss due to external attacks or internal misuse.

10.1.2 Multi-Signature Authorization

All high-value wallet operations must require multiple authorized personnel.

- Multi-signature (multi-sig) wallets or secure MPC solutions must be used for:
 - Large withdrawals
 - Cold wallet movements
 - Funding hot wallets
- Signature thresholds must be defined (e.g., 2-of-3, 3-of-5) based on risk tier.
- No individual may have unilateral authority to move significant funds.

This prevents single-point-of-failure risk.

10.1.3 Private Key Protection

Private keys must be protected using industry-grade cryptographic safeguards.

- Keys must be stored in a secure, audited custody platform (e.g., MPC/HSM-based provider).
- No private key may ever:
 - Be exported
 - Be stored on local devices
 - Be shared or transmitted
- Backup keys must be encrypted and stored separately under strict access controls.

Access to key management systems must require MFA and role-based privileges.

10.1.4 Withdrawal Approval Procedures

Weeekly defines a structured, tiered approach to approving withdrawals:

Tier 1 — Low-value withdrawals

- Processed automatically by system rules
- Still subject to AML/sanctions/mixer screening

Tier 2 — Medium-value withdrawals

- Require manual review by Finance or AML team
- Additional transaction velocity and behavioural checks apply

Tier 3 — High-value withdrawals

- Require multi-signature approval
- Mandatory AML/EDD review

- Potential request for source-of-funds verification

Tier 4 — Exception withdrawals

- Suspicious transactions
- Requests from flagged accounts
- Blocked pending further investigation

All withdrawals must be logged and auditable.

10.2 Transaction Controls

Weeekly applies stringent monitoring and automated blockchain intelligence tools to detect suspicious or prohibited activity.

10.2.1 AML Monitoring

All deposits and withdrawals must pass through automated AML screening systems capable of identifying:

- High-risk wallets
- Structuring patterns
- Fraud indicators
- Deposit patterns inconsistent with user profile

Any flagged activity must be escalated to Compliance for review.

10.2.2 Sanctions Screening

All wallet addresses interacting with the platform must be screened against:

- Office of Foreign Assets Control (OFAC) sanctions lists
- European Union (EU) sanctions lists
- United Nations (UN) sanctions lists
- applicable New Zealand and relevant international sanctions lists
- known illicit wallet databases provided by blockchain analytics services (e.g., mixers, darknet associations, ransomware, and sanctioned entities)

Screening must occur prior to transactions being processed, and any positive matches must result in immediate blocking, review, and escalation in accordance with the AML/CFT procedures and regulatory obligations.

10.2.3 Mixer Detection

Automated systems must screen for:

- Tornado Cash exposure
- Privacy coin bridging
- High-risk mixers
- Peel chains
- Tumblers
- Obfuscation techniques

Exposure above defined thresholds must trigger:

- Automatic deposit freezing
- Mandatory compliance review

- Report filing (if required)

10.2.4 Transaction Velocity Checks

To detect abnormal behaviour:

- Automated rules must detect rapid deposit/withdrawal patterns
- Rate limits applied to withdrawals during suspicious spikes
- Daily/weekly transaction caps enforced per risk tier
- Pattern detection used to identify wash-trading-type behaviour

10.2.5 Suspicious Activity Reporting (SAR)

When suspicious activity is identified:

- The AML Officer must review the case
- The account may be:
 - Temporarily locked
 - Subject to additional KYC/EDD
 - Restricted from withdrawals
- If warranted, reporting obligations must be fulfilled in accordance with Curaçao and global AML guidelines

Records of suspicious activity report reviews must be securely retained.

10.3 Funds Protection Measures

Weeekly ensures that all player assets are protected from misuse, operational risk, or insolvency scenarios.

10.3.1 Segregation of Player Balances

Player funds must be separated from operational or corporate funds.

- Player balances held in custody must not be used for:
 - Operating expenses
 - Investments
 - Salaries
- Systems must maintain a real-time ledger of segregated balances
- Custody accounts must be reconciled daily

This ensures solvency transparency and player fund protection.

10.3.2 Tamper-Proof Audit Trails

All financial activity must be fully logged.

Audit logs must include:

- Deposits
- Withdrawals
- Internal transfers
- Wallet replenishments
- Cold→hot wallet movements
- Failed or blocked transactions

- AML/Sanctions screening results

Logs must be:

- Immutable
- Encrypted
- Stored in secure environments
- Accessible only by ISO, AML, and authorized finance personnel

Regulators may request audit logs during inspections.

10.3.3 Custody Provider Controls

Weeekly uses a regulated digital asset custody provider that offers:

- MPC level key protection
- Transaction whitelisting
- Role-based access management
- Audit logging
- Biometric/cryptographic authorization
- Withdrawal policy enforcement
- Advanced fraud and risk controls

This provider must meet industry-leading security and compliance standards and integrate seamlessly into Weeekly's AML and risk workflows.

10.3.4 Reconciliation & Financial Integrity

Daily reconciliation ensures all balances and transactions match across:

- Blockchain records
- Internal systems
- Custody provider logs
- Accounting records

Discrepancies must be escalated immediately and investigated by Finance and Security teams.

10.4 Incident Response for Crypto Assets

Any abnormal wallet or transaction-related activity must trigger immediate incident protocols.

Triggers

- Unauthorized withdrawal attempts
- Suspicious account behavior
- Private key or custody system alerts
- AML flags indicating high-risk exposure
- Failed multi-sig approvals

Actions

- Freeze affected wallets or accounts
- Escalate to AML Compliance Officer
- Notify senior management

- Conduct forensic review using blockchain analytics tools
- Document and store all evidence

11. Logging, Monitoring & Alerting

Weeekly maintains comprehensive logging and real-time monitoring of all critical systems to detect unauthorized activity, protect player funds, maintain fairness of gameplay, and ensure compliance with regulatory and AML/CFT obligations. All logs must be tamper-resistant, securely stored, and accessible only to authorized personnel.

This section applies to the entire Weeekly platform, along with backend systems, admin consoles, and third-party integrations.

11.1 Real-Time Monitoring Requirements

Weeekly must continuously monitor system activity across all critical components.

11.1.1 Login Attempts

- Successful and failed authentication attempts
- MFA failures and resets
- Brute-force detection
- Geographic anomalies (sudden login from new regions)
- Device fingerprint mismatches

Suspicious login activity must generate alerts.

11.1.2 Wallet Movements

All deposit, withdrawal, and internal wallet transactions must be monitored in real time.

Monitoring includes:

- Incoming deposits (screened for risk)
- Outgoing withdrawals (multi-sig approval and AML checks)
- Hot→cold and cold→hot wallet transfers
- Attempted unauthorized wallet access
- Rapid or unusual transaction velocity

Abnormal wallet behavior triggers immediate compliance review.

11.1.3 Administrative Actions

Admin panel activity must be logged and monitored with elevated scrutiny.

Tracked actions include:

- Account suspensions/unlocks
- Manual withdrawal approvals
- Changes to prize pool logic
- Modifications to game settings or platform rules
- Access to PII or confidential data
- Changes to system configurations

Privileged actions must be auditable and reviewed routinely.

11.1.4 System Performance

Platform performance must be monitored to ensure operational integrity.

Monitored metrics include:

- Server load
- API response times
- Memory and CPU usage
- Database performance
- Error rates and application crashes
- Uptime tracking

Performance anomalies may indicate security incidents.

11.1.5 Game Session Irregularities

Gameplay must be monitored for fairness and integrity.

Detection must include:

- Abnormal win rates
- Rapid-fire wagering patterns
- Leaderboard manipulation attempts
- Exploits or bot behavior
- Collusion or multi-account activities
- Abnormal return-to-player (RTP) shifts

Any anomaly linked to potential fraud or manipulation must be escalated.

11.2 Log Requirements & Retention

All systems must generate logs sufficient for forensic analysis, compliance audits, and operational monitoring.

11.2.1 Mandatory Logs

Logs must be generated for:

- Login events
- Admin actions
- Wallet transactions
- Game outcomes and RNG seeds/hashes (where applicable)
- API calls (incoming and outgoing)
- System errors and warnings
- AML flags and compliance actions
- Withdrawal processing and approvals

11.2.2 Retention Periods

Logs must be retained for the period required by Curaçao Gaming Authority and AML guidelines:

- **Standard operational logs:** minimum **2 years**
- **AML-related logs (transactions, KYC, SAR reviews):** minimum **5 years**
- **Security incident logs:** minimum **5 years**
- **Backup logs:** 1 year minimum

Retention may be extended for legal, AML, or audit requirements.

11.3 Tamper-Proof Logging

Logs must be protected from unauthorized modification or deletion.

Tamper-Proof Measures

- Logs stored in immutable storage (append-only or WORM)
- Access restricted to the ISO, Compliance Officer, and senior technical leads
- Cryptographic signing or hashing of log batches
- Offsite backups of logs
- Log access and modification attempts logged separately

Any evidence of tampering is classified as a **critical incident** and must be escalated immediately.

11.4 Blockchain Intelligence Integration

Weeekly must integrate a blockchain monitoring capability into all deposit and withdrawal processing pipelines to identify, assess, and mitigate AML/CFT risks in real time.

Monitoring must include detection of:

- exposure to sanctions-listed entities
- mixer, tumbler, or privacy-enhancing services
- darknet or other high-risk address associations
- known fraud networks and scam typologies
- stolen or compromised funds indicators

- wallet clustering behaviour and transaction history scoring

The monitoring solution must provide:

- automated risk scoring and classification
- real-time alerts and escalation triggers
- automated blocking or holding of high-risk transactions
- historical analysis of wallet and transaction behaviour

This capability forms a mandatory component of Weeekly's AML and Counter-Financing of Terrorism (CFT) controls and is required for risk detection, reporting, and ongoing compliance.

11.5 Automated Alerts & Threshold Monitoring

Alerting mechanisms must be configured to flag unusual or high-risk events.

Threshold Alerts Must Trigger For:

- Multiple failed login attempts
- Sudden spikes in withdrawal requests
- Large single-value withdrawal attempts
- Wallet movements outside normal operational limits
- Game integrity anomalies
- System performance degradation
- Unrecognized API calls
- Patterns consistent with bonus abuse

- Repeated AML flags from a single user
- Multiple accounts linked by device/IP

Alert Severity Levels

- **Critical:** requires immediate investigation (wallet anomalies, admin misuse)
- **High:** action within 2 hours (game manipulation, performance alerts)
- **Medium:** action within 24 hours
- **Low:** action during next scheduled review

Alerts must be logged, investigated, and documented.

11.6 Centralized Monitoring (SIEM Integration)

All logs and alerts must be aggregated into a centralized Security Information & Event Management (SIEM) solution.

SIEM Duties

- Correlate security events
- Detect multi-step attack patterns
- Flag privilege escalation
- Monitor insider threats
- Perform behavioral baselining
- Provide automated incident timeline creation

SIEM must operate continuously and generate real-time notifications.

11.7 Regular Review of Logs & Alerts

- Daily automated review of critical logs
- Weekly review of admin actions
- Monthly reporting to Senior Management
- Quarterly deep-dive for compliance
- Annual audit with external oversight if required

All findings must be documented along with corrective actions.

12. Incident Response Plan

Weeekly maintains a structured and comprehensive Incident Response Plan (IRP) to ensure rapid detection, containment, and resolution of security events. This plan ensures protection of player data, continuity of operations, and compliance with Curaçao Gaming Authority (CGA) requirements.

All incidents must be handled with urgency, accuracy, and proper documentation.

This policy applies to:

- All Weeekly systems and environments
- All staff, contractors, and vendors
- All incidents affecting security, operations, data integrity, financial systems, or player trust

12.1 Incident Categories

Incidents must be classified into one or more of the following categories:

12.1.1 Security Incidents

Events impacting confidentiality, integrity, or availability:

- Unauthorized system access
- Privilege escalation
- Malware infections
- DDoS attacks
- API abuse
- Suspicious admin activity
- Server compromise

12.1.2 Operational Incidents

Events affecting service delivery:

- Server outages
- Game provider API downtime
- System misconfigurations
- Deployment failures
- Payment processing delays

12.1.3 Data Breaches

Confirmed or suspected exposure of:

- Player PII

- Wallet transaction data
- Admin credentials
- Logs containing sensitive information

12.1.4 Fraud & Financial Incidents

Events involving:

- Abnormal win patterns
- Bonus abuse
- Multi-accounting
- SUS wallet activity
- Suspicious withdrawals
- AML flags requiring escalation
- Stolen crypto exposure
- Account takeover

Fraud incidents require coordination with AML and Compliance teams.

12.2 Incident Reporting Channels

All employees and vendors must report suspected incidents immediately using one of the following channels:

- Internal incident reporting system (ticket or form)
- Direct contact with Incident Response Lead

- Email to the security mailbox (dedicated alias)
- Automated alert from monitoring/SIEM tools
- Escalation from AML/compliance systems

No employee may ignore or delay reporting a potential incident.

12.3 24/7 Escalation Procedure

Given the global nature of gaming operations, Weeekly follows a **24/7 escalation pipeline**.

Tier 1 — Automated Detection or Support Escalation

- SIEM, monitoring tools, AML alerts
- Support team flags suspicious behaviour
- Logged immediately and sent to on-call responder

Tier 2 — Incident Response Lead

- Reviews severity
- Takes immediate action (freeze account, block IP, disable API key, etc.)
- Notifies ISO, Compliance Officer, and CTO

Tier 3 — Executive & Regulatory Escalation

Triggered for:

- Data breaches
- Theft/fraud cases

- Major outages
- High-value wallet compromises
- Regulatory exposure

Escalation to:

- CEO / Senior Management
- AML Officer
- Legal team
- Curaçao Gaming Authority (when required)

12.4 Communication Plan

Internal Communication

- Dedicated secure channel (Slack/Teams) for incident coordination
- Incident Response Lead provides updates to ISO and CTO
- Daily updates during ongoing critical incidents

External Communication

Only designated personnel may communicate to:

- Players
- Partners
- Vendors

- The public
- Authorities

External communication must:

- Be approved by Senior Management
- Avoid speculation
- Provide clear, accurate information
- Maintain confidentiality

Player Notification

If player impact occurs:

- Notify affected users promptly
- Provide steps for protection (password resets, MFA, etc.)
- Provide regulatory-approved wording

12.5 Response Timeline Expectations

Weeekly follows strict timelines:

Incident Severity	Initial Response	Mitigation	Full Investigation
Critical	within 15 minutes	within 2 hours	within 24 hours
High	within 30 minutes	within 8 hours	within 48 hours

Medium	within 2 hours	within 24 hours	within 5 days
Low	within 24 hours	within 72 hours	within 7 days

Critical incidents include:

- Wallet compromise
- Data breach
- Admin credential theft
- Fraud causing material loss
- Platform-wide outages

12.6 Containment, Eradication & Recovery Steps

Incident response must follow the structured lifecycle below.

12.6.1 Containment

- Freeze affected accounts
- Disable compromised systems or API keys
- Block malicious IPs or sessions
- Isolate infected servers from the network
- Prevent further wallet movements
- Suspend suspicious withdrawals
- Halt affected features (e.g., games, deposit flow, API endpoints)

12.6.2 Eradication

- Remove malware or malicious code
- Revoke compromised credentials
- Patch exploited vulnerabilities
- Restore secure configurations
- Update firewall/WAF rules
- Reset admin and system passwords
- Validate cleanup with fresh scans

12.6.3 Recovery

- Restore systems from verified backups
- Re-enable services gradually
- Test stability and confirm no persistence threats remain
- Monitor systems with heightened scrutiny
- Document all recovery steps
- Resume normal operations only after ISO approval

12.7 Post-Incident Analysis & Documentation

After any major incident, a formal review must be conducted within **48–72 hours**.

Post-Incident Review Must Include

- Root cause analysis

- Timeline of events
- Systems & data affected
- Actions taken
- Recommendations for improvement
- Required security enhancements
- Staff training or process updates

A full report must be:

- Approved by ISO
- Filed for compliance records
- Shared with Senior Management
- Used to update the Information Security Policy

12.8 Regulatory Notification (CGA Requirement)

Weeekly is obligated to notify the Curaçao Gaming Authority in cases where incidents affect:

- Player data confidentiality
- Platform integrity
- Wallet or financial system compromise
- Game fairness or RNG integrity
- Major outages or downtime

- Fraud or AML breaches with material impact

Notification must include:

- Nature of the incident
- Time and date of discovery
- Systems and players affected
- Immediate actions taken
- Planned remediation
- Expected next steps

Communication with CGA must be timely, accurate, and fully documented.

12.9 Continuous Improvement

Weeekly must regularly:

- Update the Incident Response Plan
- Conduct internal drills and simulations
- Train staff annually
- Integrate lessons learned into future improvements
- Review new threat intelligence and apply updates

13. Business Continuity & Disaster Recovery (BCDR)

Weeekly maintains a comprehensive Business Continuity and Disaster Recovery (BCDR) framework to ensure uninterrupted operation of gaming services, protection of player assets, and rapid restoration of critical systems in the event of a disruption. This framework applies to The entire Weeekly platform.

13.1 BCDR Objectives

The objectives of Weeekly's BCDR program are to:

- Ensure critical systems and services remain available during disruptions
- Protect player data, game integrity, and wallet security
- Restore full operations within defined recovery time objectives
- Maintain continuity of casino games, raffle draws, and financial transactions
- Satisfy regulatory expectations of the Curaçao Gaming Authority
- Minimize operational and reputational impact

13.2 Backup Strategy

13.2.1 Backup Frequency

Weeekly performs scheduled backups for all critical systems:

- **Databases (player accounts, transactions, game logs):** hourly incremental + daily full
- **Wallet/hot-wallet configuration & policy data:** real-time replication
- **Application code repositories:** continuous versioning
- **Infrastructure configurations (IaC, server settings):** daily

- **SIEM logs, AML logs, monitoring systems:** hourly

13.2.2 Backup Encryption

- All backups must be encrypted using **AES-256** or stronger
- Encryption keys must be stored in secure KMS environments (HSM/MPC custody platforms)
- Backups containing PII, wallet metadata, or transaction logs must never be stored unencrypted

13.2.3 Backup Storage Locations

Backups must be stored in:

- **Primary secure cloud storage** (same region)
- **Secondary, geographically separated region**
- **Offline/cold storage for disaster-class backups**

This ensures redundancy even in the event of cloud or regional outages.

13.3 Restoration Procedures

In the event of system failure, data corruption, or incident requiring rollback:

Restoration Steps

1. ISO or Technical Lead initiates recovery protocol
2. Validate integrity of backup version to be restored
3. Restore databases, services, or configurations in priority order (see Section 13.6)

4. Conduct integrity checks and validate system behavior
5. Re-enable public access only after security verification
6. Document restoration steps and file in BCDR log

Validation Requirements

- No corrupted or partial backups may be restored
- System must pass health checks, QA tests, and security scans before reopening
- Financial and wallet reconciliation must be verified before re-enabling transactions

13.4 Redundancy & Failover Architecture

Weeekly uses a multi-layer redundancy model to maintain availability.

13.4.2 Infrastructure Redundancy

- **Load-balanced servers** for application delivery
- **Multi-zone cloud deployment** (at least 2 availability zones)
- **Redundant database replicas**
- **Failover routing** managed by automated systems
- **High-availability wallet provider infrastructure**

13.4.3 Failover Trigger Conditions

Automatic failover activates when:

- Primary server or region becomes unreachable

- Database health checks fail
- Platform experiences major performance degradation
- Security incident requires isolation of a compromised environment

13.4.4 Manual Failover

Manual override may occur for:

- Planned maintenance
- Emergency system isolation
- Major updates affecting production infrastructure

All failover events must be logged and reviewed.

13.5 Recovery Time & Recovery Point Objectives

Weeekly defines the following RTO (Recovery Time Objective) and RPO (Recovery Point Objective):

Critical Systems

System	RTO	RPO
Wallets / Crypto Infrastructure	15 minutes	0 minutes (real-time replication)
Raffle Draw Logic & Prize Pools	30 minutes	5 minutes
Game Engines (Rivals & Casino)	30 minutes	15 minutes
Authentication / Player Login	1 hour	15 minutes
Admin Panels & Monitoring	2 hours	30 minutes

Non-critical content (marketing, public pages)

24 hours 12 hours

These targets ensure continuity of critical wagering and wallet functions.

13.6 Continuity of Raffle & Casino Operations During Outages

Weeekly must maintain fairness and player trust even during disruptions.

13.6.1 Raffle Draw Continuity

If Weeekly raffle operations are disrupted:

- All ticket entries must be preserved in secure, replicated databases
- Prize pool amounts must remain unchanged and tamper-proof
- Raffle draws must not occur until systems are fully restored and validated
- Users must be notified of any rescheduled draw
- Draw algorithms must log the timestamp of execution to maintain fairness

13.6.2 Casino Operations Continuity

If casino or Rivals systems fail:

- All active bets/spins must be resolved fairly upon recovery
- Incomplete sessions must be logged and reconciled automatically
- Player balances must remain consistent across recovery
- All third-party game providers must be notified
- Failed or interrupted transactions must be revalidated on restore

13.6.3 Wallet/Financial Continuity

Critical wallet operations follow special rules:

- All pending withdrawals must pause during outages
- Deposits must remain visible but may be delayed in settlement
- Any blockchain transactions in-flight must be reconciled upon recovery
- System must prevent double-counting or double-spending

13.7 Disaster Classes & Response Procedures

13.7.1 Minor Incident

- Single service disruption
- No data loss
- Resolved with standard restore procedures

13.7.2 Major Incident

- Database outage
- Region failure
- Extended downtime of game provider
- Requires multi-team coordination

13.7.3 Disaster Scenario

- Cloud region-wide outage
- Wallet provider downtime

- Breach requiring full environment rebuild
- RTO/RPO timelines must be strictly followed

13.8 Staff Roles During BCDR Events

- **Incident Response Lead:** coordinates activation of BCDR plan
- **ISO:** ensures security compliance during restoration
- **Technical Lead:** manages system recovery and failover
- **AML/Compliance Officer:** monitors financial and transaction integrity
- **Customer Support Lead:** prepares player communication
- **Management:** approves public statements if needed

13.9 Testing & Review

BCDR procedures must be tested to ensure readiness.

Testing Requirements

- Annual full BCDR simulation
- Quarterly backup restoration tests
- Monthly failover testing in staging
- After any major architecture change

Review Process

- Post-test reports must be documented
- Improvements must be implemented
- Senior Management must sign off on BCDR updates

13.10 Continuous Improvement

Weeekly will review BCDR policies annually or after:

- Incidents
- Infrastructure changes
- Regulatory updates
- Custody provider changes
- New gaming integrations

BCDR documentation must always reflect the current operational model.

14. Data Protection & Retention

Although Curaçao is not part of the EU and therefore not bound by GDPR, the Curaçao Gaming Authority (CGA) requires operators to implement **GDPR-style data protection controls** to protect player information, ensure fair handling, and align with international best practices.

Weeekly is committed to maintaining strict privacy, data minimisation, and secure data lifecycle management across all systems.

This section applies to all personal, financial, gaming, transactional, and operational data processed by Weeekly, Weeekly Rivals, and the casino environment.

14.1 Data Protection Principles

Weeekly follows the core GDPR-aligned principles:

- **Lawfulness, fairness, and transparency**
- **Purpose limitation** (only collect what is required)
- **Data minimisation**
- **Accuracy**
- **Integrity and confidentiality**
- **Storage limitation**
- **Accountability**

All staff and vendors must adhere to these principles.

14.2 PII Minimisation

Weeekly limits the collection, storage, and processing of personal data to what is strictly required for:

- Account creation
- Fraud prevention
- AML/KYC compliance
- Transaction and gameplay monitoring
- Regulatory reporting
- Customer support

Data Minimisation Rules

- Only essential PII (name, email, DOB, IP, device signal) is collected during onboarding
- Additional data (documents, selfie, proof of address) is collected only when:
 - Required for regulatory KYC
 - Triggered by risk-based AML checks
- No unnecessary or sensitive personal information (e.g., ethnicity, political views, biometrics beyond KYC vendor needs) is stored in Weeekly systems
- Developers must never use production PII in staging or development environments
- PII access follows the “need-to-know” principle

14.3 Data Retention Schedule

Weeekly maintains a structured data retention schedule based on operational need, regulatory requirements, and AML obligations.

14.3.1 Retention Timeframes

Data Type	Minimum Retention	Notes
Transaction & blockchain logs	5 years	AML/CFT requirement
KYC records (documents, verification data)	5 years	AML requirement (post-account closure)
Gaming logs (bets, spins, RNG data)	2 years	CGA audit expectation
Account information & profile data	Active + 2 years	Unless deletion requested
Customer support tickets	2 years	Operational requirement

Security & access logs	2–5 years	Depending on incident severity
Financial & accounting records	7 years	Standard accounting law
Backups	30–365 days	Depending on type (short-term or archival)

Retained data must be encrypted, access-controlled, and stored securely.

14.4 Secure Disposal & Data Destruction

At the end of the retention period, Weeekly must securely dispose of or anonymise data.

Requirements

- Electronic records must be securely wiped using industry-standard deletion protocols
- Physical documents (if any) must be shredded or destroyed
- Backups containing expired data must be securely overwritten or rotated out
- Vendors must provide proof of destruction for any data processed on their systems
- Destruction must be documented in a **Data Disposal Log**

No expired or unnecessary data may remain in production systems.

14.5 Player Data Access, Export & Correction Rights

While Curaçao does not impose GDPR obligations, Weeekly voluntarily applies GDPR-style user rights to ensure transparency and trust.

Player Rights Provided

1. **Right to Access**

Players can request a copy of personal data held by Weeekly.

2. **Right to Correction**

Incorrect information can be updated upon request.

3. **Right to Erasure (Limited)**

Players may request deletion of their account data **unless data must be retained** for:

- AML obligations
- Transaction history
- Fraud investigations
- Regulatory requirements

4. **Right to Data Portability**

Players may request an export of their account history (JSON/CSV).

Verification Requirements

Before fulfilling any request, Weeekly must:

- Verify account ownership
- Ensure no AML/CFT obligations prevent deletion
- Confirm the user is not subject to a compliance investigation

Requests must be fulfilled within **30 days** unless extended for complexity.

14.6 Player Data Export Controls

Data exports must be securely controlled to prevent misuse or unauthorized disclosure.

Controls

- Export requests must be logged
- Only authorized personnel (Compliance or Support Lead) may initiate exports
- Files must be encrypted before delivery
- Export delivery must use secure channels (encrypted email or secure download link)
- Sensitive fields must be masked where unnecessary

No PII may be exported to third parties without legal justification and security agreements.

14.7 Secure Backup Handling

All backups containing sensitive or operational data must be protected with strong security controls.

Backup Security Requirements

- All backups must be encrypted with **AES-256**
- Access to backup storage must be role-based and MFA-protected
- Backups must not be stored on personal or portable devices
- Backup logs must record:
 - Creation time
 - Storage location
 - Access attempts
- Backups must be stored in secured cloud regions

- Backups containing expired data must be rotated out according to retention schedules

Backups must be tested periodically to ensure restorability (see BCDR section).

14.8 Data Sharing with Third Parties

Any sharing of player or operational data must be:

- Purpose-limited
- Restricted to essential operational partners
- Covered by a Data Handling Agreement (DHA)
- Logged and auditable
- Reviewed by the ISO and Compliance Officer

Examples of allowed sharing:

- KYC vendors (identity verification)
- Blockchain analytics providers (AML compliance)
- Game aggregators (session & win/loss data)
- Payment processors (transaction confirmations)

Unauthorized sharing is strictly prohibited.

14.9 Confidentiality & Access Controls

To ensure confidentiality:

- Access to PII must be limited to minimal required personnel
- PII must not be visible to developers, external consultants, or game providers
- Viewing or exporting PII must be logged
- Admin access to PII requires MFA and special privileges
- Sensitive data must never be transported unencrypted

14.10 Regular Audits & Compliance Review

- Annual audit of data retention and destruction processes
- Quarterly review of data classification and access logs
- Vendor compliance audits verifying proper data handling
- Security team must review whether systems collect unnecessary data
- Policy updates must occur after system changes or regulatory updates

15. Staff Security Training

Weeekly ensures that all employees, contractors, and privileged users understand their security responsibilities and possess the necessary knowledge to protect platform integrity, player data, and financial systems.

Security training is mandatory at multiple stages of employment and is reinforced regularly to maintain high awareness.

These requirements apply to all staff involved in Weeekly, Weeekly Rivals, the casino, and any supporting systems.

15.1 Mandatory Onboarding Training

Every new employee or contractor must complete security training **before receiving access** to Weeekly systems.

Training Topics Include

- Overview of Weeekly's Information Security Policy
- Data protection rules (PII handling, confidentiality)
- Access control requirements
- Secure communication practices
- Use of MFA, password policies, and account rules
- Reporting suspicious activity or incidents
- Anti-fraud overview (relevant to gaming operations)
- AML red flags and escalation channels
- Prohibited practices (password sharing, storing keys, unauthorized exports)

Completion must be logged and verified by HR and the ISO.

15.2 Annual Refresher Training

All staff must complete annual security training to stay updated on:

- Policy changes
- Emerging cyber threats
- Updates in Curaçao regulatory requirements

- New internal procedures
- Changes to AML or KYC rules
- New gaming or wallet security risks

Refresher training is mandatory for all roles, including contractors and temporary staff.

15.3 Phishing & Social Engineering Awareness

Phishing poses a major threat to gaming and crypto environments. Weeekly enforces ongoing awareness and testing.

Phishing Training Must Cover

- Identifying malicious emails or messages
- Recognizing fake admin or wallet alerts
- Avoiding social engineering traps via email, SMS, or Telegram
- Reporting suspected phishing attempts

Monitoring & Testing

- Periodic simulated phishing campaigns
- Results reviewed by the ISO
- Mandatory follow-up for anyone who fails simulations

15.4 Secure Coding Training for Developers

Developers must receive advanced training related to secure engineering practices.

Topics Include

- OWASP Top 10 vulnerabilities
- SEI CERT coding standards
- Secure API design
- Safe handling of secrets and API keys
- Secure CI/CD usage
- Avoiding injection vulnerabilities
- Server vs. client-side security responsibilities
- RNG protection considerations
- Game fairness/integrity mechanics
- Wallet and blockchain integration security

Training must be completed during onboarding and refreshed annually.

15.5 Remote Work & Device Security Policies

Given Weeekly's global footprint and remote workforce, strict controls apply to remote environments.

Device Requirements

- Company-managed devices preferred
- If personal devices are approved:
 - Mandatory device encryption
 - Updated operating system

- Active endpoint protection
 - Screen lock enabled
- No public/shared computers allowed for administrative access

Network Requirements

- Remote staff must use:
 - Secure, private Wi-Fi
 - VPN enforced for admin/system access
- Public Wi-Fi is prohibited for:
 - Admin console access
 - Accessing internal systems
 - Handling player data

Physical Security

- Screen privacy filters required for sensitive work
- Devices must not be left unattended in public spaces
- Confidential conversations must not occur in public areas

15.6 Role-Based Training Requirements

Certain roles require specialized training.

For Customer Support

- Safe account recovery procedures
- Identity confirmation methods
- PII handling and masking
- Fraud detection basics

For Compliance/AML Teams

- Deep AML/CFT training
- Wallet risk scoring
- Suspicious activity handling
- Transaction monitoring tools
- Regulatory obligations under CGA

For Admin Users

- Privileged access best practices
- Logging and audit requirements
- Safe modification of backend systems

15.7 Policy Acknowledgement

All employees must formally acknowledge:

- Understanding the Information Security Policy
- Compliance with internal procedures

- Agreement to confidentiality obligations
- Awareness of consequences for violations

HR must maintain documentation for each acknowledgement.

15.8 Tracking & Reporting

To maintain accountability:

- All training completion records must be stored securely
- The ISO must review training participation quarterly
- Non-compliant staff must be flagged and followed up with
- Training materials must be updated annually

15.9 Consequences for Non-Compliance

Failure to comply with security training requirements may result in:

- Removal of system access
- Mandatory retraining
- Disciplinary action (up to termination, depending on severity)

16. Physical Security

Weeekly ensures that all physical locations supporting platform operations—including registered offices, employee work environments, third-party hosting facilities, and cloud data centre infrastructure—are protected against unauthorised access, environmental threats, and physical tampering.

Physical security complements logical controls, ensuring end-to-end protection of Weeekly systems and data.

16.1 Access Control Systems

Requirements

- Physical access to office areas containing sensitive equipment (servers, secure storage, backup media) must be restricted using:
 - Keycards
 - Biometric access
 - Physical locks
- Only authorized personnel may access restricted areas.
- Access rights must be:
 - Reviewed quarterly
 - Removed immediately upon offboarding
- Physical access logs must be retained for audit and incident investigation.

16.2 CCTV Monitoring

Where applicable, Weeekly or hosting providers must maintain surveillance controls:

- CCTV coverage of server rooms, entrances, and restricted areas
- 24/7 monitoring capability
- Retention of footage for at least **30–90 days**, depending on the provider

- Tamper-proof storage of recordings
- Access restricted to authorised staff only

Third-party data centers must provide CCTV coverage as part of their compliance certification.

16.3 Server Rack & Equipment Protection

Controls

- Server racks must be:
 - Locked
 - Bolted or secured to prevent removal
 - Located in temperature-controlled environments
- Sensitive hardware (firewalls, switches, storage devices) must be labeled and inventoried
- No unauthorized device may be connected to secure network racks

For cloud infrastructure, equivalent protections are enforced by the provider and validated through vendor due diligence.

16.4 Offsite Backup Security

Backups stored offsite must be protected from physical theft, damage, or tampering.

Requirements

- Offsite backups must be encrypted with AES-256

- Offsite storage must be located in:
 - A secure secondary region
 - A facility with controlled access and environmental protections
- Paper-based records (if any) must be locked in secure storage
- Transportation of backup media (if used) must follow a documented chain of custody
- Cloud backup providers must offer physical security compliant with industry standards

16.5 Environmental Protections

Hosting areas must include:

- Fire detection and suppression systems
- Power redundancy (UPS + generator backup)
- Flood protection where applicable

Cloud data centers satisfy these requirements through their own certified controls.

17. Change & Configuration Management

Weeekly maintains strict change and configuration management procedures to protect system stability, prevent unauthorized modifications, and maintain auditability across production systems.

These controls apply to infrastructure, application code, game engines, wallet systems, and administrative configurations.

17.1 Approval Process for Updates

All changes—code, infrastructure, configuration—must follow a documented approval workflow.

Requirements

- Change Request (CR) must be submitted describing:
 - Purpose
 - Impact
 - Risk level
 - Testing plan
- Approval required from:
 - Technical Lead
 - ISO (for sensitive changes)
 - Compliance Officer (if financial/AML related)
- High-risk changes must undergo peer review and formal management approval.

17.2 Version Control

All application and backend code must be maintained in a secure version control system.

Controls

- Mandatory use of Git repositories
- Branching strategies for development, staging, production

- Every change must be traceable to a user and ticket
- Sensitive files may not be stored in version control (API keys, passwords)
- Commit history must be retained indefinitely

17.3 Production Deployment Rules

Deployment Requirements

- Production deployments must:
 - Pass automated tests
 - Pass code reviews
 - Pass security scans (SAST/DAST)
 - Be approved by the Technical Lead
- No developer may deploy directly to production without authorization
- Deployments must be:
 - Logged
 - Monitored
 - Performed using CI/CD pipelines with MFA
- Production environment must not allow ad-hoc manual code changes

17.4 Emergency Change Procedures

In emergencies (critical bug, outage, security threat):

- Emergency Change Request (ECR) may be submitted
- ISO and CTO must approve expedited deployment
- Monitoring must verify system stability post-deployment
- Full documentation must be completed **retroactively** within 24 hours
- Emergency changes are subject to post-implementation review

17.5 Configuration Management

Systems and applications must maintain standardized, secure configurations.

- Baseline configurations must be documented and stored in secure repositories
- Unauthorized configuration changes are prohibited
- Configuration changes must be tracked through version control
- Sensitive components (firewalls, WAF, servers, wallet integrations) must follow a strict approval path
- Drift detection tools should monitor for unauthorized changes

17.6 Rollback Strategy

To protect against failed deployments or unstable changes:

Rollback Requirements

- Every deployment must have:
 - A defined rollback plan

- A previous stable version ready
 - Automated or manual rollback capability
- Rollbacks must:
 - Be executed if health checks fail
 - Be logged
 - Trigger a root cause analysis

Systems must return to a stable state with minimal downtime.

18. Policy Governance & Review

Weeekly's Information Security Policy must be maintained as a living document, reviewed regularly, and approved by senior leadership to ensure ongoing compliance with operational and regulatory requirements.

18.1 Annual Review

- The policy must be reviewed **at least once per year**
- Review includes:
 - Updating sections reflecting new threats
 - Including new regulatory changes
 - Updating vendor or technology changes
 - Incorporating lessons learned from incident reviews

Policy revisions must be documented with version history.

18.2 Review After Major Incidents

In addition to annual review, immediate review is required after:

- Security breaches
- Major outages
- Wallet or transaction anomalies
- Fraud events
- Audit findings
- Infrastructure migrations

The review must analyze whether existing controls were adequate and update them accordingly.

18.3 Policy Approval by Senior Management

- The Information Security Policy must be approved by:
 - CEO or Managing Director
 - CTO or Technical Director
 - ISO (Information Security Officer)
- Approval must be documented and recorded
- Only authorized executives may approve changes or exceptions

This ensures accountability and governance oversight.

18.4 Documentation Control & Versioning

All versions of the Information Security Policy must be:

- Version-controlled
- Time-stamped
- Stored securely
- Archived for a minimum of **5 years**
- Distributed only through secure internal channels

Change logs must include:

- Author
- Approver
- Summary of changes
- Date of revision

18.5 Accessibility

- The latest approved version must be accessible to all staff
- Sensitive appendices (e.g., wallet procedures) may have restricted access
- All employees must be notified of major changes