

Information Security Policy

1. Purpose

This Information Security Policy ("**Policy**") sets out the commitment of Get Zapped Gaming N.V. (the "**Company**", "**we**", "**our**") to protect the confidentiality, integrity and availability of all information assets, including player data, transaction records, and gaming system outputs, in accordance with the requirements of the CGA and the LOK. We recognise that robust information security is essential to maintain operational resilience, protect players and stakeholders, uphold game fairness, and preserve our reputation.

2. Scope

This Policy applies to all employees, directors, officers, contractors, third-party service providers and other persons authorised to access or process the Company's information and systems. It covers all information assets, including but not limited to:

- player accounts, balances, stakes, wins and losses;
- financial transaction records (deposits/withdrawals);
- gaming software (own or third-party supplied);
- infrastructure (servers, databases, networks, applications);
- business-critical logs and audit trails;
- communications and backups;
- physical assets and premises used for data processing.

3. Governance & Responsibilities

- The Board of Directors has ultimate responsibility for information security.
- We will hire a Chief Information Security Officer (CISO) (or equivalent) who will be responsible for implementation, maintenance, monitoring and reporting of this Policy.
- All managers shall be responsible for ensuring their staff and contractors comply with the Policy.
- All employees, contractors and third-party providers must comply with this Policy, relevant procedures, and cooperate in audits and incident investigation.

4. Risk Management & Asset Classification

- We maintain an inventory of all information assets (hardware, software, data, network components) and classify them according to confidentiality, integrity and availability requirements.
- A formal risk assessment is performed at least annually and when significant changes occur (new services, suppliers, geographies).
- Controls are selected and implemented to reduce information security risks to a level acceptable to the Board.

5. Access Control

- Access to systems and data is granted on a "least-privilege" and "need-to-know" basis.

- Unique user identities shall be used; shared accounts are minimised and only permitted when formally approved and logged.
- Strong authentication (passwords, two-factor authentication where appropriate) is required.
- Access rights are reviewed at least quarterly and immediately upon role change or termination.
- Third-party providers must have access controls at least equivalent to ours, and their access shall be contractually controlled and monitored.

6. Infrastructure, Network & System Security

- All network components are configured to deny all traffic by default, then allow necessary services only.
- Firewalls, intrusion detection/prevention systems, network segmentation, anti-malware and log-monitoring systems shall be deployed.
- We will use secure AWS hosting servers (including databases) for hosting critical player or financial data.
- Regular vulnerability scanning and penetration testing shall be conducted (at minimum annually and after major changes).
- Patch management: critical patches will be applied within a defined timeframe, non-critical patches within a reasonable timeframe.
- All communications between components (client-to-server, server-to-server) will use encryption (TLS or stronger) for confidentiality and integrity.

7. Data Protection & Encryption

- Personal data of players and transaction data shall be processed and stored in accordance with applicable data-protection laws.
- Sensitive data such as authentication credentials, payment card data, personal identifiers and transaction logs shall be encrypted at rest and in transit.
- Backup data and archive media shall be encrypted and stored in a secure cloud with appropriate access controls.
- Data retention and deletion policies are in place: logs and records are retained for a period of 5 years as required by law/regulation and securely deleted when no longer required.

8. Change Management & Software Testing

- All changes to critical systems (gaming platforms, account systems, payment modules) shall follow a formal change-management process: planning, risk assessment, testing (including regression), approval, rollback planning, implementation and post-implementation review.
- After changes, relevant security controls must be verified, logs reviewed, and any anomalies addressed.

9. Incident Management & Reporting

- We maintain an incident-response plan which defines roles, responsibilities, escalation paths, communication (internal and external), forensics and remediation. Incidents shall be classified (e.g., data breach, intrusion, denial-of-service, fraud, system integrity compromise).

- The CGA will be notified within 24 hours of an incident once confirmed.
- Affected systems must be contained, root cause analysed, corrective and preventive actions implemented, and lessons learned documented.
- Incident records shall be maintained for audit, regulatory review and legal compliance.

10. Business Continuity & Disaster Recovery

- A business-continuity plan and disaster-recovery plan must be in place, documented and tested at least annually.
- Critical services (player account services, deposits/withdrawals, gaming operations) will have defined recovery-time objectives (RTO) and recovery-point objectives (RPO).
- Backups shall be performed regularly, stored securely off-site (or in a redundant region) and disaster-recovery rehearsals shall be conducted.

11. Supplier & Third-Party Risk Management

- Third-party service providers (hosting, payment processors, game suppliers, software vendors) shall be assessed for information-security risk before onboarding, and contractually bound to comply with security and confidentiality obligations.
- We maintain an inventory of third-party providers and their risk classification.
- Third-party performance (including incident reporting, audit rights, security controls) shall be monitored periodically.

12. Monitoring, Logging & Audit

- Logging: all access to critical systems, admin activities, game engine events, financial transactions and security events shall be logged and retained per policy.
- Logs must be protected from unauthorised modification and available for review.
- Regular audits (internal and external) shall be conducted to verify compliance with this Policy and other relevant policies.
- Audit results and findings shall be reported to senior management and remediated within defined timeframes.

13. Training & Awareness

- All employees, contractors and relevant third-parties must receive information-security awareness training upon hire and at least annually, plus additional training when security risks materially change.
- Training content covers data protection, phishing, social engineering, password hygiene, incident reporting, and role-specific security procedures.

14. Policy Review & Revision

- This Policy shall be reviewed at least annually, or whenever significant changes occur (e.g., legal/regulatory change, organisational restructure, major incident).
- Management must approve any revisions, and employees/contractors must be made aware of updated versions.

15. Enforcement & Non-compliance

- Non-compliance with this Policy may lead to disciplinary action and may expose the Company to regulatory enforcement by the CGA.
- We will co-operate fully with CGA investigations and provide required documentation, audit reports and independent expert evaluations when requested.