

1. Policy Purpose and Scope

This policy ensures that U8 Group B.V. protects all digital assets, player data, and operational systems from unauthorized

2. Data Security & Access Control

- All sensitive data is encrypted in transit and at rest using industry standards (e.g., AES-256).
- Role-based access controls (RBAC) are enforced for systems and databases.
- Two-factor authentication (2FA) is mandatory for admin logins.

3. Infrastructure Protection

- Servers are hosted in ISO 27001-certified data centers with 24/7 monitoring.
- Firewalls, DDoS protection, and IDS/IPS systems are in place.
- Regular vulnerability scans and security patches are applied.

4. Employee Responsibilities

- All employees must sign an IT and confidentiality agreement.
- Employees receive quarterly training on phishing, malware, and data handling.
- Immediate reporting of security incidents is mandatory.

5. Third-Party Vendors

- All third-party providers (e.g., game studios, payment processors) must sign a data protection agreement.
- Vendors are evaluated annually for security compliance.

6. Business Continuity & Disaster Recovery

- Data backups are performed daily and stored in geographically redundant locations.
- A formal disaster recovery plan (DRP) is reviewed semi-annually.
- Simulated recovery drills are conducted annually.

7. Audits & Compliance

- Internal audits are conducted twice a year to review system logs and access patterns.
- Policies are reviewed and updated annually or upon material changes in regulations.