

Information Security Policy

Version 1.0 — WoT N.V.

Effective Date: October, 2025

1. Purpose and Scope

This Information Security Policy (“Policy”) defines the principles and minimum controls that WoT N.V. applies to protect information assets, IT systems and services supporting its online gaming operations.

The Policy applies to all employees, contractors and third parties who access WoT N.V. information or systems.

2. Compliance Statement

WoT N.V. is committed to safeguarding data in line with generally accepted information-security practices (including ISO/IEC 27001 control objectives) and applicable legal requirements. This Policy forms part of the internal control framework submitted under the CGA checklist.

3. Roles and Responsibilities

- **Management:** approves this Policy, provides resources and ensures enforcement.
- **Information Security Lead (ISL):** coordinates risk mitigation, access controls, incident handling and policy reviews.
- **IT Administrators:** implement technical safeguards, backups, monitoring and patching.
- **All Users:** follow this Policy, use strong passwords and report incidents without delay.

4. Access Control and Data Protection

4.1 Access is granted on a least-privilege and need-to-know basis; accounts are individual and not shared.

4.2 Strong authentication is required for privileged access; passwords comply with complexity and rotation requirements.

4.3 Data at rest and in transit is protected with industry-standard encryption where feasible.

4.4 Personal data is processed only for legitimate purposes and retained no longer than necessary.

4.5 Third-party access is governed by contracts and technical restrictions (segregated credentials, IP allow-lists).

5. Network and System Security

5.1 Production services are segregated from test environments; inbound access is restricted by firewalls/security groups.

5.2 Servers and applications are kept up to date; critical security patches are applied without

undue delay.

5.3 Anti-malware/EDR is used on endpoints where practical; security-relevant logs are retained for forensic purposes.

5.4 Changes to production follow change-management (peer review, approval, rollback plans).

6. Backup and Recovery

6.1 Critical databases and configuration repositories are backed up at regular intervals (daily minimum for production).

6.2 Backups are encrypted and stored separately from production; restore tests are performed at least quarterly.

6.3 Recovery objectives: **RPO ≤ 24h** for core gaming data; **RTO ≤ 24h** for core services where feasible.

7. Incident Management

7.1 All suspected or actual security incidents must be reported to the ISL immediately via the designated channel.

7.2 Incidents are triaged, contained, eradicated and reviewed; evidence is preserved where relevant.

7.3 Notifiable events (e.g., data breaches) are assessed for regulatory notification and customer communication.

8. Physical Security

8.1 Production infrastructure is hosted at professional data centres or cloud providers with access controls and CCTV.

8.2 Access to offices/rooms with equipment is restricted and logged where applicable.

9. Policy Maintenance and Review

This Policy is reviewed at least annually or upon material changes to systems, risks or regulatory requirements.