

INFORMATION TECHNOLOGY POLICY

Magic365.com

1. Purpose and Scope

This Information Technology Policy (hereinafter referred to as the "Policy") establishes the technical and organizational controls implemented by Magic Stones N.V., operator of <https://magic365.com>, to guarantee the confidentiality, integrity, and availability of information systems and data. The Policy applies to all assets, including hardware, software, databases, communications infrastructure, third-party integrations, and user-facing applications. It is binding on all employees, contractors, vendors, and service providers operating within or integrating with the IT environment.

The Policy is based on regulatory obligations under the National Ordinance on Games of Chance (LOK), guidance issued by the Curaçao Gaming Authority (CGA), and incorporates provisions of the General Data Protection Regulation (GDPR), European Accessibility Act (EAA), and, voluntarily, industry standards such as ISO/IEC 27001, 27002, 27701, and NIST SP 800-53. Where applicable, provisions of the Digital Services Act (DSA) are applied as benchmarks.

2. Access Control and Identity Management

Magic365.com maintains centralized identity and access management (IAM) processes. All access to critical systems is governed by role-based access control (RBAC), with multi-factor authentication (MFA), session timeout, IP-based restriction, and logging. User lifecycle management (Joiner, Mover, Leaver) procedures are in place, including access provisioning, privilege audits, and account deactivation.

Prior to being granted access, users undergo mandatory cybersecurity awareness training, background screening, and execute binding confidentiality and data protection agreements. Access to player data or financial systems is restricted to a need-to-know basis, monitored via audit trails and regularly reviewed.

3. Infrastructure and System Security

The infrastructure is hosted in certified Tier III+ data centers with geographically redundant paths, redundant power supply, and disaster recovery capabilities. Systems are protected by next-generation firewalls, intrusion prevention and detection systems (IPS/IDS), endpoint detection and response (EDR), and network segmentation.

Security controls include vulnerability scanning, anti-malware, DDoS mitigation, and application-layer security (WAF, RASP). Secure development lifecycle (SDLC) practices are enforced through static and dynamic code analysis, patch management, and OWASP Top 10 compliance.

4. Logging, Monitoring, and Security Oversight

Comprehensive and immutable logging is enforced for system events, user authentication, data access, administrative actions, and configuration changes. Logs are digitally signed, stored in secure write-once repositories for a minimum of five (5) years, and accessible for forensic reconstruction.

A SIEM platform aggregates log data and issues real-time alerts for anomalies, threat indicators, and violations of security policy. Monitoring includes automated behavioral analysis and correlation rules aligned with MITRE ATT&CK and NIST frameworks. Internal audits are conducted quarterly, and independent security audits are performed annually.

5. Business Continuity and Disaster Recovery

Magic365.com maintains a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), covering all mission-critical services. The Recovery Time Objective (RTO) does not exceed four (4) hours, and Recovery Point Objective (RPO) is fifteen (15) minutes for priority systems.

Backups are encrypted and stored in geo-diverse locations, subject to monthly restore tests. A crisis communication plan is established, with accessibility measures in place to ensure continuity of service for users with disabilities under EAA standards.

6. Software Lifecycle and Patch Management

All updates to production systems are subject to change control processes, including peer review, QA validation, regression testing, and staging. Software vulnerabilities are managed using a dedicated ticketing system, prioritizing remediation based on CVSS scores and criticality.

CI/CD pipelines are secured, incorporating automated tests, rollback logic, and full traceability. Critical vulnerabilities are patched within 48 hours, with documentation maintained for all deployments and hotfixes.

7. Regulatory and Legal Compliance

Magic365.com complies with GDPR requirements, including records of processing activities (ROPA), data minimization, consent management, DPIAs, and user rights. The platform voluntarily implements controls aligned with ISO/IEC 27001, 27002, 27701, and NIST SP 800-53.

Oversight of third-party technology providers and data processors is ensured via due diligence, contractual clauses, and service level agreements. The EAA is implemented through WCAG 2.1 AA-compliant interfaces.

8. Protection Against External Threats

Traffic is monitored 24/7 using behavior analytics, bot detection, WAF, and country/IP-based filtering. Threat intelligence feeds and anomaly patterns inform

blacklisting and response automation. Remote admin access requires VPN, hardware tokens, and temporal access controls.

Penetration tests, red team simulations, and threat modeling exercises are performed semi-annually. All third-party libraries are vetted for supply chain risks, and software composition analysis is applied in development.

9. Data Subject Rights and Accessibility

Magic365.com provides a centralized platform for data subject rights (DSR) requests in line with GDPR Articles 12–23, including access, erasure, portability, and consent withdrawal. The Data Protection Officer (DPO) oversees processing timelines and registry of all requests.

Accessibility testing is conducted on each interface release, ensuring compatibility with assistive technologies, screen readers, keyboard navigation, and alternative CAPTCHA solutions.

10. Accountability and Governance

The CTO, jointly with the CISO and DPO, is responsible for oversight of this Policy's implementation, including enforcement, internal investigations, and training. Violations are subject to disciplinary action and, if relevant, notifications to CGA or EU data protection authorities.

Policy compliance is monitored through periodic review, audit findings, and lessons learned from incidents. Breaches of this Policy may result in suspension of access privileges, contract termination, or legal action.

This Policy is reviewed annually or in response to material changes in the regulatory, operational, or technological environment.

Approved by the Management Board of Magic Stones N.V.

Effective Date: 16.06.2025



By: Vivian Ersilia o.b.o (SMES) Solutions for Management and Employment Support N.V.

Managing Director

Date: 09.07.2025