

INFORMATION SECURITY POLICY

Breakout Group B.V.

Version: 1.0

Effective Date: September 26, 2025

A handwritten signature in blue ink, consisting of a stylized 'W' or similar character.

1. Introduction and Definitions

1.1. It is the official policy of Breakout Group B.V. ("the Company") to ensure a secure, lawful, transparent, and responsible use of the Internet, corporate information technology infrastructure, digital assets, and personal information. This Information Security and Privacy Policy ("the Policy") establishes the fundamental principles, detailed rules, and binding procedures governing the collection, processing, storage, use, and protection of information by the Company and its affiliates, subsidiaries, contractors, consultants, vendors, and service providers.

1.2. For the purposes of this Policy:

1.2.1. Odds96 shall mean the online gaming and betting platform operated by Breakout Group B.V., available at <https://odds96.com>, including, without limitation, all related websites, subdomains, mobile applications, servers, databases, hosting environments, and any other systems or digital services controlled or managed by the Company.

1.2.2. Policy shall mean this Information Security and Privacy Policy of Breakout Group B.V., as amended, updated, or restated from time to time and formally approved by the Company's Executive Management.

1.2.3. Website shall mean the official website of Odds96, as well as any affiliated domains, portals, or web-based applications operated, owned, or lawfully controlled by Breakout Group B.V.

1.3. By accessing or using Odds96, you expressly confirm that you have carefully read, fully understood, and voluntarily agreed to this Policy and that you consent to the lawful collection, secure processing, authorized use, and controlled disclosure of your personal and non-personal information strictly in accordance with the terms and provisions set out herein. If you do not agree with any of the terms of this Policy, you must immediately refrain from using Odds96, the Website, or providing your personal information.

2. Purpose

2.1. The purpose of this Policy is to ensure a secure, responsible, and compliant use of the Internet, corporate IT systems, network infrastructure, and all other digital assets by employees, officers, executives, consultants, contractors, and service providers of Breakout Group B.V.

2.2. The objectives of this Policy include, but are not limited to:

2.2.1. Protecting the confidentiality, integrity, and availability of all Company Assets and information resources.

2.2.2. Preventing unauthorized access, misuse, manipulation, loss, destruction, alteration, or exfiltration of Company information and digital resources.

2.2.3. Ensuring compliance with all applicable international, regional, and national laws, regulations, and contractual obligations, including those relating to personal data protection, gaming regulation, telecommunications, cybersecurity, and



intellectual property rights.

2.2.4. Establishing clear responsibilities, obligations, and accountability mechanisms for all individuals acting for or on behalf of the Company.

2.2.5. Reinforcing trust among users, clients, regulators, and stakeholders by demonstrating a proactive and effective approach to information security and privacy.

3. Scope

3.1. This Policy governs the use of and access to the following:

- (a) Internet access, mobile internet, telecommunications, and related services provided by or on behalf of the Company;
- (b) Internal corporate IT systems, networks, servers, databases, and cloud environments;
- (c) End-user devices, including company-owned equipment and approved personal devices used for business purposes;
- (d) Platforms, applications, servers, and systems developed, owned, hosted, or lawfully managed by the Company;
- (e) All digital assets, electronic records, and information resources belonging to or under the control of the Company.

3.2. This Policy applies to all employees, officers, members of executive management, directors, temporary staff, interns, affiliates, contractors, consultants, vendors, suppliers, third-party service providers, and any other individual or legal entity acting for, on behalf of, or in partnership with Breakout Group B.V.

4. Definitions

4.1. "Company Assets" means all information, records, intellectual property, software, hardware, systems, networks, devices, applications, and data, regardless of form or medium, that are owned, licensed, or managed by Breakout Group B.V.

4.2. "Device" means any endpoint, including but not limited to desktop computers, laptop computers, mobile phones, tablets, removable media, or virtualized environments, used to access, process, or store Company Assets.

4.3. "Personal Data" has the meaning given in Section 3 of this Policy and includes any data subject to the European Union General Data Protection Regulation (GDPR), the United Kingdom General Data Protection Regulation (UK GDPR), and any other applicable data protection legislation.

4.4. "Remote Access" means any access to Company Assets conducted over external networks or the public Internet, using Company-approved methods and security mechanisms, including but not limited to Virtual Private Networks (VPN) with enforced Multi-Factor Authentication (MFA).

4.5. "Security Incident" means any event, occurrence, or suspected activity that compromises, threatens to compromise, or is reasonably likely to compromise the confidentiality, integrity, or availability of Company Assets or Personal Data. This

includes but is not limited to data breaches, malware infections, unauthorized access attempts, theft of devices, or suspected insider threats.

5. Roles and Responsibilities

5.1. Employees and Contractors must:

- 5.1.1. Comply with this Policy and all supporting standards and guidelines.
- 5.1.2. Complete mandatory information security and data privacy training as required.
- 5.1.3. Promptly and accurately report any suspected or actual Security Incidents through designated reporting channels.

5.2. Managers must:

- 5.2.1. Ensure that all team members under their supervision understand and adhere to the provisions of this Policy.
- 5.2.2. Regularly review and update access rights to ensure they accurately reflect current job responsibilities.

5.3. The IT and Security Department is responsible for:

- 5.3.1. Provisioning, managing, and revoking access rights in line with the principle of least privilege.
- 5.3.2. Monitoring systems for suspicious or unauthorized activity.
- 5.3.3. Investigating, containing, remediating, and documenting Security Incidents.
- 5.3.4. Maintaining, updating, and enforcing supporting standards and procedures, including but not limited to password management, data loss prevention, and remote work security.

5.4. Vendors and Service Providers must:

- 5.4.1. Fully comply with the Company's security and privacy requirements.
- 5.4.2. Enter into binding agreements that include confidentiality, data processing, and security obligations.
- 5.4.3. Use access to Company Assets strictly for the purposes of performing the contracted services.

6. Acceptable Use

6.1. Company Assets shall be used exclusively for legitimate business purposes.

Limited personal use is tolerated only where such use:

- 6.1.1. does not interfere with an employee's work responsibilities;
- 6.1.2. does not consume excessive system or network resources;
- 6.1.3. does not violate this Policy, applicable law, or any contractual obligations of the Company.

6.2. Users must not install, configure, or operate any unauthorized hardware, software, cloud services, or collaboration tools for the storage, processing, or transmission of Company data.

6.3. All users must:

- 6.3.1. protect their login credentials;

- 6.3.2. use strong, complex passwords in compliance with Company standards;
- 6.3.3. enable multi-factor authentication (MFA) wherever available;
- 6.3.4. lock or log off devices whenever left unattended.

7. Restricted and Prohibited Use

7.1. Prohibited activities include, but are not limited to:

- (a) attempting unauthorized access to systems, networks, or data;
- (b) deliberate or negligent exfiltration of Company data;
- (c) distribution, creation, or introduction of malware, ransomware, or malicious code;
- (d) disabling, bypassing, or tampering with security controls, firewalls, antivirus systems, or monitoring tools;
- (e) infringement of intellectual property rights, including but not limited to use of pirated software;
- (f) dissemination of offensive, discriminatory, harassing, or abusive content;
- (g) unauthorized operation of servers, wireless hotspots, or peer-to-peer/file-sharing services;
- (h) storing Company data on unapproved personal devices, personal cloud accounts, or removable media without encryption and written approval;
- (i) uploading or transmitting Company data into generative artificial intelligence tools without prior documented authorization and adequate safeguards;
- (j) excessive non-business activities (including gaming, streaming, or downloading) that degrade system or network performance;
- (k) sharing account logins or using shared or generic accounts without express authorization.

7.2. Users must not attempt to circumvent content filters, VPN enforcement, data loss prevention mechanisms, or endpoint protection systems.

8. Access Management and Authentication

8.1. Access to Company Assets shall follow the principle of least privilege and role-based access control (RBAC).

8.2. All access requests must be formally approved by a line manager and verified by the IT/Security Department.

8.3. Access rights must be reviewed periodically and revoked immediately upon employee transfer, termination, or completion of contractual work.

8.4. Authentication requirements:

8.4.1. passwords must contain at least 12 characters and include complexity requirements (uppercase, lowercase, numbers, special symbols);

8.4.2. MFA must be enforced for remote access, administrative accounts, and all critical applications;

8.4.3. generic or shared accounts are to be avoided. If their use is strictly necessary, they must be subject to strict access control, detailed logging, and periodic review.

9. Monitoring and Logging

9.1. The Company reserves the right to monitor, log, and review:

- (a) network traffic;
- (b) web browsing activity;
- (c) use of email and collaboration tools;
- (d) endpoint security telemetry;
- (e) access to Company systems and applications.

9.2. Such monitoring is conducted exclusively for legitimate business purposes, including security, compliance, performance, and fraud prevention.

9.3. Users shall have no expectation of personal privacy when using Company Assets, subject always to applicable laws and regulations.

9.4. Security and audit logs must be retained in accordance with the Company's retention schedule and may be used for investigations, audits, and compliance reporting.

10. Data Protection and Physical Security

10.1. All processing of personal data must comply with applicable data protection legislation, including GDPR and UK GDPR.

10.2. Data classification levels shall be applied as follows: Public, Internal, Confidential, and Restricted. Confidential and Restricted data must always be encrypted both in transit and at rest, using Company-approved encryption algorithms and key management systems.

10.3. Sensitive data shall not be transmitted via unencrypted email. Approved safeguards such as TLS encryption, password-protected archives, or secure file transfer protocols must be used.

10.4. Physical security controls include:

- 10.4.1. maintaining a clean-desk policy;
- 10.4.2. locking computer screens when unattended;
- 10.4.3. securing laptops and devices with cable locks where possible;
- 10.4.4. storing removable media in locked cabinets;
- 10.4.5. immediately reporting lost, stolen, or compromised devices.

11. Remote Access and BYOD

11.1. Remote access is permitted only through Company-approved VPNs with MFA.

11.2. Split tunneling and insecure VPN configurations are strictly prohibited.

11.3. Personally owned devices used for Company business must comply with the following baseline controls:

- (a) full disk encryption;
- (b) enforced automatic operating system and application updates;
- (c) password or biometric device lock;

- (d) updated anti-malware protection;
 - (e) enrollment in Company-managed Mobile Device Management (MDM) if required.
- 11.4. Company data must never be stored permanently on unmanaged devices. Access shall occur through secure virtual desktops or approved secure applications.
- 11.5. Use of public or shared computers for work purposes is strictly prohibited.
- 11.6. Public Wi-Fi connections must always be secured with VPN. Sensitive transactions should not be conducted over insecure or untrusted networks.

12. Third-Party and Vendor Access

- 12.1. All third parties requiring access to Company Assets must enter into written agreements that specifically address confidentiality, data protection, and information security obligations.
- 12.2. Vendor access must be:
- (a) limited in scope and time-bound;
 - (b) subject to the principle of least privilege;
 - (c) monitored and logged at all times.
- 12.3. Vendor accounts must be deactivated immediately once access is no longer required.

13. Incident Reporting and Response

- 13.1. All employees, contractors, and third parties must report any suspected or actual Security Incident immediately, without undue delay, to the IT/Security Department through designated channels, including the internal service desk or by email at support@odds96.com.
- 13.2. Reportable incidents include, but are not limited to: suspected phishing attempts, lost or stolen devices, unauthorized access attempts, malware infections, or any unusual system behavior.
- 13.3. Users must preserve evidence by refraining from deleting, altering, or tampering with data or logs related to the incident.
- 13.4. Users must not communicate externally about the incident unless specifically authorized in writing by the Company.
- 13.5. The Company shall:
- (a) promptly investigate and contain the incident;
 - (b) implement appropriate remediation measures;
 - (c) notify affected stakeholders or regulatory authorities when required by applicable law;
 - (d) document all incidents for audit and compliance purposes.

14. Regulatory Compliance

- 14.1. All users must comply with applicable international, regional, and national laws, regulations, and regulatory guidelines, including but not limited to:

- (a) the General Data Protection Regulation (EU) 2016/679 (GDPR);
- (b) the United Kingdom General Data Protection Regulation (UK GDPR);
- (c) applicable telecommunications, e-privacy, and cybersecurity regulations;
- (d) contractual obligations with regulators, gaming authorities, and commercial partners.

14.2. The Company aligns its internal controls and security practices with recognized industry standards and frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, and CIS Controls, where appropriate.

14.3. Alignment with such frameworks does not imply or represent formal certification unless explicitly and publicly stated by the Company.

15. Enforcement and Disciplinary Action

15.1. Any violation of this Policy may result in disciplinary measures up to and including termination of employment or contractual engagement.

15.2. In addition, violators may face civil liability and/or criminal prosecution, subject to applicable law.

15.3. Misuse of Company Assets that results in harm to clients, partners, regulators, or the Company itself may result in the responsible party being held liable for damages and financial losses.

16. Exceptions and Waivers

16.1. Exceptions to this Policy are permitted only under exceptional circumstances and must:

- (a) be documented in writing;
- (b) be time-bound;
- (c) be risk-assessed;
- (d) receive prior approval from the IT/Security Department and the relevant Executive Sponsor.

17. Training and Acknowledgement

17.1. All employees, contractors, and relevant third parties must complete information security and acceptable use training during onboarding and annually thereafter.

17.2. Each individual must formally acknowledge their understanding of and agreement to comply with this Policy as a condition of access to Company Assets.

18. Policy Governance

18.1. Policy Owner: Head of IT/Security or an appointed delegate.

18.2. Policy Approver: Executive Management of Breakout Group B.V.

18.3. Review Cycle: This Policy shall be reviewed at least annually, or more frequently where required due to material changes in law, regulation, organizational structure, risk profile, or technology.

18.4. Effective Date: September 26, 2025.

Appendix A – Quick Acceptable Use Rules (Non-Exhaustive)

A.1. Use Company systems primarily for business purposes. Limited personal use is permitted only if it does not interfere with work responsibilities.

A.2. Do not share passwords or store them in plain text. Enable multi-factor authentication (MFA) wherever possible.

A.3. Do not install unauthorized software or use unapproved cloud services for Company data.

A.4. Report any suspicious emails, links, or unusual system behavior immediately to IT/Security.

A.5. Lock your screen whenever leaving your workstation and ensure devices remain physically secure.

A.6. Always use the Company-approved VPN when working remotely. Do not use public or shared devices for Company work.

A.7. Treat all client and Company data as Confidential unless it has been explicitly classified as Public.

Approved by: eMagnus Curacao B.V.

Managing Director

Breakout Group B.V.

26.09.2025

