

Information Security Policy

1. Objective

Our objective is to protect client data, ensure the fairness of games, prevent fraudulent activity, and guarantee the confidentiality, integrity, and availability of all our systems and services.

2. Governance & Compliance

RedStar fully complies with all applicable data protection, Anti-Money Laundering (AML), and Know Your Customer (KYC) regulations. We operate under license number OGL/2024/168/0127 issued by the Curaçao Gaming Authority. All personal data is securely stored in monitored environments with no unauthorized third-party access.

3. Data Protection & Privacy

We collect personal data - including name, date of birth, address, identification documents, and payment details - for legitimate purposes such as account verification and transaction processing. Data is processed in accordance with the General Data Protection Regulation (GDPR) and other relevant laws.

We retain user information for a minimum of five years following the termination of an account or the last contact. For self-excluded users, the retention period is seven years. Players have full rights under GDPR to access, correct, delete, or transfer their personal information, and to file complaints with relevant authorities.

4. Access Control & Authentication

RedStar requires all users to maintain unique login credentials. Anonymous and pseudonymous accounts are not permitted. We enforce a multi-step identity verification process to comply with AML and KYC standards and to protect account security.

5. Data Transmission & Encryption

We encrypt all communications between clients and our servers using industry-standard protocols such as SSL/TLS. This ensures that player data, including sensitive gameplay information and financial transactions, is fully protected from interception or tampering.

6. Game Integrity & Fairness

We ensure fairness using a Random Number Generator (RNG) that is independently tested and certified by leading laboratories (e.g., GLI). Our automated and manual systems monitor gameplay to detect collusion, unfair patterns, or the use of prohibited software, including bots.

Any violation of game integrity policies leads to immediate investigation and potential account suspension or permanent ban.

7. Monitoring, Auditing & Incident Response

Our systems are continuously monitored through real-time alerts, log audits, and security scanning. In the event of suspected fraudulent behaviour, our dedicated Security Team initiates immediate investigations. We also implement defences against common attacks such as packet sniffing and man-in-the-middle exploits.

8. Payment Security & Financial Controls

Player funds are held in segregated accounts to ensure they remain protected and separate from operational funds. We partner with licensed third-party payment processors and conduct additional identity verifications for large transactions to ensure compliance and security.

9. Infrastructure Security

We design our infrastructure with security in mind, partnering with trusted software providers such as Playtech and BetConstruct. Our systems are protected by firewalls, anti-malware defences, regular patching, and network segmentation.

10. Third-Party & Vendor Management

All third-party service providers and affiliates working with RedStar are subject to strict data security and confidentiality requirements. We limit their access to only the data necessary for them to perform their duties under contract.

11. Cookie & Web Tracking

We use session cookies to maintain user logins and analytics cookies (e.g., Google Analytics) to improve site functionality. All cookie usage complies with privacy regulations, and users are given the option to manage their preferences.

12. User Communication Framework

We keep our users informed about security and privacy updates through periodic policy revisions and announcements. Users may contact our support team at support@redstarpoker.com to raise questions or concerns about data handling and information security.

13. Training & Awareness

Our team receives regular training on best practices for data protection, incident response, fraud prevention, and regulatory compliance. Security awareness is embedded into our organizational culture.

14. Continuous Improvement

We conduct annual penetration tests and engage third-party auditors to assess our systems. Our policies are reviewed in response to evolving threats, internal audits, and changes in legal requirements. We adopt a zero-tolerance stance toward any behaviour that undermines the integrity or security of our platform.

15. Enforcement & Accountability

We act swiftly in response to any security violations, including user misconduct such as the use of bots, collusion, or fraudulent activity. Offending accounts may be suspended or permanently banned. Internally, all RedStar employees and contractors are held accountable to our information security standards.

At RedStar, we prioritize security at every level - from infrastructure to gameplay. Our comprehensive security framework ensures encrypted communications, strict identity verification, fair play, and full regulatory compliance. We remain dedicated to providing a secure and trustworthy environment for our players.