



TRUSTDICE INFORMATION SECURITY POLICY

1. Purpose

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of TRUSTDICE's information assets, including sensitive data related to all kinds of transactions, player accounts, and other operational data. This policy aims to safeguard both customer and organizational data against unauthorized access, breaches, and loss.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and users who access or interact with the online casino platform. It covers all systems, processes, and data related to daily operations.

3. Information Security Objectives

- 1) Ensure the confidentiality of customer and transaction data.
- 2) Maintain the integrity and accuracy of all user, financial, and operational records.
- 3) Protect information from unauthorized access, disclosure, alteration, and destruction.
- 4) Ensure business continuity and minimize downtime in case of a security incident.
- 5) Comply with relevant industry regulations, such as GDPR, AML (Anti-Money Laundering), and KYC (Know Your Customer) requirements.

4. Data Protection Measures

- 1) **Encryption:** All sensitive data, including personal information and financial transactions, will be encrypted both at rest and in transit using industry-standard encryption protocols.
- 2) **Access Control:** Access to critical systems and data is granted based on the principle of least privilege. Multi-factor authentication (MFA) is mandatory for all employees and users accessing sensitive information.
- 3) **Regular Audits:** Regular internal and external security audits will be conducted to identify vulnerabilities and ensure compliance with the policy.
- 4) **Data Retention and Disposal:** Data will be retained only for as long as necessary to fulfill business, legal, or regulatory requirements. When no longer needed, data will be securely destroyed using approved methods.

5. Operational Security

- 1) **Network Security:** Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) will be used to protect the network from unauthorized access and attacks.
- 2) **Incident Response:** A defined incident response plan is in place to quickly respond to and mitigate any security breaches or data leaks. Employees will be trained to recognize potential security threats, including phishing attacks and social engineering.
- 3) **Third-Party Risk Management:** Third-party vendors, including payment processors and cryptocurrency exchange services, will be subject to rigorous security assessments to ensure that their practices align with this policy.

6. User Privacy and Protection

- 1) **KYC/AML Compliance:** We will ensure compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations to prevent fraudulent activity and ensure the safety of all players.
- 2) **User Anonymity and Privacy:** Players' personal data will not be shared with unauthorized parties. We commit to ensuring that our users can enjoy privacy while also complying with necessary regulatory requirements.
- 3) **Data Minimization:** Only the minimum amount of user data necessary for transaction processing and compliance will be collected and stored.

7. Crypto-Specific Security Measures

- 1) **Blockchain Security:** Transactions involving cryptocurrency are recorded on secure, immutable blockchains. We implement wallet security measures, such as cold storage and multi-signature wallets, to prevent unauthorized access and ensure safe transactions.
- 2) **Crypto Wallet Management:** We employ strict protocols for the management and storage of cryptocurrency wallets, ensuring private keys are stored securely and not accessible to unauthorized users.

8. Compliance with Regulatory Standards

The casino is committed to adhering to local, national, and international data protection laws and regulatory frameworks governing the use of cryptocurrencies and fiat currencies. We will regularly review compliance requirements and update the policy accordingly.

9. Employee and User Awareness

- 1) **Training:** Employees will receive regular training on information security best practices, data protection policies, and how to spot potential security threats.

- 2) **User Education:** We will provide guidance for players on maintaining the security of their accounts and data, including using strong passwords, recognizing phishing attempts, and securing their devices.

10. Security Incident Reporting

Any employee, user, or third-party vendor who identifies a potential security incident or breach is required to report it immediately to the designated security officer. In the event of a breach involving sensitive user data, we will notify affected users in accordance with applicable laws and regulations.

11. Policy Review

This policy will be reviewed annually or after significant security incidents, changes in the law, or modifications to our operations. Updates will be communicated to all employees, contractors, and users as necessary.

12. Violations and Enforcement

Violations of this policy will result in disciplinary actions, which may include termination of employment, access revocation, or legal action, depending on the severity of the breach.