SECURITY POLICY

Last Updated: 29/01/2026

Applies to all Quantisca platforms, software, systems, and data processing activities

1. Introduction

This Security Policy ("Policy") describes the technical, organizational, and procedural measures implemented by Quantisca ("we", "us", "our") to protect systems, software, data, and infrastructure associated with Quantisca Products.

By using Quantisca Products, users acknowledge and accept the security practices described in this Policy.

2. Security Objectives

Quantisca's security framework is designed to ensure:

- Confidentiality — preventing unauthorized access to data
- Integrity — preventing unauthorized modification of systems or data
- Availability — ensuring reliable access to Quantisca Products
- Resilience — maintaining operational continuity under adverse conditions

3. Scope

This Policy applies to:

- all Quantisca websites and platforms

- all software (EAs, indicators, scripts, tools)
- all internal systems and infrastructure
- all data processed or stored by Quantisca
- all employees, contractors, and partners
- all third party service providers acting on behalf of Quantisca

4. Technical Security Measures

4.1. Encryption

Quantisca implements industry standard encryption for:

- data in transit (HTTPS/TLS)
- sensitive internal communications
- licensing and authentication mechanisms

4.2. Access Controls

Access to systems is restricted based on:

- role based permissions
- least privilege principles
- secure authentication methods

Unauthorized access attempts are monitored and logged.

4.3. Secure Development Practices

Quantisca follows secure coding principles, including:

- code reviews
- version control
- vulnerability scanning
- controlled release processes

4.4. Infrastructure Security

Quantisca uses secure hosting environments with:

- firewalls

- intrusion detection systems
- DDoS protection
- automated monitoring

4.5. Data Minimization

Quantisca collects and stores only the minimum data necessary to operate its services.

5. Organizational Security Measures

5.1. Confidentiality Obligations

All employees, contractors, and partners are bound by:

- confidentiality agreements
- IP assignment agreements
- access restrictions

5.2. Security Training

Personnel with access to systems receive:

- security awareness training
- operational guidelines
- incident response procedures

5.3. Vendor Management

Third party providers must:

- meet security standards
- comply with data protection requirements
- implement appropriate safeguards

6. Licensing & Software Protection

Quantisca implements multiple layers of protection for its software, including:

- license activation systems
- hardware or account binding

- anti tampering mechanisms
- obfuscation and code protection
- periodic license verification

Users must not attempt to bypass or interfere with these systems.

7. Monitoring & Logging

Quantisca monitors systems for:

- unauthorized access attempts
- suspicious activity
- performance anomalies
- potential security threats

Logs are retained for security and diagnostic purposes.

8. Incident Response

8.1. Detection

Quantisca uses automated and manual methods to detect:

- breaches
- unauthorized access
- system failures
- data exposure risks

8.2. Response

In the event of a security incident, Quantisca will:

- investigate promptly
- mitigate risks
- restore normal operations
- notify affected parties when legally required

8.3. Recovery

Quantisca maintains:

- backup procedures
- redundancy mechanisms
- disaster recovery plans

9. User Responsibilities

Users are responsible for:

- securing their devices
- maintaining strong passwords
- protecting account credentials
- ensuring stable internet/VPS for automated trading
- keeping their trading platform updated
- avoiding unauthorized modifications to Quantisca software

Quantisca is not responsible for security failures caused by user negligence.

10. Limitations of Liability

Quantisca is not liable for:

- user misconfiguration
- compromised user devices
- broker/platform failures
- VPS or internet outages
- third party service vulnerabilities
- force majeure events
- attacks targeting the user's environment

Users acknowledge that no system is 100% secure.

11. Continuous Improvement

Quantisca regularly reviews and updates:

- security controls
- infrastructure

- internal procedures
- risk assessments

Security evolves continuously to meet industry standards.

12. Changes to This Policy

Quantisca may update this Policy at any time. Continued use of Quantisca Products constitutes acceptance of the updated version.

13. Contact

For security inquiries or incident reporting, contact: contact@quantisca.com