INFORMATION SECURITY POLICY

Cybersecurity and Data Protection Framework

NIHAO CARBON CERTIFICATES

Version 1.0
Effective Date: January 1, 2024
Classification: CONFIDENTIAL

1. Purpose

This policy establishes the framework for protecting the confidentiality, integrity, and availability of information assets in accordance with MiFID II organizational requirements, DORA, and industry best practices.

2. Scope

This policy applies to all information systems, data, employees, contractors, and third parties with access to Nihao Carbon Certificates information assets.

3. Information Classification

Classification	Description & Handling
CONFIDENTIAL	Highly sensitive data (client PII, trading data, credentials). Encrypted at rest and in transit. Access on need-to-know basis.
INTERNAL	Internal business information. Not for external distribution without authorization.
PUBLIC	Information approved for public release (marketing materials, public announcements).

4. Access Control

- Unique user identification for all system access
- Multi-factor authentication (MFA) required for all critical systems
- Role-based access control (RBAC) with least privilege principle
- Quarterly access reviews and prompt revocation upon termination
- Password policy: minimum 12 characters, complexity requirements, 90-day rotation

5. Network Security

- Firewalls and intrusion detection/prevention systems
- Network segmentation between trading, corporate, and DMZ
- VPN required for all remote access
- Continuous monitoring and logging of network activity

6. Encryption

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Hardware security modules (HSM) for cryptographic key management

7. Incident Response

Security incidents must be reported immediately to IT Security. The incident response process includes:

1. Detection and initial assessment
2. Containment and eradication
3. Recovery and restoration

4. Post-incident review and lessons learned
5. Regulatory notification (if required under DORA/GDPR)

8. Security Awareness Training

All employees must complete annual security awareness training covering phishing, social engineering, data handling, and incident reporting.