

INFORMATION & CYBERSECURITY POLICY

Document Ref: SEC-POL-01 | Effective Date: September 2026 | Version: 2.4 | Status: Approved

At Onnytech LTD, we take the security of our clients, engineers, industrial facilities, and application data with the utmost seriousness. As an industrial engineering and automation firm specialising in Anaerobic Digestion facilities, our digital infrastructure is designed and maintained to be as resilient and reliable as the physical automation plants we engineer.

This Information & Cybersecurity Policy defines the technical, operational, and organizational security controls implemented across the Onnytech digital platform, client dashboards, and engineer mobile portals to defend against unauthorized access, data interception, and abuse.

1. Transport Layer Security & Encryption

All network communications between user browsers and Onnytech cloud services are strictly encrypted in transit and defended against downgrade attacks:

- **Forced HTTPS / Modern TLS:** All HTTP connections are upgraded to HTTPS using modern Transport Layer Security (TLS 1.3/1.2). Insecure plaintext connections are rejected across all platform endpoints.
- **Content Security Policy (CSP):** We enforce strict Content Security Policy headers that restrict browser script execution, style injection, and object loading to approved first-party origins, preventing Cross-Site Scripting (XSS) and code injection.
- **Defensive Security Headers:** Comprehensive HTTP security headers are enforced across all server responses, including X-Frame-Options: DENY (clickjacking defense), X-Content-Type-Options: nosniff (MIME-sniffing prevention), and strict Referrer policies.

2. Exclusive Passwordless Authentication

To eliminate the vulnerabilities of weak, reused, stolen, or phished passwords, Onnytech operates an exclusively passwordless identity architecture:

- **FIDO2 / WebAuthn Passkeys:** All portal access requires public-key cryptography via WebAuthn. Users authenticate locally using hardware biometrics (FaceID, TouchID, Windows Hello) or a device PIN. Private cryptographic keys never leave the user's physical device hardware.
- **Phishing Immunity:** Passkeys are cryptographically bound to the origin domain (onnytech.co.uk), making credential theft, credential stuffing, and interception impossible. Traditional passwords and SMS codes are completely excluded.

3. Traffic Throttling & Abuse Prevention

Our application gateway incorporates a multi-tiered Token Bucket rate-limiting engine to safeguard availability and prevent brute-force probing:

- **Global Request Throttling:** Standard API and web traffic is bounded at 60 requests per minute per IP address, smoothing traffic bursts and deterring scraping.
- **Authentication Endpoint Guarding:** Login initiation routes are constrained to a strict maximum of 5 requests per minute per IP, neutralizing denial-of-service attempts and credential exhaustion scripts.
- **Privacy-Preserving IP Hashing:** Rate-limiting states are tracked using one-way cryptographic hashes (SHA-256) of incoming IP addresses, enforcing abuse prevention without persisting raw, identifiable network telemetry in operational caches.

4. Session Lifecycle & Access Controls

Authenticated user sessions are managed with defense-in-depth safeguards to prevent session hijacking and unauthorized persistence:

- **Continuous Session Regeneration:** Session identifiers are regenerated every 5 minutes (300 seconds), instantly destroying previous tokens and invalidating stale cookies.
- **Role-Based Idle Timeouts:** Server-enforced inactivity timeouts automatically terminate idle sessions: 30 minutes for Administrators, 1 hour for Clients, and 12 hours for field Engineers.
- **Cryptographic Remember-Me Tokens:** Persistent login options employ split-token verification (a public selector coupled with a SHA-256 hashed validator) stored in HttpOnly, SameSite=Lax, and Secure cookies.

5. Hardware-Bound Session Credentials (DBSC)

Onnytech implements Device Bound Session Credentials (DBSC) to neutralize cookie theft and malware-based session hijacking:

- **Hardware Cryptographic Binding:** On supporting modern browsers, a dedicated public/private key pair is generated inside the client device's physical Trusted Platform Module (TPM) or Secure Enclave upon login.
- **Proof-of-Possession Validation:** The session is bound directly to this hardware key. Every subsequent request verifies cryptographic proof-of-possession. If a session cookie is exfiltrated by malware, it cannot be used on any other physical device and is blocked.

6. Infrastructure Hardening & Vulnerability Disclosure

- **Principle of Least Privilege:** Database accounts operate with constrained permissions. Administrative, engineer, and client access tiers are physically and logically segregated.
- **Tamper-Evident Audit Logging:** Critical administrative actions, permission changes, and security events are logged with timestamps, user IDs, and context for full oversight.
- **Responsible Disclosure:** If you discover a potential vulnerability, please contact our security team at info@onnytech.co.uk. We verify and resolve reported issues promptly.

Security & Data Protection Office — Onnytech LTD

Direct Inquiries: info@onnytech.co.uk | Telephone: 01588 650537

Physical Facility: Old Farm, Wentnor, Bishops Castle, Shropshire, SY9 5EE, United Kingdom