Cyber Security Policy

Company Name: MDD Fabrication & Engineering Limited

Policy Owner: Nathan Diniz

Effective Date: 06/09/2025

Review Date: 06/09/2026

1. Purpose

This policy outlines the principles and procedures MDD Fabrication & Engineering Limited will follow to protect its digital assets, systems, and data from cyber threats. It ensures compliance with UK laws including GDPR and supports the Cyber Essentials framework.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who access MDD's IT systems, data, or networks.

3. Roles & Responsibilities

- Director: Overall accountability for cyber security strategy.
- IT Administrator (or designated staff): Day-to-day implementation and monitoring.
- All Staff: Responsible for following cyber security procedures and reporting incidents.

4. Key Principles

4.1 Access Control

- Role-based access to systems and data.
- Multi-factor authentication (MFA) for sensitive systems.
- Regular audits of user access rights.

4.2 Data Protection

- Personal and sensitive data handled in accordance with GDPR.
- Encryption of data at rest and in transit.
- Secure disposal of obsolete data and devices.

4.3 Password Management

- Strong password policies enforced.
- Use of password managers encouraged.

- Passwords must not be reused across systems.

4.4 Device & Network Security

- Company devices must have up-to-date antivirus and firewall protection.
- USB and external devices must be scanned before use.
- Wi-Fi networks must be secured with WPA3 encryption.

4.5 Software & Patch Management

- Automatic updates enabled where possible.
- Critical patches applied within 48 hours of release.
- Only authorised software may be installed.

4.6 Incident Response

- All incidents must be reported immediately to the IT Administrator.
- Incident response plan includes containment, eradication, recovery, and post-incident review.
- Regular tabletop exercises conducted to test readiness.

4.7 Training & Awareness

- Mandatory cyber awareness training for all staff annually.
- Phishing simulations conducted quarterly.
- Updates on emerging threats shared via internal communications.

5. Compliance & Monitoring

- Regular internal audits and external assessments.
- Compliance with Cyber Essentials certification.
- Monitoring tools (e.g., SIEM) used to detect anomalies.

6. Third-Party & Supply Chain Security

- Vendors must demonstrate cyber security compliance.
- Contracts include data protection and incident reporting clauses.

7. Policy Review

This policy will be reviewed annually or after any significant cyber incident or regulatory change.