Information Security Policy Statement

E P Industries' senior management team recognise the importance of developing and implementing an Information Security Management System (ISMS) to protect business information assets from security threats, whether internal or external, deliberate or accidental. Demonstrating successful implementation of this ISMS will assure all interested parties of the high regard we have for their intellectual property.

1. Purpose
This policy sets out how we protect the confidentiality, integrity, and availability of all information we hold, including employee data, customer information, operational documents, and commercially sensitive material.

2. Scope
Applies to all employees, contractors, and third parties who access our systems, data, or equipment.

3. Responsibilities
- **Management**: Ensures appropriate controls, training, and resources are in place.
- **Employees & Contractors**: Follow this policy and report any security concerns immediately.
- **Third Parties**: Must handle information in line with our requirements and GDPR.

4. Access Control
- Access is granted on a need-to-know basis.
- Strong passwords and multi-factor authentication must be used where available.
- Access is removed immediately when roles change or engagement ends.

5. Data Handling & Storage
- Business data must be stored only on approved systems (OneDrive/SharePoint or secure servers).
- Confidential or personal data must not be stored on personal devices.
- Data must be shared only with authorised recipients and only for legitimate business purposes.

6. IT & Cyber Security
- Company devices must be kept updated and protected with antivirus and security controls. This is managed by IT Network Company Premier-Systems.
- Staff must be vigilant for phishing, suspicious links, or unexpected attachments.
- Only approved software may be installed on company devices.

7. Remote Working
- Devices must be used in secure environments and not left unattended.
- Screens must be protected from unauthorised viewing.
- Public Wi-Fi must not be used without a secure connection.

8. Incident Reporting
Any loss, suspected breach, or security concern must be reported to management **immediately** so that appropriate action can be taken.

9. Data Protection & Confidentiality

- Personal data must be processed lawfully and in line with GDPR.
- Information shared with customers (e.g., employee names for job sheets) must include confidentiality expectations.
- Third parties receiving data must protect it to an equivalent standard.

10. Continuous Improvement
We review risks, incidents, and controls regularly to ensure ongoing protection of information.

EDDIE PILSWORTH
Managing Director

Date: **April 2026**