Policy ID: P09	Last Reviewed: 5 May 2026	Next Review: 10 January 2027	Version: 2.0

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) POLICY

1. Introduction

An Information Security Management System (ISMS) describes the way in which a business manages and protects its information. The international standard for this is ISO 27001, which provides a framework of policies and procedures for limiting the risks to business from anything that might compromise data security, in the same way that a firewall protects access to a computer or antivirus software protects computer files.

The information covered includes financial records, customer details, employee details, supplier details, and other third-party information entrusted to the company. Much of this is governed by UK data protection law, including UK GDPR. ISO 27001 certification is not mandatory, but its implementation supports compliance with privacy and data security regulations, and MW Fire Ltd uses it as a benchmark for professionalism and good practice.

2. Confidentiality and Integrity

MW Fire Ltd is committed to ensuring the safety of all information entrusted to us. We interpret and implement the guidance in ISO 27001 as far as it applies to our business. While we are not certificated to this standard, we strive to attain that level of professionalism wherever possible and use it as a reference point whenever we review our handling and safekeeping of information.

We will:

- Implement a system to protect the integrity of all data and information.
- Review and improve the ISMS at regular intervals or whenever it becomes necessary.
- Manage requests from third parties for company information, such as for a PQQ, to identify and mitigate information security risks.
- Promote a security-driven culture within the company through employee training on data protection and information security.
- Address non-compliance or breaches through the company's disciplinary process.

3. Roles and Responsibilities

All employees at MW Fire Ltd are responsible for understanding and following established company policies and data protection regulations to a reasonable standard. This includes practical habits such as deleting sensitive information from personal devices once it has been transferred to secure company systems, and being selective about files attached to emails.

Compliance with all ISMS policies and procedures is monitored jointly by the Human Resources, Accounts, Administration and Health and Safety functions. A report is reviewed annually by the Managing Director. Responsibility for delivering staff training and communicating policies to employees, customers and suppliers lies with the Health and Safety Administration.

4. Risk Assessment

The company will perform vulnerability assessments and audits whenever a threat has been identified, or at reasonable intervals to keep pace with developments in cyber security and physical data protection. Findings are reviewed by management and any remedial actions are assigned and tracked to completion.

5. Information Systems

The majority of company data and information is held online. Critical operational data is stored on SimPRO and company information is held on a Google Drive business account. Both platforms are assessed for UK GDPR compliance. The company website does not process payments but is protected by SSL encryption nonetheless.

Any third-party cloud services used to store or process data are reviewed for security and compliance before use.

6. Preparedness and Recovery

Business continuity procedures are incorporated into the company's Business Continuity Plan, with the primary objective of ensuring that data can be accessed without interruption, including at times of unforeseen disruption such as loss of access to the office.

Files are organised in a clear and consistent folder structure, for example: /policies, /health and safety, /forms, /accreditations, /training, /projects. This simple classification means documents can be located quickly, which is of particular importance when accessing incident forms or emergency procedures under pressure.

7. Social Media and Public Facing Communications

MW Fire Ltd maintains accounts on Facebook, Instagram, Twitter and LinkedIn, accessible via the footer at www.mwfire.co.uk. These are monitored by the webmaster. Proposed posts, suggestions and responses are highlighted by the webmaster and all actions are authorised by the HR Manager or Managing Director before publication.

The company does not operate a dedicated media or press release function.

8. Self-Assessment

The company believes that prevention and active monitoring are the most effective means of identifying potential security issues.

We will :

- Survey the potential risks and assess vulnerabilities in our data storage methods.
- Maintain a plan of action in the event of a security breach.
- Incorporate a critical data retention solution and recovery solution into the Business Continuity Plan.

9. Management Statement of Commitment

MW Fire Ltd understands how crucial it is to process information securely. The protection of customer, employee and business data is of primary importance to us. We are committed to developing, implementing and continually improving our ISMS in line with ISO 27001 standards and applicable data regulations, and to promoting a company that can be trusted above all else.

The purpose of this policy is to formalise our obligation and to take responsibility for the trust that our staff, contractors and clients place in us as a professional company. We are committed to effectively managing and securing our information and to fostering a culture of confidentiality, accountability and continual improvement.