Information Security Policy

Introduction:

The purpose of this Information Security Policy is to ensure the protection of sensitive and confidential information within our organisation. This policy outlines the principles and practices that all employees and stakeholders must adhere to, safeguarding information assets against unauthorised access, disclosure, alteration, and destruction.

Scope:

This policy applies to all employees, contractors, and third-party service providers who have access to our information systems, data, and networks.

Policy Statements:

1. Access Control:

- Only authorised personnel are granted access to sensitive information based on their roles and responsibilities.
- Multi-factor authentication (MFA) must be used for accessing critical systems.
- Access permissions are regularly reviewed and updated as necessary.

2. Data Protection:

- All sensitive information must be encrypted both in transit and at rest.
- Regular backups of critical data must be conducted and securely stored.
- Data must be classified based on its sensitivity and handled accordingly.

3. Incident Response:

- All security incidents must be reported immediately to the Information Security team.
- An incident response plan must be in place and regularly tested.
- Lessons learned from incidents must be documented and used to improve security measures.

4. Security Scanning and Monitoring:

- Regular security scans must be conducted to identify vulnerabilities in systems and applications.
- Continuous monitoring of network traffic and system activities must be implemented to detect and respond to security threats.
- Security logs must be maintained and reviewed regularly to identify any suspicious activities.

5. Training and Awareness:

- All employees must undergo regular information security training.
- Awareness programs must be conducted to educate employees about the latest security threats and best practices.
- Employees must acknowledge and comply with the security policies and procedures.

6. Compliance and Audits:

- The organisation must comply with all relevant legal, regulatory, and contractual obligations related to information security.
- Regular internal and external audits must be conducted to ensure compliance with this policy.
- Non-compliance with this policy may result in disciplinary actions.

Fire Specialists Ltd. Registered Office: Central House, 25 Camperdown Street, London, England E1 8DZ.
Registered in England No. 16076768

Enforcement of Additional Policies:

- This Information Security Policy is reinforced through additional policies, standards, and guidelines that address specific aspects of information security.
- All related policies are reviewed regularly to ensure alignment and effectiveness.
- Any deviations from these policies must be reported and will be addressed through appropriate corrective actions.

Responsibilities:

- The Information Security team is responsible for implementing and enforcing this policy.
- Employees are responsible for adhering to the policy and reporting any security concerns.

Review and Updates:

This policy will be reviewed and updated annually or as necessary to address emerging security threats and changes in the organisation.

Steve Harrison
Managing Director

18th November 2024

Document Control:

Date	Author	Changes	Approved by	Version
18/11/24	Head of Risk & Compliance	1st Issue	Managing Director	1.0