INFORMATION SECURITY POLICY STATEMENT

1. Purpose:

The purpose of this document is to define the role that J Coffey Construction's Top Management takes in ensuring commitment to information security, the development and propagation of this policy, and the assignment of appropriate information security roles, responsibilities, and authorities to protect J Coffey Construction's assets from all relevant threats, whether internal or external, deliberate, or accidental.

2. Objective:

J Coffey Construction, which provides Provision of Labour, Plant & Equipment to facilitate Construction, Civil Engineering and Specialist Construction Services including, New Build, Refurbishment, Design & Build and Control of Subcontractors to the Construction, Infrastructure & Rail sectors within the UK & Europe and is committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets (information assets include data or other knowledge stored in any format on any system that has value to an organisation, and should be logged) throughout the organisation in order to compete in the marketplace and maintain its legal, regulatory, and contractual compliance and commercial image. To achieve this, J Coffey Construction is working towards implementing an information security management system (ISMS) in accordance with the international standard ISO/IEC 27001:2013 requirements, all of which will be subject to continual, systematic review and improvement as it evolves.

3. Roles and Responsibilities

- The Board of Directors is responsible for setting and approving the information Security Policy.
- The Board of Directors is responsible for ensuring that roles, responsibilities, and authorities are appropriately assigned, maintained, and updated as necessary.
- All Employees/Staff and those working under the control of the proposed scope of the ISMS to be implemented are responsible for the adhering to the requirements of the Information Security Policy and for fulfilling any duties related to assigned roles, responsibilities, or authorities. The consequences of breaching the information Security Policy are set out in J Coffey Construction's disciplinary policy and in contracts and agreements with third parties.

4. Policy Objectives:

It is the policy of J Coffey Construction that:

- This policy is appropriate to the purpose of the Organisation and communicated within the Organisation.
- Information is made available to all authorised parties with minimal disruption to the business processes.
- The organisation commits to satisfy applicable requirements related to information security

- The organisation commits to continual improvement of the information security system as it evolves.
- The integrity of this information is maintained
- The confidentiality of information is preserved.
- The organisation ensures compliance with all legislation, regulations, and codes of practice, and all other requirements applicable to its activities.
- Appropriate business continuity arrangements are in place to counteract interruptions to business activities and these take account of information security.
- Appropriate information security education, awareness and training is available to staff and relevant others working on the Organisation's behalf.
- Breaches of information security or security incidents, actual or suspected, are reported, and investigated through appropriate processes.
- Appropriate access control is maintained and information is protected against unauthorised access. The organisation maintains a management system that will achieve its objectives and seeks continual improvement in the effectiveness and performance of the management system based on risk. The organisation maintains awareness for continual improvement, and the ISMS is regularly reviewed at planned intervals by Senior Management to ensure it remains appropriate and suitable for the business.

The above Information Policy Objectives will be applied as is practicable, in accordance to Cl. 6.2 of the ISO 27001:2013 standard.

This policy is approved by Senior Management and is reviewed at regular intervals or upon significant change.
This policy is communicated to all Employees/Staff within J Coffey Construction and is available to customers, suppliers, stakeholders, and other interested parties upon request as appropriate.

5. Security Measures:

Security measures implemented to ensure secure data protection includes the following:

- Laptop and desktop anti-malware
- Server anti-malware
- Cloud-hosted email spam, malware, and content filtering
- Email archiving and continuity
- Website malware and vulnerability scanning
- Intrusion detection and prevention
- Desktop firewall
- Perimeter firewall

Data Security is not wholly a Data Protection issue. Business Continuity is a fundamental part of data protection and as such, the Organisation's Business Continuity Plan will be reviewed and maintained to ensure it aligns with both our requirements and our clients, to ensure all relevant controls are in place to secure sensitive information/data and have appropriate backup to continue secure service provision.

6. Setting Security Levels:

The greater the consequences of a breach of confidentiality, the tighter the security should be, to that end we will provide support training that includes:

- An initial introduction to IT security, covering the risks, basic security measures, company policies and where to get help.
- Training on how to use company systems and security software properly.
- On request, a security health check will be carried out on staff computer, tablet or phone.

In the event of a breach of confidentiality, the Organisation shall notify the relevant effected parties at risk as soon as possible, advising the nature of the breach, so the effected party can take appropriate preventative actions.

7. Document Owner and Approval:

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.
The current version of this document is available to the Board of Directors, Head of the IT Department and other identified staff as approved by the Board of Directors and is published on the K Drive/File 4/File 1.0 Policy Statements, where access and editing rights have been appropriately appointed.

This policy statement applies to all employees and other personnel engaged in J Coffey Construction operations:

Signed: *Eddie Barrett* (Original Signed) Date: 12/01/2024

Eddie Barrett

Group Managing Director

On behalf of J. Coffey Construction