

**ISG is a dynamic global construction services company. Our people specialise in fit out, technology, construction and development and are dedicated to delivering places that help people and businesses thrive.**

Information is a key resource for ISG, without which virtually all of our activities would cease. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information entrusted to ISG by our customers will also be treated in the same careful manner.

This Information Security Policy sets out ISG's strategic intent to provide a high level of security for both our own and our clients data by being independently assessed and certified against the UK Cyber Essentials Plus standard.

We will create an environment to protect our information, assure business continuity and minimise damage by proactively managing our information security environment.

ISG shall:

- Ensure the availability, confidentiality and integrity of our information.
- Ensure this policy supports the security requirements of the General Data Protection Regulation (GDPR).
- Implement controls and processes such that information is, where practicable, to be available when required.
- Ensure that information is available to authorised individuals and is managed in accordance with this information security policy, GDPR and any other relevant policies or standards.
- Ensure that information security training is available to all who have access to our systems or sensitive information.
- Ensure that Risk Management Systems are used to identify and assess the risks which may arise due to loss, corruption, misuse or theft of our information assets; and implement controls to limit the exposure to the identified risks.
- Ensure that the coverage, content and application of information security standards that support this policy are adequate to address the level of risk ISG faces, and that compliance is attained against legal, regulatory, policy and industry requirements.
- Set measurable objectives and targets for Information Security, which will provide a framework for review and improvement of the Information Security Management System.

Our approach to managing information security shall be set out in a series of policy documents that provide the mandatory controls for the governance and protection of information within ISG.

It is imperative that all those with access to our data understand their information security obligations as stated in the Acceptable Use Policy. Failure to adhere to this policy will be dealt with under ISG's disciplinary procedures and may result in summary dismissal.

This policy should always be read in conjunction with the ISG Data Protection Policy

The Group IT Director is responsible for the delivery of an Information Security Management System in order to comply with this policy. Regular reporting will occur both via the ISG Risk Committee and monthly IT reporting to the Chief Financial Officer

This policy reflects the aspirations of ISG and will be reviewed at least annually by the Chief Executive Officer.

**For and on behalf of ISG**

Signed:

A handwritten signature in black ink, appearing to be 'P. Cossell'.

Paul Cossell

**Chief Executive Officer ISG**

Date: 10 March 2021