



## INFORMATION SECURITY POLICY

The Costain Group is committed to managing its information assets in accordance with current legislation, best practice and ISO 27001:2013.

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory and contractual obligations.

To achieve this, it is Costain's information security policy to ensure that:

- Information will be protected from unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information is made available to authorised persons
- Regulatory and legislative requirements will be met
- Business Continuity plans will be produced, maintained and tested
- Information security training will be available to all staff
- All breaches of information security, actual or suspected, will be reported, investigated and resolved

The overall objective is to treat information appropriately and in accordance with the risks associated with it.

The policy applies to all employees (permanent and temporary) and any other third parties that utilise Costain Information and Communication Technology (ICT).

This policy will be reviewed annually to ensure continuing suitability, adequacy and effectiveness of managing information security in Costain.

Signed: .....

A handwritten signature in black ink, appearing to read "A. Wyllie", written over a horizontal line.

**A. Wyllie** (Chief Executive Officer)

Date: 13<sup>th</sup> Jun 2015