SECURITY POLICY

This Policy is a declaration of the Costain Board's intent in relation to ensuring business continuity is maintained through prevention and mitigation of security risks.

The Board recognises that secure operations are dependent upon employee participation, commitment and accountability. Costain will maintain the highest appropriate levels of security for our offices and sites to prevent unauthorised access while allowing authorised persons to go about their business.

The Costain approach will focus on four key aspects of security. These are;

1. Protection and control of data to the required security level and ensure transmission on a need to know basis.
2. Providing suitable security clearance to personnel as appropriate.
3. Protection of Staff, Partners, Clients and Visitors from unwanted interference, malicious or otherwise.
4. Protection of Assets from damage, malicious or otherwise.

To meet the four key aspects of security all operations will be carried out in a way which provides and maintains a secure working environment. This will be achieved by;

- Prevention through threats analysis and risk evaluation on a regular basis.
- Mitigation plans will be maintained against the risks identified.
- Preparedness to rapidly and effectively respond to security incidents.
- Training staff to the level of professionalism and integrity demanded by our policy.
- Investigate and report all security incidents and develop and close out corrective actions
- Demonstrate compliance with recognised standards and best practise by regular audit from appropriate third party organisations.

This policy (and all associated policies and procedures) will be reviewed annually to ensure continuing suitability, adequacy and effectiveness of managing security within Costain.

Signed: .....

Date: 6th Feb 2015

A. Wyllie (Chief Executive Officer)