BUILDING AND SITE SECURITY POLICY

Providing a secure working environment, resilient to malevolent forces is critical to the success of Costain and the security of our critical national infrastructure. This Policy is a declaration of the Costain Board's expectations for all employees, partners, contractors, and suppliers in relation to maintaining safe and secure buildings/sites.

Cyber security matters are covered in our Information security and data protection policy and should be read in conjunction with this policy. Additionally, the Costain Business continuity management policy sets out the principles for ensuring business continuity in the event of an incident.

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

To ensure a secure working environment is maintained, building and site operations **must** adhere to the following minimum expectations:

- Only authorised people (i.e., those with a legitimate purpose) have access to the building/site and the Building Access Control Standard is followed at all times.
- A current security risk or threat assessment of the building/site is in place.
- A building (or where applicable, a site) security plan is in place, detailing risk mitigation actions for all identified risks.
- An up-to-date incident response or crisis management plan is in place and briefed accordingly, ensuring all incidents are rapidly, effectively, and appropriately responded to.
- All incidents of unauthorised access are notified immediately to the local incident response team and Costain Security and where required, reported to the police.
- All security incidents are recorded and reported to Costain Security in a timely fashion to ensure lessons learnt are appropriately captured.
- Only security providers listed on the 'Approved Contractors Scheme' of the Security Industry Authority (SIA) are to be used.
- People who have nominated responsibilities for security matters must be trained to the appropriate levels of professionalism and integrity as demanded by our Health and Safety and People policies, with appropriate guidance from the Costain Security team.

To ensure the protection of information held within Costain Offices and sites for which Costain is responsible, effective security controls must be implemented to protect both Costain and customer information in accordance with Costain, customer, and where appropriate, HMG Security Policy Framework (SPF), GovS: 007, and Office for Nuclear Regulation requirements, governed [where applicable] under the National Security Act (2023) and The Official Secrets Act (1989), including, but not limited to:

- Operating a robust security screening procedure for Employees, Off Payroll Workers (OPW) and Contractors
- Ensuring the "need to know" principle is adhered to
- National Security Vetting (NSV) is applied where required
- Ensuring confidential or classified information is handled correctly and in accordance with Costain and customer requirements, applying Government Security Classifications (GSC) where necessary

Business Owner: Group Security Manager

- Ensuring that information is correctly shared (or not shared), with particular attention and where applicable, regarding any ‘notifiable’ nationalities
- Ensuring a clear desk/screen policy is in operation.

Compliance to this policy and our security procedures is monitored by our internal audit process and reported to the Board. To ensure continuing suitability, adequacy, and effectiveness of managing building and site security within Costain, this policy, referenced policies and associated guidance documents will be reviewed annually, and as required.

Signed: DocuSigned by: 4E139DD4F384417... 8/1/2026 | 12:33 GMT

A Vaughan (Chief Executive Officer)