Information Security Policy

Balfour Beatty

The security of Balfour Beatty's information[1], and that which is trusted to us by our customers, partners, suppliers and vendors who may hold information on our behalf, is fundamental to protecting maintaining and operating our business.

The loss, corruption or theft of information and supporting systems could have a serious impact on the Group's business activities and reputation.

Our people, information and processing systems are critical to our business and need to be protected appropriately.

Our policy is to create an environment in which our information is secure. We achieve this by:

- Ensuring the availability, confidentiality and integrity of our information, data and business systems are maintained and controlled
- Providing a well-managed security function that offers a high level of trust and confidence to our internal stakeholders as well as customers and partners
- Ensuring we have a robust, secure and monitored IT infrastructure which protects Balfour Beatty's data and commercial interests
- Ensuring that the use of information systems by employees does not create unnecessary business risk through inappropriate behaviour
- Managing assets so they are identifiable, traceable and compliant with legal and business requirements and remain fit for purpose, ensuring that contractual and business conditions are met
- Having appropriate controls in place to meet regulatory and legislative requirements and to ensure those controls are effective
- Ensuring the company promotes good security, guidance, training, and advice where appropriate.

It is the responsibility of every individual in and associated with the business to:

- Handle our own and third party information appropriately according to its sensitivity and/or classification and in compliance with any applicable confidentiality obligations owed to third parties
- Take steps to minimise the chance of information being lost
- Report security incidents or anything suspicious which may give rise to a security incident
- To prevent or minimise disruption to the business that may lead to financial or operational loss or a negative impact to reputation to the company
- Exercise vigilance when using computers, removable storage devices and phones or when using online services and applications (including without limitation any generative AI tools available either publicly or within our environment)
- Comply with company policies and complete all security related training designed to minimise the risk of a cyber security incident
- Be aware of any policies and requirements before travelling with IT equipment overseas
- Identify, manage and mitigate any areas of risk when handling information by ensuring employees are subject to background checks
- Use Balfour Beatty's information and supporting business systems for approved business purposes only and in a manner that does not compromise their confidentiality, integrity or availability
- Ensure our subcontractors and supply chain meet a good cyber security baseline.

We will bring this policy to the attention of our employees, supply chain and relevant interested parties; and review it on an annual basis.

AUTHORISATION

Jon Ozanne
Chief Information Officer, March 2025

[1]Information can include (for example); electronic data, paper documents, records, conversations and people