Global Operations Policy

Information Security Policy

Purpose

BMT is committed to protecting the confidentiality, integrity, and availability of information assets owned by or entrusted to the company. This includes trade secrets, intellectual property, business plans, personally identifiable information (PII), and any sensitive data, systems or infrastructure critical to ongoing operations.

Through implementing strong access controls, data encryption, employee security training, vendor risk management, and other information security controls tailored to mitigate risks, BMT aims to maximize trust in the company's ability to handle sensitive information responsibly.

The purpose of this policy is to ensure Information Security practices are applied and adhered to throughout BMT, to protect the confidentiality, integrity and availability of sensitive internal and external information.

Scope

This policy is applicable to all BMT employees, subcontractors and third parties under the day-to-day management control of BMT, regardless of location.

It applies to all information owned and managed by BMT, including that stored, transmitted, printed, written down or spoken in conversation.

Policy Statement

BMT is committed to taking all necessary steps to protect the Company's, and our customers', information assets against threats to its confidentiality, availability and integrity. This is achieved through:

- Emphasising the importance of Information Security in everything we do;
- Adopting a risk-based assessment and priorisisation process to mitigate information security risks;
- The continuous improvement via audit, learning from experience, and pro-active reviews, of our Information Security Policy, procedures and processes;
- Training and awareness provided to employees, contractors and third parties who have access to information under our care;
- Setting and reviewing information security objectives, through the annual review process, supported by the Security Management Team;
- Driving to achieve and then maintain certification to ISO 27001 and Cyber Essentials Plus;
- Maintaining an up to date Information Security Management System (ISMS);
- Including information security as an integral part of business continuity planning.
- Regularly reviewing and updating this policy to match the evolving threat landscape.

Policy:	Information Security Policy		
Policy Owner:	Joanna Groves	Version:	1
Approver:	Sarah Kenny	Date of Issue:	3rd June 2024

Responsibilities

It is the responsibility of every individual to:

- read, understand and comply with BMT Security Procedures and this policy;
- abide by the requirements and guidance provided by BMT and external customers, including (where applicable) government bodies, with regards to handling specific information.
- adhere to National Official Secrets Acts, Data Protection Acts or regulations, and all other applicable local and national legislation relating to information security;
- notify the local Security Management Team as soon as they become aware of an information security incident, observation, near miss, or concern.

Sarah Kenny
Chief Executive
June 2024