Data Tech	**INFORMATION TECHNOLOGY AND SECURITY POLICY**	BMP 06 ISSUE 7 September 2025

It is the policy of Data Tech Holdings Ltd (DT)'s to establish and maintain effective processes for the use and control of information security systems and equipment as part of our Business Management System (BMS).

Our BMS provides resilience to threats and vulnerabilities and provides a robust capability to respond should those threats to the Company's information assets be realised. This will safeguard the interests of key stakeholders (staff, clients, sub-contractors and suppliers) by protection from unplanned business interruptions, interference or loss; and protect the Company reputation, brand and value adding activities.

We will meet all legislative requirements in the markets and sectors in which we operate and comply with accepted best practice in information security, data protection and information technology.

We will identify critical suppliers who may be required to comply with this policy and the processes covered in the BMS. This policy is also to be read in conjunction with the Data Protection Policy HRP 009.

The Company shall:

- Provide all such IT equipment, software and accessories to enable employees to carry out their appointed tasks and administer the business.
- Retain ownership of the above and all files contained therein.
- Permit reasonable personal use of the Company email and internet, subject to operational needs.
- Monitor and access all aspects of its systems including data stored on the Company's IT systems in compliance with Data Protection Legislation.
- Reserve the right to require employees to hand over all Company data held, in useable format.
- Reserve the right to withdraw facilities and privileges at its discretion.
- Encourage direct contact with individuals rather than communicating via e-mail.
- Take disciplinary action against employees who abuse the company systems, send, receive, or download material that insults, causes offence or harassment or brings the Company into disrepute.

Employees and applicable sub-contractors shall:

- Use the Company's IT systems in accordance with the Company's Employment Handbook, Data Protection and Monitoring Policies and the following guidelines.
- Maintain the confidentiality of information, both during their employment and at any time after its termination, except as required by law or in the proper course of their duties.
- Select passwords that are not easily broken and keep all passwords and passcodes confidential.
- Log on to the Company's IT systems using their own password (where provided).
- Change their password every 3 months or as directed.
- Never use someone else's password.
- Never interfere with, override or turn off any anti-virus, anti-malware or other security systems.
- Never download, install or run unauthorised games or software, or open files or communications from unknown origins.

Our objectives are to:

- Clearly identify the assets and their legal and business requirements applicable to the BMS.
- Communicate the Information Security policy and objectives throughout the organisation and set annual objectives and targets for measuring the effectiveness of this communication.
- Understand our responsibilities, liabilities and limitations in terms of providing Information Security.
- Integrate Information Security policies into the day to day tasks and operational activities.
- Implement audit programmes that check and monitors our processes.

The directors are committed to:

- Providing the necessary resources to meet the business objectives and best practice.
- Communicate this policy to all staff (and others if required); ensuring that appropriate training is given.
- Review this policy on an annual basis to ensure it is still in line with business needs and legislation.

Bob Jacobs
Managing Director