# Information Security Policy

Beauparc Group commits to respecting the security and privacy of all company data and any customer data from outside parties. To this end, management are committed to maintaining a secure physical and virtual environment in which to process information to meet these promises.

- The purpose of the Policy is to protect the Company's information assets and third-party information held to fulfil the Company's service from all foreseeable threats, whether internal or external, deliberate or accidental.
- The Senior Leadership Team has reviewed and approved the Information Security Policy.

It is the policy of the Company to ensure that:

- Information is handled in a manner that fits with its sensitivity and classification;
- Personal use of Company information and telecommunication systems is prohibited;
- The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any business-related purpose consistent with data privacy regulations and in relation to the Company's Data Retention Policy;
- Employees do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Password protocols will be established and maintained to ensure the standard and regular change of passwords to minimise the risk of long-standing or easy-to-break passwords.
- Employees do not disclose information related to personnel unless authorised, must protect sensitive information and keep passwords and accounts secure;
- Approval is requested from management prior to installing, updating, modifying or removing any new software or hardware, third party connections, etc.;
- Employees do not install unauthorised software or hardware, including modems and wireless access unless explicit management approval is given.
- The Company shall maintain a physical environment that minimises the risk of breach and loss of data.
- Visitors entry and exit will be recorded and will be escorted at all times.
- Non-disclosure agreements will be sign by third parties if their activities will have the potential to come into contact with sensitive information.
- Employees leave desks clear of company or customer data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the Information Security Officer;
- Information should be made available with minimal disruption to staff and the public as required by this policy;
- Regulatory, legislative and industry best practice and standards will be understood and met;
- Business Continuity plans will be produced to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. Business continuity plans should be maintained and tested;
- Information security education, awareness and training will be provided to staff upon company induction with refresher training provided on a regular basis;
- All breaches of information security, actual or suspected, will be reported to, and investigated by the relevant authorities both internal and, if required, statutory;
- Appropriate access control will be maintained and information is protected against unauthorised
- access;
- Policies, Procedures and Guidelines related to Information Security will be made available in an online format to support the ISMS Policy;
- The Information Security Officer has direct responsibility for maintaining the ISMS Policy. They are involved with writing and/or managing the development of relevant policies, procedures and guidelines not limited to information security;

- The Information Security Officer will develop and improve the systems to continually improve them to meet different challenges and requirements faced by the Company;
- It is the responsibility of each member of staff to adhere to the ISMS Policy;
- Information security is managed through the Company's Risk Management framework;
- The availability of information and information systems will be met as required by the core and supporting business operations;  Objectives will be set and monitored to ensure effective outcomes;

If employees are unclear about any of the policies detailed herein, they should seek advice and guidance from their line manager.

Communication of any key areas related to the Information Security Management System will take place on a regular basis through employee training and company communications which will be issued as required.

The policy will be reviewed by the Company's Senior Leadership Team at least annually.

Signed:

Chief Executive Officer

Date: 1st January 2024