Springmount SERVICES PTY LTD
www.springmountservices.com

TECHNOLOGY SECURITY POLICY

Intent & Purpose

This policy describes how information technology is to be used and managed within Springmount Services. This IT security policy and rules provide clear policy direction and support for IT security. The support and commitment of the company and its people to IT security are demonstrated through the issue of this policy.

Principles

Springmount Services maintains a secure IT system that is not vulnerable or susceptible to malicious or unintended hazards or misuse to ensure that our business operations continue without interference or abuse and with optimum professionalism and confidentiality.

Operation and Incidence

Springmount Services provides its users with Internet access and electronic communications services as required for the performance and fulfilment of job responsibilities. These services are to increase productivity and not for non-business activities.

Access to Systems

All individuals who require access to the computer system shall be appropriately identified, using an individual user log-on, an agreement process and password control.

Authorised users of computer systems must:

- Be aware of their responsibilities and what they are authorised to do,
- Expect detection if they abuse their privilege,
- Have their access privilege removed as soon as it is no longer needed.

Also, the Administrator of our company computer systems must:

- Maintain a formal record of all persons registered to use the service,
- Immediately remove or amend access rights of users who have changed or have multiple jobs,
- Remove and/or suspend access rights of users who have departed our employment.

Protection against Malicious Software

The company IT Manager is responsible for procuring and facilitating the distribution of anti-virus software throughout the network.

Users are responsible for ensuring that virus checking, and eradication occurs on systems for which they are the primary user.

To decrease the risk of the action of malicious software and to limit its spread:

- All software, data and attachments must be checked where practicable for viruses before installation,

- The provided software tools must be used to detect and remove viruses,
- The IT Manager is to be immediately advised of any systems that are shown to be infected to be isolated as quickly as practicable until removal of the malicious software occurs.

Back-up

IT systems shall be frequently backed-up. An appropriate regular back-up schedule shall be implemented to protect all data and software. A sufficient number of back-ups of all data and software shall be stored off-site to protect against significant damage occurring at the primary location.

Disaster Recovery and Business Continuity Planning

Adequate measures shall be in place to prepare for and cope with disaster and facilitate the resumption of business services in the event of a disruption and minimise threats to the information system.

Authority for Monitoring Activity

The company has the right to inspect data on a computer system provided by it to prevent, detect or minimise unacceptable behaviour on that computer system, and to provide to any authorised member of the company, or law enforcement bodies, any information it possesses regarding the use of company resources.

Users should not expect privacy while using company-owned equipment. Information passing through or stored on company equipment can and will be monitored, and any breach of acceptable use addressed.

Physical Security

Physical security of IT facilities is necessary to prevent their unauthorised use and ensure that systems are adequately protected against natural hazards, theft and damage.

Access to all offices and work area containing computer equipment, or the means to access such information, must be physically secured.

Use of Computers

No person shall use company computer facilities for private purposes, including personal commercial, political or religious purposes.

Users of the computer facilities must ensure that they:

- Use computing resources ethically,
- Show restraint in the consumption of resources,
- Observe professional integrity,
- Respect intellectual property and the ownership of data and software,
- Respect other users' rights to privacy, and freedom from intimidation, harassment and annoyance,
- Do not install, download or capture any data without the authority of an appropriate manager or their delegate,
- Create or install any form of malicious software (for example worms, viruses, sniffers) which

may affect computing or network equipment, software or data,

- Must not connect any equipment providing off-site access to the company computer system (for example, a modem) without the prior approval of an appropriate Manager,
- Do not gamble or become involved in any illegal activities while using company resources,
- Must not tamper with or move installed company computer facilities without the authorisation of the IT Manager,
- Take special care when using mobile computers (laptops, palmtops etc.) To ensure that company business is not compromised,
- Must at all times provide adequate protection for mobile computers that are high-risk items for theft,
- Must report all incidents affecting security as quickly as possible,
- Remove all data before disposal or sale of any identified computer component,
- Shall not copy, disclose or transfer any company's computer software without permission from the relevant Manager or Administrator.

Use of Passwords

The use of passwords is a method of protecting information resources from unauthorised access. The selection of appropriate passwords is one way of enhancing the security of our computer system. To enhance password security, users must follow acceptable security practices in the selection and use of passwords as follows:

- All computers are to be protected by user log-on or password controls,
- Passwords must be at least six characters in length and must not be easily accessed,
- Passwords must be kept confidential at all times, no sharing of passwords with another individual,
- Passwords are to be reviewed annually,
- Personnel must physically log-off when the computer is not going to be attended for long periods.

Privacy and Security

The following security and privacy requirements will apply:

- The company does not accept responsibility for the privacy, confidentiality or security of data or information held on or transmitted over its systems,
- The company does not accept responsibility for loss, corruption, misdirection or delays in transmission of data through its system facilities,
- All incidents affecting security must be reported to the relevant Manager as quickly as possible,
- Users are responsible for the integrity of all data,
- Users must protect all data from unauthorised access,
- IT equipment should not be taken off-site without proper authorisation.

Breach of Policy

Any breach of this policy will be investigated on a case-by-case basis and dealt with in terms of the severity warranted.

Any person in breach of any aspect of this policy may result in disciplinary action and/or Springmount Services taking legal or other action against them and being made to pay for any loss or damage.

Electronic Mail Rules

Email messages should be kept as short and specific as practicable in the circumstances. Material that must not be transmitted by email includes:

- Sensitive data, inappropriate personal observations about the company, and its management, employees or clients,
- Advertising material (other than advertisements regarding the company),
- Material of a private nature including private, commercial, political or religious material,
- Solicitation of donations or subscriptions to political causes, content used to promote discrimination based on race, colour, national origin, age, marital status, sex, political affiliation, religion, disability or sexual preference,
- Offensive text or pictures (e.g. Pornography, racism, sexism, obscenities, insults, sarcasm), content that may reasonably be considered offensive, threatening or intimidating, defamatory statements, rumours, and gossip, about individuals or organisations.

User Behaviour and Expectations

Email is provided primarily for company business use and may be used in legal proceedings.

The general laws of copyright, privacy and freedom of information apply to email communications, and all users are responsible for compliance with those laws.

Subordinate documents

Nil

RACI

Responsible	It is the responsibility of the IT Manager to implement, maintain and communicate this policy.
Accountable	The final authority for this policy lies with the CEO.
Consulted	When making changes to this policy consultation should be carried out with employees, relevant contractors and the leadership team.
Informed	All changes to this policy should be communicated to all employees and relevant contractors.

Breach of The Policy

Breach of this policy may be regarded as misconduct, leading to disciplinary action, which may result in termination of employment or engagement. An individual may also be exposed to criminal or civil liability for a breach of relevant legislation.