Rocket Minds

Information Security Policy

1. Purpose

The purpose of this Policy is to safeguard information belonging to Rocket Minds and its stakeholder (third parties, clients or customers and the general public), within a secure environment.

This Policy informs the company's staff of the principles governing the holding, use and disposal of information.

It is the goal of Rocket Minds that:

- Information will be protected against unauthorised access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this Policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to one of the staff members, and investigated through the appropriate management channel.

Information relates to:

- Electronic information systems (software, computers, and peripherals) owned by the company.
- Hardware, software and data owned by the company.
- Paper-based materials.

2. The Policy

2.1 Authorised users of information systems

Authorised users will pay due care and attention to protect company's information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- permission of the information owner
- the risks associated with loss or falling into the wrong hands
- how the information will be secured during transport and at its destination.

2.2 Acceptable use of information systems

Use of the company's information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people.

2.3 Information System Owners

System owners who are responsible for information systems are required to ensure that:

1. Systems are adequately protected from unauthorised access.
2. Systems are secured against theft and damage to a level that is cost-effective.
3. Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
4. Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
5. Data is maintained with a high degree of accuracy.
6. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
7. Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
8. Any third parties entrusted with company's data understand their responsibilities with respect to maintaining its security.

2.4 Personal Information

Authorised users of information systems are not given rights of privacy in relation to their use of company's information systems.

2.5 The University will take legal action to ensure that its information systems are not used by unauthorised persons.

3. Ownership

3.1 Rocket Minds has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.