Information Security Policy

Policy:

It is the established policy of RedboxVR Ltd to operate within the requirements of a documented Information Security Policy statement as a means to comply with all statutory, regulatory and contractual requirements, and, to protect the interests, property and information of the company, and of its clients and employees, against threats or loss.

In pursuance of this policy its stated requirements have been implemented together with the specified requirements of the company's associated information security and computer system access management work instructions.

The purpose of this Information Security Policy statement is to describe how security is implemented, to give guidance to our employees whose actions can affect the confidentiality and integrity of the business, its product and services, and, to illustrate the overall commitment to security issues within our company.

This Information Security Policy statement, which is not intended as a stand-alone document, is supported by detailed process operating procedures and where appropriate by quality management system Work Instructions (WI), to form a set of working documents, which define our company's security activities.

The Information Security Policy is maintained by audit and review, and by the methods described in the quality manual, in order to provide effective assurance that all aspects of company, employee and customer specified security requirements are being implemented.

It is company policy to ensure that the use of documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services and fax machines must be controlled to prevent unauthorized use and to reduce security risks.

All employees have a responsibility not to compromise the company, e.g. by sending defamatory or harassing electronic mail, or by making unauthorized purchases, and, must also be aware that the confidentiality and integrity of information transmitted by E-mail or facsimile may not be guaranteed.

Access by employees to the Internet is restricted to business use only and any breach of this policy will result in disciplinary action being taken.

The Manager is responsible for managing information security, and he will also ensure that all employees are trained to understand, implement and maintain the security objectives set out in this Security Policy and as detailed in the company's security related Work Instructions.

We publish this policy statement in the knowledge that the security of our company and its employees, products and client services, and our on-going good security reputation, depend upon the every day security awareness and actions of all our employees, both on-site and off-site.

I am wholly committed to this Information Security Policy, and hereby state that it is the responsibility of every individual employee of the company to ensure that all security plans, standards, procedures, work instructions and actions fully meet with agreed company and customer requirements.