Caravel
LEADING THE WAY IN PROJECTS

Security Policy

Caravel recognises that security is a top priority for all. By carrying out our activities in accordance with this policy we will protect the interests of the company, its employees, Associates, Clients, Suppliers and others who entrust articles and information to Caravel from all forms of security threat, whether physical or electronic, to the extent consistent with meeting legal, contractual and moral obligations.

This will be achieved by ensuring that:

- A security management system is created and integrated with the company quality management system in accordance with the AS/NZS ISO/IEC 27001:2006 Information Security Management standard.
- Security threats are identified, assessed and treated as required and then reviewed regularly with those concerned.
- The requirements for security management are communicated to those responsible to as to inform and educate them.
- All those responsible for performing security management tasks shall be contracted to perform that task to the extent allowed by law.
- Internationally recognised standards for security management such as ISO17799 shall form the basis for the establishment and maintenance of the security management plan.
- Trusted computing systems conforming to the internationally accepted Common Criteria standards (previously TCSEC) be applied as appropriate.
- If necessary forensically defensible records shall be created and stored so as to prove Caravel's compliance to its Security Management System.
- Clients and others shall be given the opportunity to choose on a commercial basis the level of security they require.

Paul Myers
Managing Director