

# Data Security Policy

## Information Security

We will take all reasonable steps to ensure the information you provide us remains secure and confidential. We take a range of measures to protect your personal information from:

- ▶ Misuse, interference and loss; and
- ▶ Unauthorised access, modification or disclosure

## Training

We train our staff to respect the confidentiality of client information and the privacy of individuals.

## System Access and Password Protection

Our Information Record Systems have multi-layer permission access which includes password protection and permission level access.

## Software Protection

Our software is protected as follows:

- ▶ Our network is protected using a firewall which governs internal and external access rights;
- ▶ Our emails are filtered to determine email rights, spam control and content control;
- ▶ Data is kept virus free by antivirus software which controls virus definition to all machines;
- ▶ Data access is controlled by permissions software; and
- ▶ All data is backed up both onsite and offsite.

## Hardware Protection

Our hardware is protected as follows:

- ▶ Our servers are located in dedicated, secure IT facilities. All access to IT equipment is strictly controlled.
- ▶ Our servers are protected from failure by redundant hardware features.
- ▶ All disk systems are redundant using some form of RAID; and
- ▶ Sites contain backup UPS systems to protect against power loss or power anomalies.

# Data Security Policy

## Policy on portable electronic devices

In order to protect personal information from misuse, interference and loss, we do not, as a matter of practice, issue staff with laptops, tablets, mobile phones or other portable electronic devices. Where our staff utilise their own portable devices, they are subject to our remote access and acceptable IT use policies.

## Retention and disposal

We adopt record management practices in accordance with legislative requirements and policies and guidelines on recordkeeping and management of electronic communications.

Where information is lawfully destroyed this is done by secure means of disposal.

## Clients and 3rd Parties

All client and third-party information accessed and used by our on-hired personnel during the course of their assignments with our clients is protected from disclosure or unauthorised use by:

- ▶ The confidentiality and privacy obligations that are contained in our contracts signed by such on-hired personnel; and
- ▶ The obligations to comply with all client policies and procedures, including those in relation to confidentiality and privacy that are contained in our contracts signed by such on-hired personnel