Data & Information Technology Security Policy

1. Purpose

The main purpose of this policy is to inform staff and managers of their obligatory requirements for protecting technology and information assets. This policy specifies the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit our internal systems and processes for compliance with the policy.

This Policy may be read in conjunction with our privacy policy.

2. What Needs Protecting?

The key assets requiring protection through a security policy have been identified as:

2.1. Hardware, including but not limited to:

CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers.

2.2. Software, including but not limited to:

Source programs, object programs, utilities, diagnostic programs, operating systems, communication programs.

2.3. Data, including but not limited to:

During execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.

2.4. People, including but not limited to:

Users, administrators, hardware maintainers.

2.5. Documentation, including but not limited to:

On programs, hardware, systems, local administrative procedures.

2.6. Supplies, including but not limited to:

Paper, forms, ribbons, magnetic media.

For convenience we have broken these assets down into specific business areas which we need to protect – Physical Security, IT Security, and Intellectual Property.

3. Physical Security

These are the means by which we ensure that premises and documents are kept secure from unauthorised access.

3.1. Protecting the Building

- Burglar alarm (including service notifying designated points of contact and/or security company when triggered)
- Swipe card for access to main office door [include who has access or where list can be found]
- Locked internal door preventing access to main office area
- Security cameras
- Staffed reception area to vet and sign in visitors

3.2. Protecting Documents in the Office

Documents are protected from unauthorised access by:

- Locked cabinet for storage of all paper documents
- Locked, fireproof safe for overnight storage of important client documents or cheques
- Clear desk policy to avoid documents left on desks and on view overnight
- Confidential paperwork is placed in secure containers and shredded once no longer required
- All documents are scanned and shredded within one day of receipt

If any IT administration processes such as back up of data, support of the various IT systems and data storage are outsourced the specific procedures will be followed and due diligence on the firms concerned carried out.

Cleaners or cleaning companies whose staff can access client data will also be subject to the same due diligence.

Our procedures will include:

- Understand the third party's data security procedures
- Carry out appropriate due diligence on those third parties, including their security arrangements and staff recruitment policies
- Consider whether they should allow third parties unsupervised access to the office or records.

4. IT Security

These are the means by which we ensure that any electronically stored information is kept secure from unauthorised access.

4.1. Protecting Infrastructure and Hardware

Servers, personal computers and laptops are protected by external attack from unauthorised access, viruses and Trojan Horses by:

- Hard password policy on all servers, personal computers and laptops. All passwords must be at least eight characters long, and include one capital letter and one number and one special character.
- Anti virus - we have a firewall enabled and VLAN access to our Wi-Fi. We run AV and run daily scans on our machines
- All incoming emails are scanned by an external agency before they are delivered onto the network
- All incoming emails are filtered for SPAM and quarantined for checking before they are delivered onto the network
- Remote access to server (explain including details on security of connection. Note - remote desktop connection to server or PC without a secure VPN connection may not be viewed as sufficiently secure)
- Wireless network is secured via WPA2
- The Acceptable Use Policy prohibits staff from opening emails or attachments from unknown sources
- Staff may not undertake personal work on personal computers

4.2. Use of Personal Devices

Staff may use personal devices for work but only where this has been agreed in advance and the following points have been considered:

- Being clear with staff about which types of personal data may be processed on personal devices and which may not
- Using a strong password to secure their devices
- Using public cloud-based sharing and public backup services, which you have not fully assessed, with extreme caution, if at all

4.3. Disposal of Hardware

Consideration is given to the disposal of computers, laptops, memory sticks, disks, etc:

- If a third party is used for the disposal of data, the firm will satisfy itself with their security and staff vetting arrangements
- Disposal of a computer - the hard drive will be wiped with specialist software or removed and destroyed sufficiently so that information cannot be accessed by an authorised person

5. Protecting Intellectual Property

These are the additional means by which we ensure that our intellectual property, and the goodwill of the business, is kept secure from unauthorised access.

5.1. Staff

Staff are made aware of their obligations through:

- Acceptable Use Policy/employment contract/self employed adviser contract
- Induction process which covers this security policy
- Updates to changes on security policy

Use of all company equipment is governed by the Acceptable Use Policy which ensures that:

- All company equipment is logged against staff member
- Laptops must be locked away and not left in insecure locations (eg. in cars overnight)
- Files may not be taken home
- Staff may not undertake work on personal computers
- Staff may not email work to personal email accounts

6. Security Violations/Data Compromise Reporting Policy

All staff are under an obligation to report any incident which you may feel violates the security of the firm by informing the IT by phone or email.

Equally, all staff are aware of the need to report any data compromise incidents. These can include:

- Loss of laptop

- Loss of client data either in paper form or electronic
- Loss of memory sticks/disks/USB pens etc
- Unauthorised persons in back office area where data stored
- Client information passed onto unauthorised third party

All incidents should be reported immediately to the IT Team.