1 Scope of the Policy

This Policy Document encompasses all aspects of security surrounding confidential company information and client information. It must be distributed to all company employees. All company employees must read this document fully and understand this policy in its entirety. This document will be reviewed and updated by Management on a triennial basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2 Information Security Policy

ABCconsulting handles sensitive client and customer information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect privacy, to ensure compliance with various regulations and to guard the future of the organisation. ABCconsulting commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process information so that we can meet these promises.

Employees handling sensitive data should ensure:

(a) Handle Company and client information in a manner that fits with their sensitivity.
(b) Limit personal use of the Company information and telecommunication systems and ensure it doesn't interfere with your job performance.
(c) The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.
(d) Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
(e) Do not disclose personnel information unless authorised.
(f) Protect sensitive information.
(g) Keep passwords and accounts secure.
(h) Request approval from management prior to establishing any new software or hardware, third party connections, etc.
(i) Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval.
(j) Always leave desks clear of sensitive data and lock computer screens when unattended.
(k) Information security incidents must be reported, without delay, to the legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from the legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew.

2 Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the ABCconsulting established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

(a) Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
(b) Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
(c) Employees should take all necessary steps to prevent unauthorised access to confidential data.
(d) Employees should ensure that technologies should be used and setup in acceptable network locations.
(e) Keep passwords secure and not share accounts.
(f) Authorised users are responsible for the security of their passwords and accounts.
(g) All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
(h) Because information contained on portable computers is especially vulnerable, special care should be exercised.
(h) Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless authorised to do so.
(i) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3 Disposal of Stored Data

All data must be securely disposed of when no longer required by the Company, regardless of the media or application type on which it is stored.

An automatic process must exist to permanently delete on-line data, when no longer required.

The Company will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded so they cannot be reconstructed.

The Company will have documented procedures for the destruction of electronic media. These will require:

(a) All data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped.
(b) If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

4 Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

(a) All information, applications, and infrastructure components are appropriately secured to prevent unauthorized access, use, disclosure, modification, damage or loss of data.
(b) Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
(c) Distribute this security policy document to all company employees to read.
(d) Company security policies must be reviewed triennially and updated as needed.

5 System and Password Policy

All users, including contractors and vendors with access to the Company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

(a) A system configuration standard must be developed along industry acceptable hardening standards.
(b) System configurations should be updated as new issues are identified.
(c) System configurations must include common security parameter settings.
(d) The systems configuration standard should be applied to any new systems configured.
(e) All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into the Company network and all unnecessary services and user/system accounts have to be disabled.
(f) All unnecessary default accounts must be removed or disabled before installing a system on the network.
(g) Security parameter settings must me set appropriately on System components.
(h) All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
(i) All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
(j) Any insecure protocols, daemons, services in use must be documented and justified.
(k) All user must use a password to access the company network or any other electronic resources.
(l) All user ID's for terminated users must be deactivated or removed immediately.
(m) The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled until the administrator enables the account.
(n) Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.
(o) All non-console administrative access will use SSL before the administrator password is requested.
(p) System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands.
(q) Administrator access to web based management interfaces is encrypted using strong cryptography.
(r) The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:
- Be as long as possible (min of 8 characters include numbers and special characters).
- Include mixed-case letters, if possible.
- Include digits and punctuation marks, if possible.
- Not be based on any personal information.
- Not be based on any dictionary word, in any language.

5 Anti Virus Policy

(a) All machines must be configured to run the latest anti-virus software as approved by the Company. The preferred application to use is Kaspersky Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.

(b) The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
(c) Removable media (for example USB and others) not be used.
(d) All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/requirements (6 months)
(e) Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
(f) End users must not be able to modify and any settings or alter the antivirus software
(g) E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

5 Patch Management Policy

(a) All Workstations, servers, software, system components etc. owned by the Company must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
(b) Wherever possible, all systems, software must have automatic updates enabled for system patches released from their respective vendors.
(c) Any exceptions to this process have to be documented.

6 Remote Access Policy

Remote access privileges are not permitted for any employee, freelance consultants or anyone associated with ABCconsulting.

7 Responsibilities

Any concerns relating to a breach of the Policy should be reported directly and immediately on discovery (if possible) to:

Alan Cardew Legal owner of ABCconsulting
Beverley Cardew Managing partner of ABCconsulting

8 Communication and Review

This policy will be communicated to all employees during induction, and at staff meetings. This policy will be reviewed on a triennial basis or when a material change in law dictates.