CAMPASPE COLLEGE of Adult Education Echuca

# RISK MANAGEMENT
## GENERAL COMPUTER SECURITY
**8.10**

### Policy Rationale
- Data security is vital to maintain the business operations of CCAE and to maintain the data enrolment, financial and statistical systems that are critical for payment claims from clients: people, business and governments.
- To provide elements of technical knowledge and guidelines designed to provide an orderly system of checks should the computer system appear to be compromised.

### Policy Aims
To establish and maintain a CCAE computer network that is secure from internal and external hacking, is dynamic and serves the administration and student purposes for which it was intended.

### Policy – Computer Security Co-ordinator
This is the person who is responsible for drawing together the computer security issues within CCAE. This includes:
- seeing that a security policies and procedures manual has been written.
- ensuring that all the items in the Guideline are being followed.
- arranging staff training.
- clarifying the computer security roles and responsibilities of staff.
- keeping asset register up-to-date.
- making sure that all operating manuals, installation disks and protocols are catalogued and stored safely.
- developing a policy on staff access to computer data and systems.
- coordinating the application for storage and use of digital certificates.
- knowing how and when to seek the advice of an IT technical support person and/or systems administrator.

### Procedure – Access Control
One of the key features of data security is that only certain people should see some types of information such as sensitive financial or statistical information. The use of passwords forms part of a CCAE's 'right to know' to ensure the privacy of client data and to comply with national privacy principles.

Because of the level of trust that routinely exists within CCAE, passwords are often not managed well – until someone without due authorisation abuses their privilege. Consequently:
- CCAE staff can choose passwords to provide them with their appropriate level of access.
- staff will remain responsible for their own passwords and are not share them with other CCAE members.
- restricted access will protect CCAE against misuse of financial data and lessens the risk of accidental change or deletion.
- passwords can be implemented for the operating system, application software, files within software and email.
- the systems administrator will keep a list of passwords.

### Procedure – Disaster Continuance Plan
A disaster continuance plan will help to minimise the disruption and the risk and inconvenience to CCAE when the computer system has gone down and staff have to revert to a paper-based system.

The critical functions, for which computers are used in CCAE, but which need to continue when a computer 'disaster' occurs are:
- making appointments for clients: [telephone message book to be used]
- issuing clients with receipts: [receipt book to be used]
- issuing clients with invoices: [invoice details to be noted in invoice booklet for later reference]
- enabling the staff to provide adequate enrolment and costing information while not having access to electronic records: [staff to refer to brochures in foyer for course information and to prepared enrolment forms in filing cabinet in Reception area]

**Adoption Date:** 20 June 2012
**Review Date:** 01/06/2014
**Version Control:** V1-18/08/11 V2-01/06/12

## Procedure – Reception and Staff Desk Security

Data security in reception and on staff desks is more about staff behaviour than technical matters. Some staff like their computer screens visible to clients during discussions and in some cases need to show the screen to the client to confirm data entries.

Receptionists need to be mindful that clients do not have visual access to confidential information on computer screens at the 'front desk'. There are various methods by which the information can be kept confidential. Some have to do with screen positioning, but screensavers and the use of a function key which instantly closes down an open file are useful technical options.

This is important even if it appears unlikely that clients will maliciously use the information they happen to access. Consequently:

- Office computers are to have screen savers activated – after 2 minutes of lack of computer use
- Office computers are to have a desktop shortcut which turns on the screensaver immediately.

## Procedure – Back-ups and Restoration

Having a successful back-up procedure is absolutely essential. Loss of client and financial data will cost CCAE severely, and the loss of enrolment data will be a significant time waster if records have to be reconstructed. Data can be lost through human error, software crashes and hardware problems.

It is critical to make regular back-ups of all CCAE data in case any of these occur. In order to do a back-up, three things must be considered:

- back-up procedure;
- back-up medium and software to be used; [There are various types of back-up media which include DVDs, CD-ROMs, magnetic tape, zip drives, memory cards and portable hard disks. The use of RAID hard drives also merits consideration].
- how CCAE back-up data can be restored.

Restoration includes:
who phones the technical support person [VASS/VETtrak administrator]
who reinstalls the operating and application software [IT Trainee Technician]
who reloads the data [IT Trainee Technician and VASS-VETtrak administrator]
what CCAE should do to keep functioning in the meanwhile [see Disaster Continuance]

A related matter is the archiving of files that are no longer active. CCAE might have to refer to this data in the future when computer hardware and software is different. Archived material needs to be 'future proofed' so that it remains accessible. As a consequence the following apply:

- Back-ups of data done daily [IT Trainee Technician]
- Back-ups of data stored offsite [Manager]
- Back-up procedure tested (by performing a restoration of data) at specified intervals [IT Trainee Technician and VASS-VETtrak administrator]

## Procedure – Viruses

Viruses interfere with computer systems and can cause the whole system to crash. The more time one spends on the Internet, especially with a permanently connected broadband, the more likely one is to download viruses. This can have a major impact on CCAE, especially if financial data are lost or altered. Viruses can also impede access to the Internet by clogging the network and can damage the reputation of CCAE if the virus distributes itself to everyone in CCAE's electronic address book.

There are various types of 'viruses' which are more correctly called 'malicious code' and they include viruses themselves, worms and trojan horses. They can cause minor annoyances or catastrophic system crashes. The risk of virus infection can be minimised by two means:

- having a process in place which minimises the risk of downloading a virus; and
- using regularly updated anti-viral software.

There are other sorts of programs which can be considered together with viruses. These are spyware and spam. The former refers to small programs which download themselves onto a computer while CCAE are viewing a web page. They can transmit information about CCAE use of the computer to other sites. Spam is nuisance email. Consequently the following will be adopted:

- Anti-viral software installed on all computers.
- Automatic updating of viral definitions enabled (daily if possible by IT Trainee Technician).
- Staff computers are to be kept up-to-date with current versions and the latest security patches for the software used.

## Procedure – Fire Walls

A firewall is an electronic mechanism that blocks unauthorised access into a computer system. These can be in the form of software or hardware. Various programs, some of which are freely available on the Internet, can be installed to protect 'hackers' from getting into CCAE computer network.

Hackers can steal information and can cause mischief within the CCAE computer system and this can lead to the loss of data. CCAE should consider the need for a firewall in the same category as the need for anti-viral protection. They are essential for the long-term preservation of CCAE data.

Like viruses, unwanted intruders can crash CCAE system. CCAE might think it improbable that others would want to steal CCAE data, but it is less likely that CCAE will be specifically targeted by hackers than CCAE being 'discovered' by their use of programs which 'roam' the Internet until they randomly find vulnerable computers (technically, those with open 'ports').

Unless CCAE is using a standalone computer, it is advisable to install a hardware firewall for extra security. Another major advantage of hardware firewalls is that they provide a hub for a local area network. Consequently:

- Hardware and/or software firewalls will be installed.
- Hardware and/or software firewalls will be tested.
- Firewalls will help prevent client information from appearing on the Internet.
- Firewalls are essential for anyone using the Internet.

## Procedure – Network Maintenance

The importance of some routine maintenance issues is self-evident. This might mean performing 'maintenance' work on regular occasions such as: running a program which 'cleans up' file system errors and temporary files; running a 'defragmentation' utility program; updating software; and downloading operating system and other program patches.

It includes looking after the equipment itself, hardware and software. More specifically, maintenance includes the following:

- physical protection of CCAE computers, e.g. protection against theft by the use of locks.
- protecting CCAE computer against environmental damage such as heat, water and dust.
- keeping CCAE computer programs running efficiently.
- updating the memory capacity of the CCAE server.
- installing a UPS to protect CCAE server.
- running a file 'defragmentation' utility program.

**Installing an Uninterruptible Power Supply (UPS)**

A UPS is a device that contains batteries to enable computers to shut down smoothly when the main electricity supply suddenly cuts out. This is important so that data being processed when the blackout occurs is not lost. The UPS will also help with power surges which can cause hardware damage. However, they do not generally generate sufficient power during a prolonged blackout.

- on the main sever a UPS will be installed.
- on the routers a UPS will be installed.
- on other workstations in the CCAE, a simple surge protector will suffice.

## Evaluation

This policy will be reviewed bi-annually