

# **Computer Security Policies and Procedures Manual**

## **A Template**

**1<sup>st</sup> edition**

**Date manual developed:**

**Date last updated:**

# Contents

1.	STAFF ROLES AND RESPONSIBILITIES .....	1
2.	ACCESS CONTROL.....	5
3.	CONSULTING ROOM SECURITY.....	6
4.	DISASTER RECOVERY PLAN.....	7
5.	ASSET REGISTER .....	10
6.	BACK-UP AND RESTORING PROCEDURES .....	16
7.	VIRUS CHECKING .....	19
8.	FIREWALLS .....	19
9.	MAINTENANCE.....	20
10.	SECURE ELECTRONIC COMMUNICATION .....	21

## **How to use this template**

This document is a template to be completed by the practice computer security coordinator with assistance from other practice staff or technical support person. It could form a part of the general practice policies and procedures manual.

The template is designed to be completed electronically. It should be used in conjunction with the GPCG computer security guideline and check-list.

1. Save this document on your hard drive.
2. Place your cursor where you want to add information.
3. Where there are not enough boxes you can select the table, copy and paste it.
4. Similarly, where there are not enough rows or lines in a table you can insert additional ones.
5. There may be items that are not relevant to your practice (e.g. you may not have a scanner). These items can be either deleted or left blank in case they are needed in the future.
6. Some examples have been provided in shaded areas to help clarify what you might include in that section.
7. There may be technical information that you do not know. Your technical support person will be able to assist you in completing some sections of the manual.
8. You may wish to import into this manual (by copying and pasting) the policies and procedures proformas and security check-list contained in the GPCG Guideline which can also be downloaded from the GPCG website.
9. Put the date you complete the document on the front page.
10. Remember to modify the manual when there are changes to staff responsibilities or the computer set-up at the practice. Change the date on the front page to show when the manual was last updated.

## **Acknowledgement**

Full acknowledgement for the GPCG computer security guideline and check-list, of which this template is a part, can be found in the guideline itself. However, special thanks are due to Ms Leslie Stanger of the Monash Division as well as several other divisions of general practice that provided significant input into the design of this template.

A/Prof Peter Schattner  
Monash University  
February 2004

## 1. Staff roles and responsibilities

Practice computer security co-ordinator

**Person(s) responsible:**

**Role:**

**Responsibilities:** (See Appendix A of the GPCG Guideline for suggested responsibilities)

### Other staff roles and responsibilities

Other staff may also be assigned tasks related to computer security.

Task	Person(s) responsible
e.g. do back-ups	
e.g. update software	

### Technical Support

Name	Support for	Contact Details

## 2. Access control

Staff should only have access to the systems and information required by their role in the practice. Restricting access reduces the opportunity for accidents and errors. Staff should be properly trained in the software before they are given access to it.

All staff should create their own passwords, and should be responsible for changing them periodically and keeping them secure.

<b>Staff Member</b> e.g. practice nurse	<b>Program</b> e.g. name of prescribing software	<b>Access Level</b> e.g. clinical information only or full user access

### 3. Consulting room and 'front desk' security

Record the installation of screen savers and/or other automated privacy protection devices (see column 3 below).

Computer	Screensaver installed	Shortcut/activation key  (this is a function key or combination of keystrokes which, when pressed, will activate the screen saver immediately)

## 4. Disaster recovery plan

This is a written plan which explains what should be done when the computer system, or any part of it, goes down or does not function properly for some reason.

### **Step 1** Switch to manual procedures for critical practice functions

For each critical function in the practice there should be a contingency plan so that the practice can continue to operate in the event of a disruption to computer systems. This is the 'business continuity' part of the plan. Critical functions can be divided into administrative and clinical ones.

<b>Function 1</b> e.g. billing patients	
<b>Contingency Plan</b> e.g. <ul style="list-style-type: none"><li>• Swipe Medicare cards</li><li>• Issue manual receipts</li><li>• Retain copies of all receipts to be entered into the system later</li></ul>	
<b>Person responsible</b> e.g. receptionists	

<b>Function 2</b>	
<b>Contingency Plan</b>	
<b>Person responsible</b>	

<b>Function 3</b>	
<b>Contingency Plan</b>	
<b>Person responsible</b>	

## **Step 2 Make an assessment of the computer problem**

Examples might include:

- Writing down any error messages
- Noting anything that has changed since the system last worked correctly
- Checking that all power and network connections are plugged in.

## **Step 3 Perform remedial action (with or without technical support)**

This step might involve the restoration of data from the most recent back-up.

## **Step 4 Test the functionality of all systems**

## **Step 5 Return to normal practice procedures and enter data recorded manually during downtime**

## **Step 6 Assess the reason for the problem, how the recovery was done, update the computer setup and document any important lessons.**

### Remedial action for 'disasters'

These are some common computer 'disaster' scenarios in general practice. Complete the boxes and add any additional items from your experience.

#### Server failure

<b>Immediate action</b> Implement contingency plan	
<b>Recovery procedure</b> e.g. Write down any error messages Check that no computers are accessing the server Reboot the server If the server does not reboot correctly: <ul style="list-style-type: none"><li>• Write down any error messages</li><li>• Call technical support</li></ul> If the server does reboot correctly: <ul style="list-style-type: none"><li>• Check that the last transactions entered are correctly recorded on the system</li></ul>	



<b>Person responsible</b> e.g. practice computer security co-ordinator	
---	--

### Virus detected

<b>Immediate action</b>	
<b>Recovery procedure</b>	
<b>Person responsible</b>	

### Power failure

<b>Immediate action</b>	
<b>Recovery procedure</b>	
<b>Person responsible</b>	

### File corruption or loss

<b>Immediate action</b>	
<b>Recovery procedure</b>	
<b>Person responsible</b>	

### Network problem

<b>Immediate action</b>	
<b>Recovery procedure</b>	
<b>Person responsible</b>	

## 5. Asset Register

### Hardware

#### Computers: server

	Server/Computer 1
Name	
IP Address	
Location	
CPU	
RAM	
HDD	
CD/DVD	
Internal devices e.g. modem, network card	
External devices attached e.g. printer, scanner	
Operating System (OS)	
OS Serial Number	
Make	
Model	
Serial Number	
Supplier	
Cost	
Purchase Date	
Warranty	
Support	

## Other Computers

	Computer 2	Computer 3
<b>Name</b>		
<b>IP Address</b>		
<b>Location</b>		
<b>CPU</b>		
<b>RAM</b>		
<b>HDD</b>		
<b>CD/DVD</b>		
<b>Internal devices</b> e.g. modem, network card		
<b>External devices attached</b> e.g. printer, scanner		
<b>Operating System (OS)</b>		
<b>OS Serial Number</b>		
<b>Make</b>		
<b>Model</b>		
<b>Serial number</b>		
<b>Supplier</b>		
<b>Cost</b>		
<b>Purchase date</b>		
<b>Warranty</b>		
<b>Support</b>		

## Peripherals and Network Equipment

	<b>Printer 1</b>	<b>Printer 2</b>	<b>Printer 3</b>
<b>Name</b>			
<b>IP Address</b>			
<b>Location</b>			
<b>Make</b>			
<b>Model</b>			
<b>Serial number</b>			
<b>Supplier</b>			
<b>Cost</b>			
<b>Purchase date</b>			
<b>Warranty</b>			
<b>Support</b>			

	<b>Scanner</b>	<b>Modem</b>	<b>Network Hub/Router</b>
<b>Name</b>			
<b>IP Address</b>			
<b>Location</b>			
<b>Make</b>			
<b>Model</b>			
<b>Serial number</b>			
<b>Supplier</b>			
<b>Cost</b>			
<b>Purchase date</b>			
<b>Warranty</b>			
<b>Support</b>			

## Network

<b>Type (e.g. client server, peer to peer)</b>	
<b>IP Address Range</b>	
<b>Subnet Mask</b>	
<b>Domain/Workgroup</b>	
<b>WINS Server IP</b>	
<b>DNS Server IP</b>	
<b>DHCP Server IP</b>	
<b>Gateway</b>	
<b>Number of nodes</b>	
<b>Locations of nodes (and identification)</b>  Could be cross-referenced to network diagram	1.  2.  3.
<b>Maintenance details</b>	

## Software Database Shares

These are the databases or other files that reside on the server and are accessible by other workstations in the practice.

<b>Shared Database Name</b> e.g. <a href="#">\\Server\C\program</a>

## Network Diagram

If you have hubs and/or routers, a network diagram can assist in locating equipment and diagnosing problems.

All equipment, including printers, should be shown on the diagram.

## Email

<b>Practice email address</b>	
<b>Incoming Mail Server</b> e.g. POP3	
<b>Outgoing Mail Server</b> e.g. SMTP	
<b>Other details</b>	

## Internet

<b>Provider (ISP)</b>	
<b>Dial-up number</b> (if appropriate)	
<b>Access plan</b>	
<b>Proxy server</b>	
<b>TCP/IP address</b>	
<b>DNS</b>	
<b>Secondary DNS</b>	
<b>Modem type</b>	

<b>Support details</b>	
------------------------	--

## Software

Include all clinical and practice management software, as well as email, firewall, back-up, virus checking and other utilities.

<b>Name/Version</b>	
<b>Description</b>	
<b>Serial numbers/Licence codes</b>	
<b>Which computers</b>	
<b>Location of media</b>	
<b>Location of manuals</b>	
<b>Location of licence codes and agreements</b>	
<b>Date purchased/ Upgraded</b>	
<b>Supplier</b>	
<b>Support details</b>	

<b>Name/Version</b>	
<b>Description</b>	
<b>Serial numbers/Licence codes</b>	
<b>Which computers</b>	
<b>Location of media</b>	
<b>Location of manuals</b>	
<b>Location of licence codes and agreements</b>	
<b>Date purchased/ Upgraded</b>	
<b>Supplier</b>	
<b>Support details</b>	

Note: Original software media and manuals should be stored securely

## 6. Back-up and restoring procedures

Any data and files that change should be backed-up. This includes practice management and clinical systems data as well as documents, email files, Internet favourites and bookmarks, etc. You may need different back-up and recovery procedures for each of these.

You do not need to back-up your operating system or programs as these can be restored from the original CDs.

Note: You should also keep a copy of this manual backed up and offsite so that systems can be restored in the event of a theft or fire at the practice.

<b>Back-up procedure</b> e.g. for an automated back-up At the end of the day: <ul style="list-style-type: none"><li>• Insert back-up media for the day in the server</li><li>• Ensure that all other computers have logged out of the server</li></ul> Next morning: <ul style="list-style-type: none"><li>• Check for any error messages on the server</li><li>• Check that the files on the back-up media look correct (name, size and date)</li><li>• Remove back-up media and store in secure location</li></ul>	1.  2.  3.  4.  5.
<b>When</b> E.g. daily	
<b>Person Responsible</b> E.g. receptionist	
<b>Media cycling</b> E.g. <ul style="list-style-type: none"><li>• Daily disks/CDs</li><li>• Weekly</li><li>• Monthly</li><li>• Annual (end of financial year)</li></ul> See an example below	
<b>Offsite Storage procedure</b>	



## Back-up media cycling

Sometimes problems occur with data or files (or even back-ups) that are not noticed immediately. It is useful to have a series of back-ups so that you can restore a file from a point before the problem occurred. Having a system of daily, weekly, monthly and annual back-ups enables you to do this.

**Daily back-ups:** Have a different tape/disk/CD for each day of the week. Label them Mon, Tue, Wed, etc. Monday's tape is always used on Monday night. The data from the previous Monday is overwritten. The weekly, monthly and annual back-ups replace these daily back-ups.

**Weekly back-ups:** On a particular night of the week (e.g. Friday) have a different tape/disk/CD for each week of the month (labelled Fri#1, Fri#2, etc.). These replace the daily back-ups. Fri#1 is used on the first Friday of the month, etc.

**Monthly back-ups:** Have one tape/disk/CD labelled "Monthly". This should be used once every month, for example, on the first Monday of the month (replacing the daily back-up).

**Annual back-up:** This should be done at the end of the financial year. It should be done to a CD or tape that can be retained for at least a year.

### Worked example for a practice working 7 days a week

The following table can be adjusted and printed each month as a reminder of what tape/disk/CD to use and as record that the back-up has been done and checked. If the working week does not begin on a Monday, the monthly back-up can replace the Monday back-up in Week 2.

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
<b>Week1</b>	Monthly ÿ Done ÿ Checked	Tue ÿ Done ÿ Checked	Wed ÿ Done ÿ Checked	Thu ÿ Done ÿ Checked	Fri#1 ÿ Done ÿ Checked	Sat ÿ Done ÿ Checked	Sun ÿ Done ÿ Checked
<b>Week2</b>	Mon ÿ Done ÿ Checked	Tue ÿ Done ÿ Checked	Wed ÿ Done ÿ Checked	Thu ÿ Done ÿ Checked	Fri#2 ÿ Done ÿ Checked	Sat ÿ Done ÿ Checked	Sun ÿ Done ÿ Checked
<b>Week3</b>	Mon ÿ Done ÿ Checked	Tue ÿ Done ÿ Checked	Wed ÿ Done ÿ Checked	Thu ÿ Done ÿ Checked	Fri#3 ÿ Done ÿ Checked	Sat ÿ Done ÿ Checked	Sun ÿ Done ÿ Checked
<b>Week4</b>	Mon ÿ Done ÿ Checked	Tue ÿ Done ÿ Checked	Wed ÿ Done ÿ Checked	Thu ÿ Done ÿ Checked	Fri#4 ÿ Done ÿ Checked	Sat ÿ Done ÿ Checked	Sun ÿ Done ÿ Checked
<b>Week5</b>	Mon ÿ Done ÿ Checked	Tue ÿ Done ÿ Checked	Wed ÿ Done ÿ Checked	Thu ÿ Done ÿ Checked	Fri#5 ÿ Done ÿ Checked	Sat ÿ Done ÿ Checked	Sun ÿ Done ÿ Checked

<b>Restoring procedure</b> E.g. <ul style="list-style-type: none"> <li>• Locate back-up media for the previous day</li> <li>• Insert back-up media in the server</li> <li>• Ensure that all other computers have logged out of the server</li> <li>• Perform restore for particular system/files</li> <li>• Check that the system/files restored look correct (name, size and date)</li> <li>• Check that the system functions correctly</li> <li>• Remove back-up media and store in secure location</li> </ul>	1.  2.  3.  4.  5.
<b>When</b> E.g. as required	
<b>Person Responsible</b> E.g. practice computer security co-ordinator	

<b>Check/Test Recovery procedure</b> E.g. Restore file/system on a different computer to the one on which the system normally runs Check that the restored system functions correctly Compare the records to ensure that the restored files contain the latest information	1.  2.  3.  4.  5.
<b>When</b> E.g. quarterly and when system changes are made	
<b>Person Responsible</b> E.g. practice computer security co-ordinator	

## 7. Virus Checking

<b>Software, name and version</b> (See software register)	
<b>Computers</b>	
<b>Support</b>	
<b>Upgrade procedure</b>	
<b>Person responsible</b>	
<b>Annual subscription renewed</b>	

## 8. Firewalls

<b>Name and version</b>	
<b>Hardware</b>	
<b>Software</b>	
<b>Maintenance required</b>	
<b>Support</b>	

## 9. Maintenance

There are certain maintenance procedures which, if performed regularly, will help to keep computers and other equipment running smoothly.

These procedures include:

- Adding the latest patches to your operating system and application software
- Upgrading software
- Deleting temporary files
- ‘Defragging’ the hard disk
- Cleaning around the back of computers and other equipment so that dust, etc. does not accumulate near the fans and power supplies.

<b>Item 1</b>	
<b>Person responsible</b>	
<b>Frequency</b>	
<b>Procedure</b>	

<b>Item 2</b>	
<b>Person responsible</b>	
<b>Frequency</b>	
<b>Procedure</b>	

### Maintenance Log

(Attach as a separate page to be completed as maintenance is performed)

<b>Date</b>	<b>Task performed</b>	<b>By whom</b>

## Uninterruptible power supply (UPS)

<b>Type</b>	
<b>Equipment attached</b>	
<b>Maintenance required</b>	
<b>Battery life</b>	
<b>Support</b>	

## 10. Secure Electronic Communication

If more than one method is used (for communication with different health organisations) each one should be detailed separately.

<b>Encryption method used by practice</b>	
---	--

*End of doc.*