## **1.0 Computer Information Security**

Policy

WGPN has systems in place to protect the privacy, security, quality and integrity of the data held electronically. Doctors and staff are trained in our security policies and procedures.

The IC&T Manager has designated responsibility for overseeing the maintenance of our computer security and our electronic systems.

All staff have access to a computer to conduct various administration tasks and document clinical care. Staff log in under their own username and password to record and document activities they have undertaken.

WGPN ensures that:

* computers are only accessible via individual password access to those who have appropriate levels of authorisation.
* computers have screensavers or other privacy protection devices enabled to prevent unauthorised access to computers.
* servers are backed up and checked at frequent intervals, consistent with a documented business continuity plan.
* back up information is stored in a secure off site environment.
* computers are protected by antivirus software that is installed and updated regularly
* computers connected to the internet are protected by appropriate hardware/software firewalls.
* we have a business continuity plan that has been developed, tested and documented.

Electronic data transmission of patient health information from WGPN is in a secure format.

WGPN has the following information to support the computer security policy:

* current asset register documenting hardware and software including software licence keys
* logging of maintenance, backup including test restoration, faults, virus scans

WGPN reserves the right to check individual’s Computer System history as a precaution to fraud, workplace harassment or breaches of confidence by employees. Inappropriate use of the Computer Systems or breaches of Computer Security will be fully investigated and may be grounds for dismissal.

WGPN has a sound backup system and a contingency plan to protect information in the event of an adverse incident, such as a system crash or power failure.

This plan encompasses all critical areas of operations such as making appointments, billing patients and collecting patient health information.

This plan is tested on a regular basis to ensure backup protocols work properly and that WGPN can continue to operate in the event of a computer failure or power outage.

**2.0 IT Support**

To improve our support service to you we would like to implement the following process.

All support requests that are Medium or Low priority should be emailed to: helpdesk@wheatbelt.com.au

All Emergency and High Priority requests can be directed to: helpdesk@wheatbelt.com.au or 08 9621 1530 during office hours or 0419 950 363 after hours or when you cannot get IT Support using 08 9621 1530.

To assist you to determine the priority of your request see below;

IT Support Priority Levels

Emergency:

This is a major problem, i.e. impacting everyone in the office, the network or server has gone down, immediate action required.

High Priority:

The user who reported the problem needs immediate help. There is no work-around for the problem, and the user cannot work until the problem is solved.

Medium Priority:

The problem is affecting the user's work, but there is a work-around until the problem is solved.

Low Priority:

The problem is annoying and should be fixed, but it is not time critical.

**3.0 Data Backup**

**Tape Backups**

1.0 Objective: to ensure the WGPNSERV data is being backed up on a nightly basis to enable recovery if required.

2.0 Tapes and boxes are marked with the days of the week.

3.0 Tapes are stored in the fire proof safe (Senior Contracts Manager Office).

4.0 The box for the current tape is left on top of the server.

5.0 Tapes are changed daily in the morning.

6.0 Daily procedure for changing backup tapes 6.1 Retrieve current days tape from safe.

6.2 Press the grey button located below the tape insert.

6.3 The server will eject the previous day’s back-up tape. This is stored in the relevant cover.

6.4 Insert current days tape in with the arrow pointing forwards. The tape should go in easily – do not force.

6.5 Return previous days tape in its cover to the fireproof safe.

**External Drive Backup**

1.0 Objective: to ensure the WGPNDATA server data is being backed up on a nightly basis to the drive to enable recovery if required.

2.0 Drives not being used are stored in fire proof safe (Senior Contracts Manager Office).

3.0 A power supply and USB cable are stored in the fire proof safe.

4.0 One drive is stored off-site at a location specified by the IT Manager.

5.0 The drives are rotated on a daily basis, changed at the same time as the tapes.

6.0 Daily procedure for changing the USB drives. 6.1 Retrieve current days drive from safe.

6.2 Unplug power and USB lead from front of existing USB drive on top of WGPNDATA server (Left side of server storage cupboard).

6.3 Insert USB and power leads into current days drive.

6.4 Return unplugged drive to fireproof safe.

7.0 Off-site storage of USB drives. 7.1 Rotation of drives to suitable location as directed by IT Manager.

7.2 At all times at least one drive will be stored off-site.