Information Management & Technology (IM&T) Uninterruptible Power Supply Procedure

Effective: 3 August 2021

1. Guiding Principles

Under Section 3.2.9 of the WA Health MP 0067/17 Information Security Policy, WA Country Health Service (WACHS) is committed to ensuring "physical and environmental security of ICT systems, infrastructure, facilities/buildings and network components… to prevent unauthorised physical access, damage and interference to health information." This includes protecting equipment against power failure.

The preference is for WACHS facilities to have connectivity to uninterruptible power via a building Uninterruptible Power Supply (UPS) maintained as a part of facilities management. This ensures ongoing, clean power to critical devices. Where this is not available, rack mounted UPS units may be used.

This procedure will outline the specifications and management of UPS units within WACHS.

2. Procedure

UPS units and other failsafe equipment and utilities are to be purchased by each region via the local ICT department, in line with the WA Health *Procurement Policy Framework*.

2.1 UPS Unit Management

Managed UPS units are attached to critical hardware and they require monitoring of self-tests of battery condition, power status and temperature. These units are to be plugged into essential power and have management cards for monitoring purposes.

Non-managed UPS units are to be attached only to non-critical systems and do not need support management cards. Being plugged into essential power is optional, however it is recommended. IM&T are not responsible for the maintenance of non-managed UPS units.

All managed and non-managed UPS units are to have checks and be tested with details recorded, including the check date and staff name. Self-testing UPS units are to be tested regularly, while units that do not self-test must be tested at least annually. WACHS ICT will conduct checks and testing on managed UPS units only. Owners of non-managed UPS units may coordinate with their local ICT department, however, remain responsible.

All UPS units are to be replaced regularly with consideration of manufacturer guidelines, warranty and regional budget.

2.2 Managed UPS Unit Specifications

WACHS ICT departments are to purchase managed UPS units to the following specifications:

- Illuminated LCD display, switchable to show:
  - input voltage, current and frequency on mains
  - output voltage, current and frequency on mains or battery
  - UPS load (percentage) on mains or battery
  - estimated remaining run time (in minutes) on battery
  - battery charge (percentage) on mains or battery.
- An audible alarm for each of:
  - on battery
  - overload
  - short circuit
  - over temperature
  - faulty battery
  - abnormal operation.
- Audible alarms able to be cancelled by button-press on the unit.
- Locally stored maintenance history, including:
  - unit age / time in operation
  - battery replacement history
  - limited unit event history.
- A network interface to provide centralised monitoring, interrogation and management, using either or both of:
  - Simple Network Management Protocol (SNMP) v3, including:
    - transmission of SNMP traps for all UPS alarm states with an audible alarm
    - acceptance of SNMP query to retrieve real time and historical data
    - acceptance of SNMP commands to perform specific actions, including;
      - cancel audible alarm
      - self-test, and
      - cancel self-test
  - an integrated web server hosted by the UPS, accessible via a standards-based web browser.
- Support design load for at least 30 minutes.
- Are of an online, double conversion type.
- Have hot-swappable batteries which can be safely field-replaced without needing to shut down the supported equipment.
- Have a bypass mode
- Include at least four IEC C14 sockets for power outlet.
- Are rack-mountable in a standard communications enclosure.

Hot-swappable power modules are recommended but not essential.

3. Definitions

Critical Systems	Systems that are required for use by multiple users or business areas such as WAN routers, LAN infrastructure, remote site racks and main communications racks, clinical / medical equipment that transmit or use critical data for patients.
Managed UPS Units	UPS units that are attached to critical hardware and require monitoring of self-tests of battery condition, power status and temperature. These units are to be plugged into essential power and have management cards for monitoring purposes.
Non-Managed UPS Units	UPS units are attached only to non-critical systems and do not need support management cards. Being plugged into essential power is optional, however it is recommended.
Simple Network Management Protocol (SNMP)	An internet standard protocol for collecting and organising information about managed devices on IP networks and for modifying that information to change device behaviour.
Uninterruptible Power Supply (UPS)	A type of power supply system that contains a battery to maintain stable power output to devices/systems in the event of a power surge or outage.

4. Roles and Responsibilities

Area Manager ICT Operations is responsible for:

- Enabling Central Office ICT staff and regional ICT Managers to meet their responsibilities under this procedure.

Regional ICT Managers are responsible for:

- Ensuring regional ICT processes are in place as required to support regional ICT staff to meet the requirements under this procedure.
- Oversight of all UPS units housed within the region, including purchase, storage, management and disposal.

ICT Officers are responsible for:

- monitoring UPS units:
    - operating state
    - input voltage, current and frequency
    - output voltage, current and frequency
    - load
    - remaining runtime
    - battery charge (percentage)
    - age / time in operation
    - battery replacement history

    - unit event history
    - issuing commands to the UPS, including:
        - cancel audible alarms, and
        - initiate self-test, if unit is not self-testing.
- raising maintenance requests as required
- reporting any issues/faults in the Service Manager

All Staff are required to work within policies and guidelines to make sure that WACHS is a safe, equitable and positive place to be.

5. Compliance

This procedure is a mandatory requirement under the WA Health *Information and Communications Technology Policy Framework* pursuant to section 26(2)(k) of the *Health Services Act 2016*.

Failure to comply with this procedure may constitute a breach of the WA Health Code of Conduct (Code). The Code is part of the Integrity Policy Framework issued pursuant to section 26 of the *Health Services Act 2016* (WA) and is binding on all WACHS staff which for this purpose includes trainees, students, volunteers, researchers, contractors for service (including all visiting health professionals and agency staff) and persons delivering training or education within WACHS.

WACHS staff are reminded that compliance with all policies is mandatory.

6. Records Management

All WACHS corporate records must be stored in the approved Electronic Documents and Records Management System.

Records Management Policy

7. Evaluation

Monitoring of compliance with this document is to be carried out by the **ICT Manager** quarterly, using the following means or tools:

- ICT Operations Checklist

8. Standards

National Safety and Quality Health Service Standards:

Clinical Governance Standard: 1.5

9. Legislation

Health Services Act 2016

10. References

MP 0067/17 Information Security Policy

11. Related Forms

Nil

12. Related Policy Documents

WACHS Records Management Policy

13. Related WA Health System Policies

MP 0067/17 Information Security Policy

14. Policy Framework

Information and Communications Technology Policy Framework

This document can be made available in alternative formats on request for a person with a disability

Contact:	Area Manager ICT Operations		
Directorate:	Innovation & Development	**EDRMS Record #**	ED-CO-13-65454
Version:	4.00	**Date Published:**	3 august 2021