Data Backups Procedure

1. Guiding Principles

Effective: 8 March 2022

In accordance with Section 3.2.10.1 of the WA Health MP 0067/17 Information Security Policy, WA Country Health Service (WACHS) is required to have backup plans and provision for redundancies to ensure ongoing availability of information processing facilities in the event of an Information & Communications Technology (ICT) incident or disaster. This procedure will prescribe data backup procedures, testing and storage requirements.

This procedure does not apply to core clinical or corporate applications data under the management of Health Support Services (HSS).

2. Procedure

This procedure is to be read in conjunction with the WACHS ICT Disaster Recovery Plans Procedure and applicable regional ICT Disaster Recovery Plan.

The preferred method of backup within WACHS is Backup as a Service (see Section 2.1 Backup as a Service), however, non-BaaS methods may be used (see Section 2.2 Non-BaaS Data Backups).

2.1 Backup as a Service (BaaS)

Critical servers, as per regional Disaster Recovery Plans, are to be included in the BaaS. BaaS client services/agents are to be installed and functioning, and backup frequency and retention requirements configured correctly for each server (see section 2.3 Backup Frequency & Retention).

Backup reports supplied by the BaaS provider are to be reviewed a minimum of once per week to ensure that backups are being reported as successful.

2.1.1 BaaS Testing Requirements

A monthly recovery test is to be performed on files/folders to ensure that they can be recovered.

An annual recovery test is to be performed on servers or, if different, in line with requirements of Information Management & Technology (IM&T) Disaster Recovery Testing Guidelines.

2.1.2 BaaS Reporting Requirements

A summary report is to be tabled each meeting of the regional Information Governance Committee (IGC), or equivalent.

2.2 Non-BaaS Data Backups

Backups are to be executed within the timeframes (see section 2.3 Backup Frequency & Retention) and housed in a remote location from the systems and data being captured.

Where the primary backup equipment is in the same location as the systems and data being captured, a second off-site copy is to be established on another storage system. Secondary backup storage is to be kept on tape or other suitable removable media or on another hard disk-based system.

All removable backup media is to be clearly labelled and stored off site in a safe, secure and environmentally sound location such as a fireproof safe with a minimum rating of four (4) hours.

Monthly backups are to be registered and recorded indicating successful completion or otherwise and signed off as such by a member of the regional ICT team. Where tape libraries are in place, a full backup set of tapes are to be archived once a month.

If a full month off-site backup has been unsuccessful, an ICT officer is to investigate immediately and determine whether the back-up can be re-started or, following consultation with their ICT Manager and Manager ICT Operations, it is approved to wait until the next logical back up cycle.

2.2.1 Non-BaaS Testing Requirements

A monthly recovery test is to be performed on backups to ensure the backup regime is working correctly and that folders and files can be recovered, and these results logged, and results sent to the Manager ICT Operations.

An annual recovery test is to be performed on servers or, if different, in line with requirements of WACHS IM&T Disaster Recovery Testing Guidelines.

2.2.2 Non-BaaS Reporting Requirements

A summary report is to be tabled each meeting of the regional Information Governance Committee (IGC), or equivalent.

2.3 Backup Frequency & Retention

The frequency of backups and retention settings required for each server differs depending on the purpose of the server. On configuring the retention, regions are to follow these guidelines:

- File/Database/Application servers that may contain Health Department records:
  - Data Drives: Backup daily and retain 7 years;
  - Databases: Backup daily and retain 7 years;
  - System Drives & System State: Backup weekly and retain 6 months.

- Servers that have a functional role with no records (e.g., DHCP):

- System Drives & System State: Backup weekly and retain 6 months.

The backup frequency represents how often the servers are backed up, however, back ups may be consolidated for retention purposes.

3. Definitions

WACHS Information Governance Committee (IGC)	The WACHS Information Governance Committee is the main advisory body to the WACHS Executive forum and WACHS CEO on ICT matters pertaining to WACHS and the broader reform agenda of WA Health
ICT Networks	The ICT Networks is the main advisory group to the ICTGC on all Information Communications and Technology matters pertaining to WACHS.
Health Support Services (HSS)	The HSS was established to drive the Information, Communications and Technology reform program, provide a focus on the importance of health information in our system and enable efficient and integrated technology services.
Disaster Recovery Plan (DRP)	A plan that outlines the process and timeframes, communication strategy when there is an ICT disaster or pending ICT disaster.
Dynamic Host Configuration Protocol (DHCP)	Server infrastructure that ensures a device network address based on its location in WA Health.
Backup as a Service (BaaS)	Backup as a service (BaaS) is an approach to backing up data that involves purchasing backup and recovery services from an online data backup provider.

4. Roles and Responsibilities

Area Manager ICT Operations is responsible for:

- Ensuring any WACHS-wide contracted arrangements specify the responsibilities of all parties in protecting health information to an appropriate level.
- Ensuring appropriate measures are in place to protect WACHS data.
- Enabling regional ICT Managers to meet their responsibilities under the WA Health Information Security Policy and WACHS Data Backups Procedure*.*

Regional ICT Managers are responsible for;

- Ensuring appropriate measures are in place to protect regional data.
- Ensuring regional ICT procedures are in place as required to support regional ICT staff to meet the requirements under this procedure.
- Tabling summary reports to the regional IGC or equivalent.
- BaaS management, where applicable, including:

  - Ensuring that all critical regional servers are included in BaaS, clients/agents are installed and functioning, and that backup frequency and retention requirements are correct for each server.
- Non-BaaS backup management, where applicable, including:
  - Oversight of all data backups and supporting activities where the equipment is housed within the region.
  - Oversight and approval of back up testing.
  - Ensuring backups are executed within the timeframes as per section 4.2.2 of regional Disaster Recovery Plans.

Regional ICT Officers are responsible for

- Adhering to regional ICT processes as required to support this procedure.
- BaaS maintenance, where applicable, including:
  - Weekly review of backup reports provided by the BaaS provider.
  - Testing the server recovery.
  - Performing recovery tests on files / folders.
- Non-BaaS backup maintenance, where applicable, including:
  - Labelling and storage of backups and removable backup media.
  - Execution of backups.
  - Registering, recording and obtaining regional ICT Manager sign off on monthly backups, including investigation of unsuccessful backups and re-running as required.
  - Archiving a full backup set of tapes once per month, where tape libraries are in place.
  - Performing recovery tests on backups.

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.

WACHS Records Management Policy

7. Evaluation

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

- A report to the regional ICG or equivalent with ICT Manager endorsement. The report will provide evidence that backups have been captured and regular testing has been undertaken.
- Approval of the regional ICT Operations Checklist to indicate that backups and testing have been completed.
- Monthly security reports to the WACHS ICT Security Coordinator.

Further evaluation will be undertaken annually by the Office of Auditor General (OAG) based on the OAG audit schedule.

8. Standards

National Safety and Quality Health Service Standards:
Clinical Governance Standard: 1.5

Australian Standards for Information Security:
AS/ISO 27002 Information Technology – Security Techniques – Code of Practice for Information Security Controls
AS/ISO 27799-2011 Information Security Management in Health using ISO/IEC 27002

9. Legislation

Health Services Act 2016

10. References

MP 0067/17 Information Security Policy
WACHS ICT Disaster Recovery Plans Procedure
Disaster Recovery Testing Guidelines

11. Related Forms

Nil

12. Related Policy Documents

WACHS ICT Disaster Recovery Plans Procedure
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:	Information Management & Technology	**EDRMS Record #**	ED-CO-13-65451
Version:	4.00	**Date Published:**	8 March 2022