ITP106

DATA BACKUP POLICY

Table of Contents

1. PURPOSE

The purpose of this policy is to describe the overall backup policy for information and ICT systems within the Corporation, including the minimum backup frequency for the different types of information and ICT systems.

2. SCOPE

This policy applies to all staff, third party contracts and temporary personnel within the company that are responsible for the installation and support of company's ICT systems and information, individuals charged with information resources security and data owners.

3. ROLES AND RESPONSIBILITIES

- Procedures & processes to meet this policy are created, owned and managed by the IT Department.
- It is important that all staff understand what is required of them and comply with this policy.
- The concerned IT staffs are responsible for ensuring the Backup schedules is followed in compliance with this policy.
- It is also a responsibility of all individuals and handlers of National Ambulance information Technology Services, data and information to ensure that all policies and procedures dealing with all Information Technology (IT) & security, integrity of information and data are followed.

4. POLICY STATEMENT

4.1 Data Backup for Systems, Applications and Data

Up-to-date backups of all critical items shall be taken regularly to ensure the continued provision of the minimum essential level of service. These items include:

- Instant VM recovery
- Entire VM (Including registration)
- Databases
- Documents
- Application aware backup

All Virtual Servers backups is set as per below Procedures

- Backup on disk – Everyday Incremental Backup and Weekly Full Backup for all VM servers with 7 restore points.
- Backup on tape – Every week full backup with 3 weeks' retention.
- Every month full backup with one-month retention.
- Every quarter full backup maintain as a offsite backup with infinity period retention.
- Replication on a disk to the DR site – Everyday replication has set to DR site with 7 restore points
- Backup copy on a disk to the DR site – Retention is 10 restore points. This is treat as a offsite backup on a disk.
- Backup logs are receiving everyday to the IT team by email. The servers backup is tested regularly by the sure backup process of the Veeam.

5. DEFINITIONS

Backup on Disk - is the copy of the files and applications and entire Virtual servers made on a SAN storage to avoid loss of data and facilitate recovery in the event of a system crash.

Backup on a Tape – is the copy of the files and applications and entire Virtual servers made on Tape to avoid loss of data and facilitate recovery in the event of a system crash or site crash.

Replication on a disk – is the copy of the files and applications and entire Virtual servers made on SAN storage on to a DR Site to avoid loss of data and facilitate recovery in the event of a system crash or site crash.

Backup Copy on Disk – is the copy of the "backup on disk" data made on SAN storage on to a DR Site to avoid loss of data and facilitate recovery in the event of a system crash or site crash.

6. ENFORCEMENT

Any employee found to have violated this policy may be subjected to disciplinary action.

7. RELEVANT LEGISLATION

National Ambulance Privacy

International, federal or local legislation and circulars relevant to this Policy. Full detail on this legislation can be found in QHP109 Legal Register.

Code, Name of Legislation	Jurisdiction
Code, Name of Legislation, Year here	Jurisdiction here

8. RELATED POLICIES AND FORMS

List related policies and procedures to the created/updated policy.

Policy & Procedure /Form

9. FEEDBACK

Any feedback or suggestions for improvement to this Policy, Processes or Procedures can be submitted to qhse@nationalambulance.ae

10. DOCUMENT CONFIGURATIONS CONTROL DATE

A review and update of this document will take place as necessary, when changes occur that identify the need to revise this Policy such as changes in roles and responsibilities, release of new legislative or technical guidance, or identification of a new policy area.

This document ownership for editing is identified as:

IT Manager

Change Brief

Version No.	Date	Changes
1	January 2014	New Documents
2	September 2014	Backup Schedule Changes, Backup location added
3	February 2017	Modification of Backup Schedule
4	October 2019	Introduce a new backup method. Include note that the new backup system cover all existing back up requirement including those specified in version 3
5	August 2022	Due to review, updated the roles and responsibilities and transfer to new template of the Policy and Procedure

Review & Approval:

_____

(Enter final approver title here)