15 Organisation/ICT/02/01/15 – Back- up

15.1 Description

Backup is a copy of a program or file that is stored separately from the original. These duplicated copies of data on different storage media or additional hardware resources are used to restore the original after a data loss event. Backups are used primarily for two purposes. The most common is to restore small numbers of files after they have been accidently deleted or corrupted. The second is to restore a state following a disaster. Backups are not archives and are not a substitute for record retention plans, nor are they, by themselves, business continuity plans

15.2 Objective

This Guideline defines the backup for computer systems that store State data. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include file servers, mail servers, web servers, application servers and database servers.

This Guideline is to establish the rules for the backup and storage of electronic information at Organisation.

This Guideline is also designed to prevent the loss of Organisation data in the event of an equipment failure or destruction

15.3 Scope

This Guideline applies to all Staff, permanent or temporary, and third parties who use ICT devices connected to the Organisation network or who process or store information owned by Organisation. All users are responsible for arranging adequate data backup procedures for the data held on IT systems assigned to them

The back procedures in this Guideline apply to all Network Managers, System Administrators, and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer. ICT department are responsible for the backup of data held in Organisation databases

This Guideline applies to:

i. All employees who create data on the organisation’s computer systems

ii. All data owners whose data is maintained on any of our central shared systems

iii. All mission critical data, collected, generated, processed, stored or transmitted on the organisation’s infrastructure

15.4 Standard Guidelines

The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

The Organisation Information Resources backup and recovery process for each system must be documented and periodically reviewed.

The vendor(s) providing offsite backup storage for the Organisation must be cleared to handle the highest level of information stored.

Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest Organisation sensitivity level of information stored.

A process must be implemented to verify the success of the Organisation electronic information backup.

Backups must be periodically tested to ensure that they are recoverable. This period shall be set according to the criticality of the data backed up and the frequency of its change

Signature cards held by the offsite backup storage vendor(s) for access to Organisation backup media must be reviewed annually or when an authorized individual leaves Organisation.

Procedures between Organisation and the offsite backup storage vendor(s) must be reviewed at least annually.

Backup tapes must have, at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:

i. System name

ii. Creation Date

iii. Sensitivity Classification [Based on applicable electronic record retention regulations.]

iv. Organisation Contact Information

All user information on the servers must be identified and scheduled for back-up in line with the routine back up procedures based on the sensitivity classification.

All back-up tapes or medial shall be tested post the back-up exercise to confirm that all the data has been adequately and completely backed up in cases of incremental back up.

All routine server back- up shall include server scripts and database scripts to ensure that in cases on server failure the System Administrators are in a position to restore the server to its last known good configuration including the data on the server.

Data backup

The ICT department recognizes that the backup and maintenance of the files for all organisational servers, PCs (including application data files) are critical to the viability and operations of the organisation. Therefore IT must put in place certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

Restoration

In-line with business requirements, ICT Department must put in place restoration procedures and mechanisms and ICT Department shall test the backup & restoration plan to ensure that the backup operation and media work as expected. The process of backup and restoration shall be reviewed quarterly;

Regular verification of usability of back-ups;

v. Security and integrity and accuracy of the stored data; and

vi. Automated schedule job monitoring and exception reporting

Restoration to the production and test environment will be formerly requested for and authorized to ensure a consistent and predictable computing environment.

15.5 Procedure

Network Server Backups

The servers deployed in the Organisation's Network have a backup tape device attached to the server, or have access to a backup tape devices attached to another server in the local network. The type of backup tape device varies with the model of the server and the volume of data to be backed up.

Backup software on the network server is used to control the backup processes (e.g. Windows NT Backup for Win Servers);

i. Organisation's ICT Department shall ensure all backups are completed successfully and review the backup process on all network servers daily.

ii. Logs are maintained to verify the success backup process

Daily backups

iii. The Logs shall be retained for a period of 7 days and be over-written on the 8th day

Backup Contents

The contents of the backups vary with the server and location. The primary data that will be backed up are:

Data files:

iv. Transactional data, document files (like Word, Excel, PowerPoint, PDF, HTML etc. and Images.)

v. E-Mail data for all email accounts located on our E-Mail server.

vi. User files on the servers on dedicated folders

System Data:

vii. Applications files for the server and other selected software installed on the server.

viii. Server Scripts and logs including database scripts and logs

Daily Backups

ix. Backups of data on production servers will occur every business day at 8:00PM

x. Backup of the satellite labs environment on the branch servers will occur every business day after end of day processes.

Tape Rotation and incremental back ups

To reduce backup tape costs and to promote an efficient and reliable backup, the following schedule is defined for the Organisations server backup tape rotations:

xi. Daily backups (Monday – Sunday) take place on a 1-week rotation; tapes over-written on the 8th day

xii. Monthly full backups of servers occur on the last day of every month and these tapes shall not be rotated;

xiii. Special backups may be made for longer retention periods before or after system upgrades, major business projects, or for financial reporting periods.

xiv. Tapes preceding service disruption events (such as power failures that could lead to data loss, transaction stripping) shall be isolated and treated as special backups for longer retention periods.

xv. Incremental backup will be taken on the same cartridge at least twice a week.

Offsite Storage of tapes

xvi. Daily backups for days other than the current day will be stored in the safe at the server room.

xvii. Monthly Backups: Monthly backups for all network locations will also be moved to an offsite location for long-term storage. The retention period for the monthly tapes is as follows:

xviii. A monthly backup will be kept for each month, for each server for a period of at least 5 years.

Documentation and Tracking

xix. All backup media and tape drives shall be appropriately labelled;

xx. A tape transfer log shall be appropriately signed off by staff responsible for migration of the backup media to the organisation's off-site storage location;

15.6 Responsibility

These are people that are affected by this Guideline

Roles	Responsibilities
ICT Department	• doing the backups or delegating • checking that they have been successfully completed • recording the information on the backup sheets • ensuring that the backups are stored securely • ensuring that the tapes are properly labelled and rotated • advising the ICT Department on requirements for new tapes

15.7 Procedure

Below are guidelines of procedures and responsibilities for defined information and communications technology (ICT) employees (i.e., system administrators, network administrators). These guidelines will include a backup strategy that applies to the following:

i. Computerized systems that store source or original Organisation information.

ii. Implement standard frequency and type of backup for each type of computer system or platform in use based on the significance of the information and its frequency of change.

Backups should occur on a daily basis or be based on the significance of the information and its frequency of change. A preferred method of backup is disk-to-disk backup. If this method is not applicable for the system, then tape backup is required.

Back up all necessary data files and programs to recreate the operating environment.

Implement procedures for transferring a recent copy of backup media to a physically and environmentally secure off-site storage location. An inventory and tracking system must be maintained. Ensure that the following are stored at the off-site storage location:

iii. Source and object code for production programs

iv. Master files and transaction files necessary to recreate the current master files

v. System and program documentation

vi. Operating systems, utilities, and other environmental software

vii. Other vital records

Ensure that documented procedures exist for the recovery and restoration of information from backup media.

Identify I.T. staff responsible for ensuring successful back-ups.

Routinely copy operating software, application software, and production information to backup media based on frequencies set by management. This applies to major systems (e.g., local area network (LAN) or wide area network (WAN) servers, client/server database servers, special-purpose computers) in use

Maintain at least three generations of backup media, i.e. “grandfather, father, son” arrangement for operating and application software.

Define data model to be used for each type of data; i.e. full + incremental, full + differential, (for file servers) or database exports or extracts (for applications)

Back up of the printed documentation and pre-printed forms necessary for recovery. Convert printed documentation and pre-printed forms into electronic format and move them into the DR site.

Test the backup to determine if data files and programs can be recovered

16 Organisation/ICT/02/01/16 - ICT System Access Control

27 Organisation/ICT/02/01/27 - Contingency Planning

27.1 Description

An ICT Contingency Plan refers to a plan for recovering ICT services following a system disruption. Such measures may include the recovery of ICT functions using alternate equipment or the relocation of ICT systems and operations to an alternate site. The ICT Contingency provides guidance to ensure that Organisation is able to do the following before, during and after a disruptive event:

i. Process and manage critical information,

ii. Maintain national and international communications,

iii. Maintain Internet access,

27.2 Objective

ICT contingency planning is be part of the fundamental mission of the Organisation as a responsible and reliable public institution.

To ensure the continuous performance of the Organisation information systems especially during emergencies through;

i. Protecting equipment, data, and other assets. reducing or mitigating disruptions to operations.

ii. Reducing damage and losses.

iii. Achieving timely and orderly recovery from emergencies and resumption of full service to the public

27.3 Scope

The scope of the contingency plan should cover all critical systems identified by Organisation

The contingency plan will apply in all cases of disruption of operation where the critical systems will be affected

27.4 Standard Guidelines

In order to achieve workable ICT contingency capability the Organisation should be able to maintain a certain level of readiness and implement contingency procedures when the need arises.

The contingency plan for Organisation shall cover all critical applications within Organisation and shall also be updated regularly to accommodate changes in the systems.

The contingency plan shall be tested from time to time to confirm its relevancy and applicability to the present ICT operating environment.

All staff within the ICT department shall be trained on the execution of the contingency plan.

27.5 Responsibility

Department	**Role(s)**
CIRT	See detailed roles as in the Incident Management guidelines
ICT Operations	Ensure that all necessary mechanisms are in place to be able to recover in case of a disaster
ICT Department	Ensure that all Sections in the Unit are able to respond to any disasters

27.6 Procedure

This procedure will be executed in conjunction with the Incident management procedures

- Perform risk assessment
- Define disruption Categories
- Develop Risk and Impact Ratings
- Identify critical ICT resources and Critical Data
- Develop preparation and preventive measures
- Develop preventive measures for disruption Categories
- Developed essential contingency procedures
- Develop notification and contingency plan activation procedures
- Develop recovery strategies and plans
- Test the contingency plan
- Maintain contingency plan
- Train the Organisation Team on the contingency plan

The detailed processes to support the steps above can be found in the Annexes detailing the Contingency plans and incident management procedures and the

27.7 Flow Chart

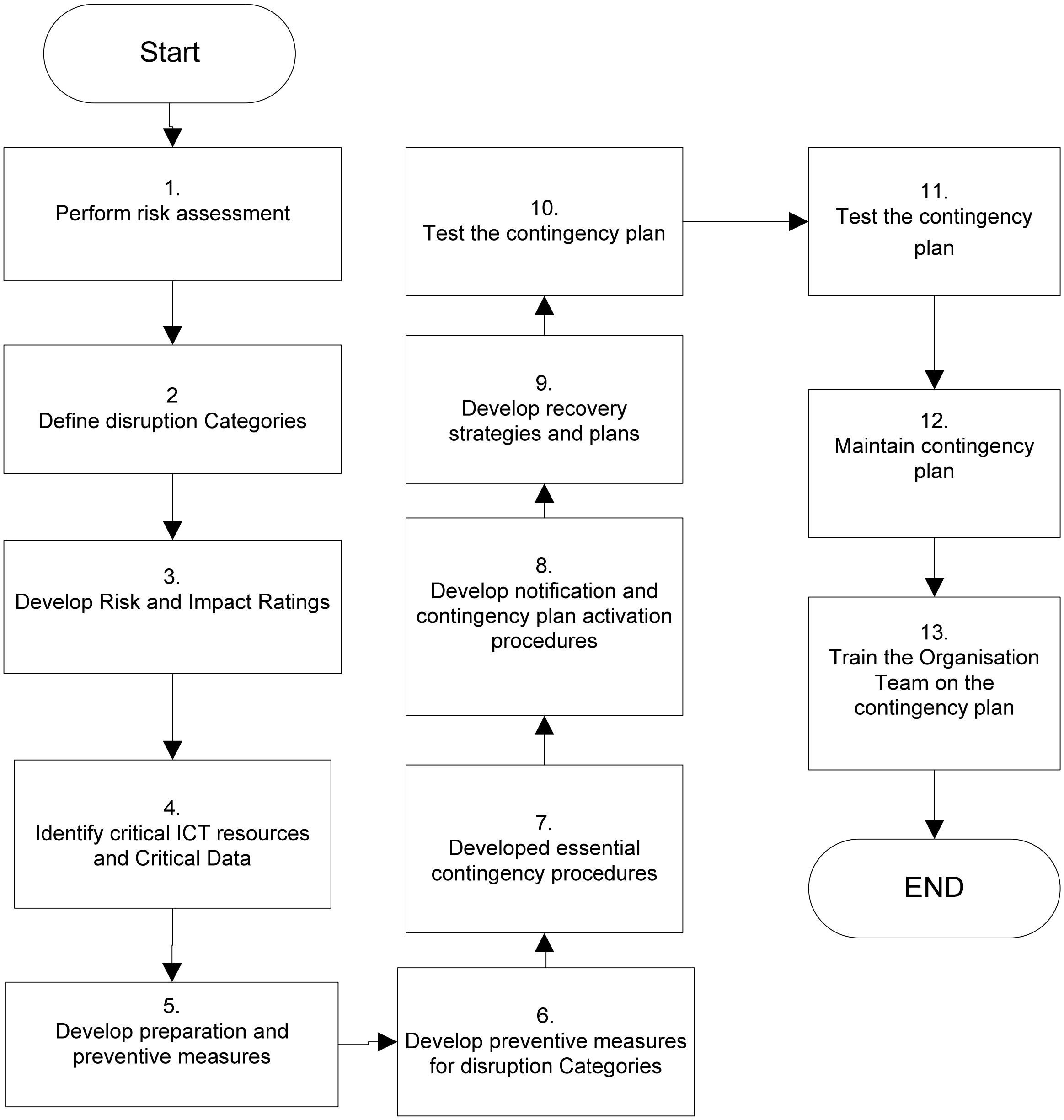
Start
1.
Perform risk assessment
2
Define disruption Categories
3.
Develop Risk and Impact Ratings
4.
Identify critical ICT resources and Critical Data
5.
Develop preparation and preventive measures
6.
Develop preventive measures for disruption Categories
7.
Developed essential contingency procedures
8.
Develop notification and contingency plan activation procedures
9.
Develop recovery strategies and plans
10.
Test the contingency plan
11.
Test the contingency plan
12.
Maintain contingency plan
13.
Train the Organisation Team on the contingency plan
END

Figure 13: Contingency Planning flowchart