SERVER BACK UP POLICY

Version number	Review date	Reviewed by	Approval date	Approved by	Summary of Changes	Next review date
1.0	Jul 2012	G. Price	Jul 2012	J. Ilag	Baseline	
2.0	Dec 2015	G. Price	Jan 2016	J. Ilag	Changed DMS Service Desk to Integrated Service Desk in para 5; added example of acceptable offsite backup facility in para 6; updated MailStorage information in para 16	Jul 2017

A. Policy Objective:

1. The purpose of this policy is to define the backup schedules for all the server groups and ensure server continuity to support the backup and restoration of archived information in the event of a natural disaster, equipment failure, and/or accidental loss of files. The goals of this backup policy are outlined as follows:

   - To safeguard the information assets of UNFPA.
   - To prevent the loss of data in case of accidental deletion or corruption of data, system failure, or disaster.
   - To permit timely restoration of information and business processes
   - To manage and secure backup & restoration processes and the media employed within these processes.

B. Intended Audience:

2. This policy covers UNFPA users who are involved in providing backup and restoration services to any UNFPA HQ servers such as IT Backup Administrators and Local Area Network Managers.

C. Policy Statement:

a. Staff Responsibilities and Accountability:

3. MIS is responsible for backing up user data stored on HQ servers. MIS must designate a dedicated Backup Administrator as well as an alternate, who will work under the supervision of Applications Development Manager and/or Technology Manager and will be responsible and accountable for backup and restoration management.

b. Backup Criteria:

4. Backup Administrator must put in place procedures to create backup copies of all critical data stored on UNFPA servers. Critical data is defined as application source code, email data, and

official documentation which is stored on production servers. Methods are implemented for authorized users to gain access to the backup data quickly. These procedures are updated yearly to accommodate changes in policies or procedures at UNFPA. We must consider the following criteria in implementing the backup policy on a per system basis.

- Selections: what information is to be backed up on systems.
- Priority: relative importance of information for prioritizing of backup jobs.
- Type: the frequency and amount of information backed up within a set of backup jobs.
- Schedule: the schedule to be used for backup jobs.
- Duration: the maximum execution time a backup job may take prior to its adversely affecting other processes.
- Retention Period: the time period for which backup images created during backup jobs are to be retained.

c. Restore Request procedure:

5. All requests for restoration services must be submitted through the Integrated Service desk. The Backup Administrator must complete all the restoration requests within one business week.

d. Off Site Backup:

6. UNFPA offices must maintain an offsite **secure** backup facility where critical data is stored. An acceptable offsite backup facility could be another agency, bank, etc…Preferred storage media forms are tape and hard drive cartridges. Refer to **Annex I** for the detailed schedule for the HQ Remote Data Retention category under each server group which should be backed up.

e. Tape Backup:

7. For HQ, an additional backup is done quarterly on tapes. These tapes must be stored in a secure onsite location in a physically secured safe at the UNFPA headquarters data center, New York with restricted access. Only the Backup Administrator, Application Development Manager, Technology Manager and the Chief, MIS Branch will have access to this safe.

f. Defining what is to be backed up:

8. All data and software essential for the continued operation of all UNFPA services must be backed up.

9. In backing up information, all supporting material (e.g. programs, control files, and operating system software) required to process the information must also be backed up, although not necessarily with the same frequency as the data.

10. For headquarters, the Backup Administrator will determine what information to back up, in what form, and how often, in consultation with the Applications Development Manager, Technology Manager and the technical staff that are responsible for the specific data.

g. Types of data backup:

11. There are various procedures for backing up data which are listed below:

- Full data backup: With this procedure, all data requiring backup are stored on an additional data medium without consideration as to whether the files have been changed since the last backup. Therefore, this method requires a high storage capacity.
- Differential data backup: This procedure stores only the files that have been changed since the last full data backup. For restoration of data, the latest full data backup followed by the most recent differential backup, will suffice to restore the data.

h. Data Backup Procedures:

12. Depending on the degree of automation that is required and the storage location the Backup Administrator should select and implement the appropriate backup procedure as outlined in the paragraph below.

13. Automatic data backups is the first preference for all data backup procedures. It must be implemented in all cases possible by triggering a program at certain intervals as defined in **Annex I** schedule.

14. The manual data backup will be performed by the Backup Administrator only as needed.

i. Storage medium:

15. The Backup Administrator determines the appropriate media for backups considering the following criteria:

- The amount of time it takes to identify the data media necessary for backup and making them available to the system.
- The actual time required for restoring the data, which depends on the average time needed to access the data on the storage medium, the rate of data transfer, and the number of files involved.
- Storage capacity of the data media to ensure large volumes of data are being backed up effectively.
- The cost of data backup (cost of read/write devices, data media and time required for operations).
- The life and reliability of the data media should also be taken into consideration.
- The availability of requirements for faster access to data media for backup purposes, and for re-importing the relevant data from the backup data media.
- In the case where retention schedules call for deletion/erasure of data at specific times, the selected storage medium must allow this deletion.
- In case of confidentiality and integrity issues which prevent encrypted data, then consideration should be given to data media whose design and transport characteristics would allow their storage in locked vaults.

j. Server Groups:

16. All servers that require backup are classified in the following categories:

- MailStorage – following the outsourcing of UNFPA’s mail system to Google in 2014 and with the addition of Google Vault archiving, the need for a formal backup process for email and related applications is no longer required.
- UnixServers - Backup of all Unix/Linux servers including applications, databases and application data.
- Windows Servers - Backup of Windows servers and file shares.
- Catalog Backup - Backup of the backup server catalog/index database and configuration.
- The backup schedule for each of these server groups is described in detail in Annex 1.0.
- The backup selections and the policy clients for each Server Group are listed in Annex 2.0.

D. Policy date:

17. The Server Backup Policy (originally approved and issued on 18 July 2012 with subsequent revisions as shown in the beginning of this document) will remain in force without time limit, and will be reviewed annually to ensure relevance.

E. Policy owner:

18. The Technology Services Section Chief is responsible for the Server Backup Policy.

F. Change authority:

19. The MIS Chief and Technology Services Section Chief have the authority to change the server backup policy. The MIS Branch, Technology Services Section Chief, and Business Services Section Chief can give exception waivers to it.

Annex I: HQ Backup Schedule

Back Up Type		Retention Period	Schedule
1. Server Group: Unix Servers			
a.	Local data retention of 1 year on local disk device (fpadd1)		
	a. Quarterly full backup	1 year retention	2nd weekend of March, June and September
	b. Daily differential backup	1 year retention	Monday Through Sunday
b.	Local data retention of 3 years on local tape device		
	c. Yearly full backup	3 year retention	2nd weekend of December
c.	Remote data retention of 2 months on remote disk device (fpadd2)		
	d. Monthly full backup	2 month retention	2nd weekend of the Month
	e. Daily differential backup	2 month retention	Monday Through Sunday
3. Server Group: Windows Servers			
a.	Local data retention of 1 year on local disk device (fpadd1)		
	f. Quarterly full backup	1 year retention	3rd weekend of March, June and September
	g. Daily differential backup	1 year retention	Monday Through Sunday
b.	Local data retention of 3 years on local tape device		
	h. Yearly full backup	3 year retention	3rd weekend of December
c.	Remote data retention of 2 months on remote disk device (fpadd2)		
	i. Monthly full backup	2 month retention	3rd weekend of the Month
	j. Daily differential backup	2 month retention	Monday Through Sunday
4. Server Group: Catalog Back up			
a.	Local data retention of 1 month on local disk device (fpadd1)		
b.	Local data retention of 1 month on local tape device		
c.	Remote data retention of 1 month on remote disk device (fpadd2)		

Annex II: Backup Selections and Policy Clients Details

1) **Server Group: MailStorage**

   a) Backup selections: /opt/MsgBackup/mb1, /opt/MsgBackup/mb2, /opt/MsgBackup/mb3, /opt/MsgBackup/mb4, /opt/MsgBackup/mb5

   b) Policy clients:
   fpabbs.unfpa.org

2) **Server Group: UnixServers**

   a) Backup selections: / (root)

   b) Policy Clients:

apollo.unfpa.org
appserv01.unfpa.org
appserv02.unfpa.org
appserv03.unfpa.org
appserv04.unfpa.org
appserv05.unfpa.org
appserv06.unfpa.org
appserv07.unfpa.org
ares.unfpa.org
athena.unfpa.org
cognos1.unfpa.org
cognos2.unfpa.org
cognos3.unfpa.org
dmzdns.unfpa.org
fp-roxy.unfpa.org
fpabbs.unfpa.org
fpacf01.unfpa.org
fpadev02.unfpa.org
fpadns01.unfpa.org
fpaftp.unfpa.org
fpahold01.unfpa.org
fpaintgw.unfpa.org
fpamail1.unfpa.org
fpamgw1.unfpa.org
fpamgw2.unfpa.org
fpastor01.unfpa.org
fpaweb.unfpa.org
fpaweb03.unfpa.org
hades.unfpa.org
helios.unfpa.org
jupiter.unfpa.org
lbdns1.unfpa.org
mars.unfpa.org
mercury.unfpa.org
mysqldev.unfpa.org
mysqlprod.unfpa.org
neptune.unfpa.org
oracledb.unfpa.org
orion.unfpa.org
pluto.unfpa.org
ray.unfpa.org
sso2.unfpa.org
venus.unfpa.org
webnew.unfpa.org
www02.unfpa.org
zeus.unfpa.org

3) **Server Group: Windows Servers**

a) Backup selections: K:\, R:\, H:\, J:\, E:\

b) Policy clients:

- winhqfc1
- winhqfc2
- winhqfc3
- winhqfc4

- winhqfc5