UNFPA
Policies and Procedures Manual
Server Back Up Policy

SERVER BACK UP POLICY

<table>
<thead>
<tr>
<th>Version number</th>
<th>Review date</th>
<th>Reviewed by</th>
<th>Approval date</th>
<th>Approved by</th>
<th>Summary of Changes</th>
<th>Next review date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Jul 2012</td>
<td>G. Price</td>
<td>Jul 2012</td>
<td>J. Ilag</td>
<td>Baseline</td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>Dec 2015</td>
<td>G. Price</td>
<td>Jan 2016</td>
<td>J. Ilag</td>
<td>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</td>
<td>Jul 2017</td>
</tr>
</tbody>
</table>

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
UNFPA

Policies and Procedures Manual
Server Back Up Policy

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

<table>
<thead>
<tr>
<th>Back Up Type</th>
<th>Retention Period</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Server Group: Unix Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Local data retention of 1 year on local disk device (fpadd1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Quarterly full backup</td>
<td>1 year retention</td>
<td>2nd weekend of March, June and September</td>
</tr>
<tr>
<td>b. Daily differential backup</td>
<td>1 year retention</td>
<td>Monday Through Sunday</td>
</tr>
<tr>
<td>b. Local data retention of 3 years on local tape device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Yearly full backup</td>
<td>3 year retention</td>
<td>2nd weekend of December</td>
</tr>
<tr>
<td>c. Remote data retention of 2 months on remote disk device (fpadd2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Monthly full backup</td>
<td>2 month retention</td>
<td>2nd weekend of the Month</td>
</tr>
<tr>
<td>e. Daily differential backup</td>
<td>2 month retention</td>
<td>Monday Through Sunday</td>
</tr>
<tr>
<td>a. Local data retention of 1 year on local disk device (fpadd1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Quarterly full backup</td>
<td>1 year retention</td>
<td>3rd weekend of March, June and September</td>
</tr>
<tr>
<td>g. Daily differential backup</td>
<td>1 year retention</td>
<td>Monday Through Sunday</td>
</tr>
<tr>
<td>b. Local data retention of 3 years on local tape device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>h. Yearly full backup</td>
<td>3 year retention</td>
<td>3rd weekend of December</td>
</tr>
<tr>
<td>c. Remote data retention of 2 months on remote disk device (fpadd2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. Monthly full backup</td>
<td>2 month retention</td>
<td>3rd weekend of the Month</td>
</tr>
<tr>
<td>j. Daily differential backup</td>
<td>2 month retention</td>
<td>Monday Through Sunday</td>
</tr>
<tr>
<td>4. Server Group: Catalog Back up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Local data retention of 1 month on local disk device (fpadd1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Local data retention of 1 month on local tape device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Remote data retention of 1 month on remote disk device (fpadd2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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  fpacf01.unfpa.org  mars.unfpa.org
   appserv01.unfpa.org  fpadev02.unfpa.org  mercury.unfpa.org
   appserv02.unfpa.org  fpadns01.unfpa.org  mysqldev.unfpa.org
   appserv03.unfpa.org  fpaftp.unfpa.org  mysqlprod.unfpa.org
   appserv04.unfpa.org  fpahold01.unfpa.org  neptune.unfpa.org
   appserv05.unfpa.org  fpaintgw.unfpa.org  oracledb.unfpa.org
   appserv06.unfpa.org  fpamail1.unfpa.org  orion.unfpa.org
   appserv07.unfpa.org  fpamgw1.unfpa.org  pluto.unfpa.org
   ares.unfpa.org  fpamgw2.unfpa.org  ray.unfpa.org
   athena.unfpa.org  fpastor01.unfpa.org  sso2.unfpa.org
   cognos1.unfpa.org  fpaweb.unfpa.org  venus.unfpa.org
   cognos2.unfpa.org  fpaweb03.unfpa.org  webnew.unfpa.org
   cognos3.unfpa.org  hades.unfpa.org  www02.unfpa.org
   dmzdns.unfpa.org  helios.unfpa.org  zeus.unfpa.org
   fp-roxy.unfpa.org  jupiter.unfpa.org
   fpabbs.unfpa.org  lbdns1.unfpa.org

3) **Server Group: Windows Servers**
   a) Backup selections: K:\, R:\, H:\, J:\, E:\

   b) Policy clients:

   - winhqfc1
   - winhqfc2
   - winhqfc3
   - winhqfc4
• winhqfc5