GOVERNMENT OF KERALA

Abstract

Finance Department-SPARK-Backup Policy –Approved-orders issued.

FINANCE (IT SF) DEPARTMENT

G.O.(MS) No.421 /2016/FIN Dated, Thiruvananthapuram, 31/10/2016

Read: U.O. (f) No. SPK-A1/109/2016-Fin From SPARK PMU

ORDER

The Chief Project manager (SPARK) vide e-file read as first paper above has furnished the Backup policy prepared and approved by the National Informatics Centre (NIC) for SPARK.

Government have examined the matter in detail and are pleased to approve the SPARK Backup Policy as appended to this order for strict compliance.

By order of the Governor
SURESH KUMAR.O.B
UNDER SECRETARY TO GOVERNMENT

To: The Principal Account General (A&E),Kerala, Thiruvananthapuram.
The Principal Account General (G&SSA),Kerala, Thiruvananthapuram.
The Account General (E&RSA),Kerala, Thiruvananthapuram.
The State Informatics Officer,National Informatics Centre (NIC),Kerala Circle,CDAC Campus,Vellayambalam,Thiruvananthapuram.
The Chief Project Manager,SPARK, Thiruvananthapuram.
Finance (Accounts A) Department.
The Sub Treasury Officer,Secretariat.
Stock file /Office Copy.

Forwarded/By order,

Accounts Officer.

Backup Procedure for SPARK

(Version 1.0)

Government of India

Ministry of Electronics and Information Technology

National Informatics Centre

Kerala State Centre, Thiruvananthapuram

Prepared by: G. Jaya Kumar
Senior Technical Director

Reviewed by: N. Ranjit
SeniorTechnical Director

Approved by: T Mohanadhas
State Informatics Officer

Amendment Log

Version No	Release Date	Change Number	Brief Description	Sections changed
0.1	22.12.2009	-	Draft Release	
1.0	26.09.2016		First Release	Over all

Table of Contents

1. Introduction

Data is one of the most important aspects of the IT initiatives of the Government of Kerala and it is accumulated over years and months of effort. The probability of failure of systems is lower these days due to upcoming technologies and improved reliabilities. Still the government should not lose its data. One of the most common causes is physical failure of the media the data is stored on. Other possible causes for data loss are through viruses, software bugs, natural calamity, and accidents. It is very important to restore the data in the event of failure to continue operations.

Storing copies of data either on-line or off-line is one of the main security safeguards against loss of data. The objectives of this procedure manual are to ensure availability of critical data and application by performing regular backups, ensure the protection of backup data, and timely restoration of backup data. Also, this procedure elaborates the need for the minimum security controls that must be applied to Information backup, media handling, disposal of media, Information handling procedures and protection of media at transit and at storage.

2. Scope

The scope of this document includes information security aspects that are mandatory for SPARK. The backup requirements are as follows

- Full Database Backup
- Differential Database Backup
- Transactional logs
- Web Application Backup
- Web Server Log (IIS) backup
- Server certificates

3. Full Database backup

3.1 **Daily Full Database Backup:** Full DB backup may be scheduled as an automated process. Backup is to be stored in the hard disk of DB server on the partition earmarked for database backup (eg: E:\SparkDBBack)

Frequency: Daily at 12.30 AM

at 2 AM Compress the backup using 7zip named with Full_bkp_date

Copy 1 :at 4.00 AM copy compressed backup to the server which is not in production at SDC 1.

Copy 2 (SDC 2): This backup file folder scheduled to be copied to the TAPE Library of Data Centre at 5AM everyday. Which should be labeled with the day of the week. Separate media should be used for each day of week (7 tapes, Sun – Sat). These tapes will be reused on a weekly basis.

Copy 3(SPARK-PMU) :at 6.00 AM copy compressed to local system at SPARK-PMU .

Copy 4 (SDC 1): Near DR copy to be created in the SAN partition allotted for SPARK.

Verification: In the morning itself it should be verified that the DB backup has taken place in the server and copied to all four locations as above.

Responsibility: System Administrator / DBA. He will submit a consolidated backup report for the week every Monday to Chief Project Manager, SPARK. The reports should be kept in a separate file titled "SPARK onsite backup log".

Note: Initially daily Full database backup is advised. However, when the DB size becomes larger, full database back may be scheduled on a weekly basis.

3.2 **Monthly Full Database Backup:** Back up of the last day of every month should be copied to a removable media.

Frequency: First day of next month.

Labeling: This backup file need to be labeled with the month name and year (eg: DECEMBER2009.Bak).

Media copy: This should be copied to two removable media, which should be labeled with the month name (eg: DECEMBER), one copy to be kept with SPARK PMU and the other in SDC. Separate media should be used for each month and these tapes will be reused on an annual basis.

Verification: as above

Responsibility: System Administrator / DBA. He will submit a backup report for the month to Chief Project Manager, SPARK. The reports should be kept in a separate file titled "SPARK monthly backup log".

3.3 **Annual Full Database Backup:** Back up of the last day of every calendar year should be copied to a removable media.

Frequency: First day of next year.

Labeling: This backup file need to be labeled with the year

(eg: 2009.Bak)

Media copy: This should be copied to two removable media, which should be labeled as above, one copy to be kept with SPARK PMU and the other in SDC. Separate media should be used for each year.

Verification: as above

Responsibility: System Administrator / DBA. He will submit a backup report for the year to Chief project Manager SPARK. The reports should be kept in a separate file titled "SPARK yearly backup log".

4. **Differential Database Backup:** Differential backup may be scheduled as an automated process. Backup to be stored in the hard disk of DB on the partition earmarked for database backup (eg: E:\SparkDDBBack.).

Frequency: Daily start at 3.00 AM and repeat every 6 Hours

Copy 1 : After 45 Minutes of schedule, copy backup to the server which is not in production at SDC 2. Compress the backup using 7zip named with Diff_bkp_datetime

Copy 2 : After 1 Hour copy last compressed differential backup to the local system at SPARK-PMU .

Copy 3 (SDC 1): Followed by above, Near DR copy to be created in the SAN partition allotted for SPARK.

Verification: It should be verified that the DB backup has taken place in the server and is being copied as above.

Responsibility: System Administrator / DBA. He will submit a consolidated backup report for the week every Monday to Chief Project Manager

SPARK. The reports should be kept in a separate file titled "SPARK onsite backup log".

5. **Transaction log Backup:** Transaction log backup should be scheduled as an automated process. Backup to be stored in the hard disk of DB on the partition earmarked for Transaction log backup (eg: E:\TRLogbak.)

   Frequency: starts at 1.00AM and repeat Every Half an hour.

   Copy 1 : After 15 Minutes of schedule, copy backup to the server which is not in production at SDC 1. Compress the backup using 7zip named with Trans_bkp_datetime

   Copy 2 : Copy last compressed Transactional backup to the local system at SPARK-PMU .

   Copy 3(SDC 1): Near DR copy to be created in the SAN partition allotted for SPARK.

   Verification: It should be regularly verified that the Transaction log backup has taken place in the server and is being copied as above.

   Responsibility: System Administrator / DBA. He will submit a consolidated backup report for the day to Chief Project Manager SPARK. The reports should be kept in a separate file titled "SPARK TrLog backup".

6. **Web server log backup :** Web server log file(s) should be should be copied manually to the partition earmarked for web server log backup.

   (eg: E:\WebLogbackup.)

   Frequency: Every day at 6 PM (The log file may be scheduled to open a new file at 5.30 PM)

   Copy 1(Media copy): This backup to be copied to the TAPE Library of Data Centre every day after the backup.

   Copy 2(SDC 1): Near DR copy to be created in the SAN partition allotted for SPARK.

This should also be copied to a PC, located at SPARK PMU, provided exclusively for keeping backup files. This is a manual function and it should be done on every day immediately after the backup.

Verification: It should be regularly verified that the IIS log backup has taken place at the server and is copied to the PC and tape library.

Responsibility: System Administrator / DBA. He will submit a consolidated backup report for the day to Chief Project Manager SPARK. The reports should be kept in a separate file titled "SPARK IIS Log backup".

7. Certificates

An on-site backup of the server SSL certificate should be taken during each update in certificate.

Off-site backup of certificate should be also taken during each update in certificate.

Responsibility: System Administrator

8. Backup Restoration

8.1 Database Restoration Testing:

On every month / quarter, the data integrity (restore) should be verified.

It should be tested on test server. The name of the DB should be 'sparktestDB'.

It should be verified by the SPARK manager.

All the daily activities should be recorded in a Register.

Responsibility: Database Administrator (DBA).

8.2 Database Restoration during crash

- First take a tail log back up of transaction log. (it can be taken even if the database is offline)
- Database Restoration can be done from the latest Database Backup stored in the server. If the DB Backup is not available in the server, then the latest Database Backup can be uploaded to the DB Server from the Local DB Backup PC or from the Tape Library at Data Centre or DR site.
- The restoration is to be done on spark DB Server.
- Restore the last full DB backup and then restore the last Differential DB backup followed by subsequent transaction log backups in the order of time stamps.
- Finally, restore the tail log backup if one was taken successfully.
- It should be monitored and verified by the SPARK manager.
- All the activities should be recorded in a Register.

Responsibility: DBA.

9. **Storage:** Backup media shall be stored in fire proof cabinets with controlled and restricted access. Backup media must be protected from physical damage by protection against environmental threats, including exposure to heat, moisture, light and electromagnetic fields, and stored and handled in accordance with the manufacturers ,recommendations. Physical access to backup media must be restricted to authorized individuals. Necessary protection policy may be defined and followed for the backup tapes by SPARK PMU as per requirements.

10. **Data retention requirements**

    Data retention period should be defined for all data which are getting backed up. It is suggested to maintain the backups at least for next five years.

11. **Media retention requirements**

    The backup media used for daily/weekly/monthly backups should not be used beyond their recommended lifetime. The backup media will not be used after it gives the error for first time during course of a Backup /Restore. The date of first write on the media should be recorded visibly on the media. Media used for daily backups should be replaced with a new one after six months continuous use.

12. **Disposal of media**

    Discarded backup media must be disposed of in a secure way to make any kind of recovery impossible, e.g. through physical destruction or a similar process.

    All records to be disposed of have to meet the retention requirements before physical destruction of the media. The SPARK PMU shall have a proper e-waste disposal policy.

13. **Monitoring**

    There must be an adequate monitoring mechanism in place in order to detect any fault or error while performing backups. Moreover, all backup requests must be logged and backup jobs must be monitored for success. Backup and restore failures must be logged and reported.