GOVERNMENT OF KERALA

Abstract

Information Technology Department – Introduction of Back Up Policy to e-Governance application being implemented by Government Departments/Organisations - Orders issued.

INFORMATION TECHNOLOGY (B) DEPARTMENT

G.O.(MS)No:10/2010/ITD. Dated, Thiruvananthapuram, 05.03.2010

ORDER

Government Departments and Organisations are in the process of implementing e-Governance applications and creating electronic records. There is a chance for loss of electronic records data and in the event of an equipment failure or physical and cyber disaster. A Backup Policy has become important to ensure that the electronic records (application and databases) are not lost due to equipment failure or physical and cyber disaster. The policy would help the Government Departments /Organisations to take action to back up electronic records to minimize the risk of such loss.

In the circumstances Government are pleased to approve the Back Up Policy annexed to this Government Order, and the Policy is made applicable to all e-Governance applications being implemented by Government Departments/Organizations with immediate effect.

By Order of the Governor

DR. AJAY KUMAR

PRINCIPAL SECRETARY TO GOVERNMENT

To

Additional Chief Secretaries, Principal Secretaries, Secretaries.
All Departments in the Secretariat
All Heads of Departments
The Director, Kerala State IT Mission - He is requested to upload the Government Order in the KSITM website.
The Director, IKM
General Administration (SC) Department.
Stock File/Office copy.

Copy to: PA to Principal Secretary (IT)

)

Forwarded/By order

Section Officer

e-Governance Data Centre

Government of Kerala

BACKUP POLICY

1. Overview

This policy defines the backup policy for computers co-located in the e-Governance Data Centre, Govt. of Kerala. These systems are typically servers with internal hard disks / disk arrays or SAN / NAS based storages Servers expected to be backed up include database servers, application servers, web servers, mail servers etc.

2. Purpose

This policy is designed to protect data in the computers to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster in the data centre.

3. Definitions

(i) Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

(ii) Archival - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

(iii) Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system.

(iv) Storage replication - Storage replication is a service in which stored or archived data is duplicated in real time over a storage area network. Storage replication service provides an extra measure of redundancy that can be invaluable if the main storage backup system fails. Storage replication may be done in the same storage array, different storage array/s in the same location or a storage array in a remote location. Immediate access to the replicated data minimizes downtime and its associated costs. The service, if properly implemented, can streamline disaster recovery processes by generating duplicate copies of all backed-up files on a continuous basis. It can also speed up and simplify recovery from a natural or human-caused disaster such as a fire, flood, hurricane, virus, or worm.

(v) Disaster Recovery - The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

4. Scope

This policy applies only to backup and restore of data for all computers and storage equipment in the e-Governance Data Centre, owned and operated by Kerala Government Departments. This does not include the policies for archival, storage replication and disaster recovery

5. Backup Timing

Full backups are to be scheduled nightly on Monday, Tuesday, Wednesday, Thursday, Friday Saturday and. Sunday. All tapes are to be tested on Sunday during day time. Removal of tapes to be kept in safe locker shall be performed after testing of tapes are completed. Loading new tapes shall also be performed during this time.

6. Tape Storage

There shall be separate set of tapes for each daily backup. There shall be additional set of tapes for each Saturday of the month such as Saturday 1, Saturday2, Saturday3, Saturday4 etc. Backups performed on Saturday on the additional set shall be kept for one month in safe locker and used again the next month on the applicable Saturday. Backups performed on Monday through Friday shall be kept for one week and used again the following appropriate day of the week. All tapes shall be properly labelled.

In addition, differential back up should be taken midday, preferably between 1.00 PM and 2.00 PM on all days including Sunday and holidays.

Transaction Log Back up should be done additionally and copied to a remote location every half an hour/one hour depending on system requirements.

The remote Transaction Log Back up need not be retained once the next differential/full backup is taken.

7. Tape Drive Cleaning

Tape drives shall be cleaned weekly and the cleaning tape shall be changed monthly.

8. Monthly Backups

Every month two sets of monthly backup shall be made. One set shall be kept in the tape drive and the other set in the safe locker

9. Age of tapes

The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than six months shall be discarded and replaced with new tapes.

10. Responsibility

The System Administrator or IT manager of each department or his delegate from the IT cell of the department shall perform all backup related activities. He / she shall develop a procedure for testing backups and test the ability to restore data from

backups on a monthly basis. The System Administrator or IT manager shall verify the records and media and certify them on a monthly basis. Restoration of data from backup shall be performed only by the System Administrator / IT manager after obtaining written permission from the department head.

11. Testing

The ability to restore data from backups shall be tested at least once in a month.

12. Data to be Backed Up

Data to be backed up include the following information:

(i) System state data.
(ii) Registry data
(iii) User data
(iv) Applications and their configurations

Systems to be backed up include but are not limited to:

(i) Production database server
(ii) Production application server
(iii) Production web server
(iv) Mail server
(v) Domain controllers, DNS servers
(vi) File servers
(vii) Test database server
(viii) Test web server

13. Archives

Archives are made at the end of every year in December / March based on the archival policy. User account data associated with the file and mail servers are archived one month after they have left the organization.

14. Restoration

Users that need files to be restored from the backups / archives must submit a request to the department head. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

15. Tape Storage Locations

Offline tapes of archives, monthly and weekly backups shall be stored in a fireproof safe locker under the custody of the department head in a different building away from the data centre.

Responsibility

The Backup shall be the responsibility of the Application Administrator where the Department has its own SAN and Tape Library. In case, the application uses SAN & Tape Library of the SDC, it shall be the responsibility to SDC Back up Administrator to undertake backup as proposed.

17. 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.

18. Relaxations

Relaxation to above backup may be done with specific permission of IT Department.