TechSture Technologies

Backup Policy

Document No – TT-ITP/04

Purpose

The objective of this policy is to ensure information integrity for business-critical applications by ensuring periodic backups and restorations.

Scope

This policy is applicable for Techsture IT system servers, computers and others where Techsture is providing IT maintenance services and security devices as per defined department-wise backup and retention procedures and for Department IT systems as per project/account specific backup plans.

Policy

Information Technology recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

Back up of all important Data is taken by IT Administrator.

1. For the Techsture IT systems centralized Backup is taken every Day. This is done from all the Servers to NAS Storage. All these servers and NAS are protected by Antivirus software.
2. On event basis and on request from Project/Group, the most critical data to be backed up is scanned for Virus and then the backup is taken on NAS/Cloud.
3. Back up of database of the application server hosted on the Data Centre is taken on secondary storage periodically as well as to NAS. The system administrator also takes the backup of the data base remotely on regular intervals on Cloud.
4. Back up will be replica of existing server/data.
5. Responsibility of taking backups for individual's Desktops/Laptops lies with the respective user.
6. Backup of servers will occur every day after regular business hours.

Backup Type

Full Backup: Full backup includes all the source files. This method ignores the file's archive bit until after the file is backed up. At the end of the job, all files that have been backed up have their archive bits turned off. Only one full backup will be done once in 7 days followed by incremental backup.

Incremental backup: Includes only files that have changed since the last Full (Clear Archive Bit) or Incremental backup. The next time an incremental backup is done, this file is skipped (unless it is modified again).

On-Site backup: Centralized Backup is taken every day. Daily backup take after day end (after midnight)

Off –Site backup: Any data that requires offsite storage must be requested by the owner of the server.

Handling, Packaging, Storage and Preservation

All backed-up resources (DVDs and backup media) are stored in a safe (fire-proof cabinets) and protected place to prevent them from dust, heat and physical damage like scratches.

While transporting the DVDs and backup media, they are put in a plastic container and properly protected from direct sunlight, heat and electromagnetic field. **Refer _Media Handling Policy** for detailed process.

Backup Testing/Restore

Backed-up data are checked for its integrity and effectiveness through restoration of selective data on monthly basis.

Retention Period

IT Department provides the **retention policy** to create a persistent and automatic backup retention policy for controlling how long backups and copies should be retained. When a backup retention policy is in effect, IS Officer considers the backups and copies of data files and control files as obsolete (i.e., the backups / copies are no longer needed). The retention policy is continuous process. IT Department does not automatically delete the backups or copies.

There are two options for implementing a backup retention policy:

1. IT Department, retain backups up to period of 7 to 8 years or as per work order/agreement.
2. IT Department then determines which backup should be obsolete and checks period as per work order / agreement.
3. System admin will inform to superior if any error occurred during in backup process, issues will have recorded in Ticket system.
4. Any records or evidence of incident should be retained for at least 3 years and should be reviewed quarterly. It will be disposed by the decision of ISMS Team.

Roles and Responsibilities

Roles and responsibilities details are mention below.

User/Group	Responsibility	Comments
Technical Director, IT Administrator	System Administrators	• Data Backup Verification • Verify Backup storage device • Restoration of backup • Download/Upload backups • System/web/App Servers logs backup and verification

Database Server backup and Procedure

- DB Admin will take Database Backup and verify on daily basis, they will inform to system admin by email if any system related issue occurred during backup.
- DB Admin will assign backup data to IT Administrator for safely keeping database backup. The procedures for DB backup and storage will follow the guideline mentioned in the previous section of this document.

Roles and Responsibilities

Server access roles and responsibilities details are mention below.

User/Group	Responsibility	Comments
-IT Administrator -Technical Director	DB User/System Administrator	• Schedule Database Backup • Monitoring Backup process • Database Back up and Restoration • DB Backup verification and restoration process

Firewall/System logs backup and Procedure

System admin will take firewall logs and configuration backup on daily basis, they also monitoring real-time firewall logs in day times.

Roles and Responsibilities

User/Group	Responsibility	Comments
- Information Security Officer	IT Department	- Monitor Firewall events - Take Monthly firewall configuration backup

Destruction/ Transfer of Media to 3rd party

- Media (magnetic or optical or in other forms), not limiting to one which has reached/passed, the expiry date or is damaged and not in use shall be destroyed in a manner that prevents the recovery of the information.
- Tools and procedures shall be used to wipe off and /or destroy the physical form of such media owned by the organization.
- It should be ensured that all the data/information should be wiped out using authorized data erasing tools (such as kill disk/ de-magnetization tools) prior to handing over to 3rd party/disposal.

Following table shows the options of media disposal and their applicability and Conditions:

Media Type	Tool	Conditions
Paper	Shredder	-
CD/DVD	Break CD into pieces after use	CD media being optical in nature cannot be degaussed
Hard Disks	Disk Manager/Format	- Temporary Disposal for cases like desktop/ laptop reissues. - Hard Disk can be reused.
Hard Disks	Hard Disk Demagnetizer	- Permanent Disposal for cases like customer contractual requirements or disposing data with Confidential/Very Confidential data. - Hard disk cannot be reused. - Approval must to be taken prior to Disposal as it is a cost decision. - Physical destruction of the HDD media for cases like permanent disposal

All destruction of the media to be authorized by Technical Director/CEO of the company with log record to be kept.

Other Records and Backup

- CCTV Backup

  As a part of premise security and surveillance of the entire area CCTV backup must be kept for past 30 days from the present date. The CCTV backup should also be taken into NAS storage and backup to be kept there.

  The roles and responsibility of CCTV backup to rest with IT Security Officer and daily backup file to be provided to IT Administrator for NAS storage.