TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.10.01 - Backup and Recovery

PURPOSE: Departments are responsible for the creation of electronic and/or paper copies of institutional data and retention of that institutional data as defined by HSCEP OP 10.09, Records Retention Operating Policy. Disaster Recovery backups are not considered a valid retention mechanism for record retention purposes and must not be used by departments to meet record retention requirements.

REVIEW: This policy will be reviewed once a year by the Managing Director of Datacenter Operations and will be approved by the Chief Information Officer (CIO).

POLICY/PROCEDURE:

Shared resources (e.g., Network File Shares) serve as the primary method of protecting institutional data. Non-business-related data must not be stored on shared resources and are subject to deletion. No end user devices (e.g., personal computers or laptops) are backed up. It is up to end-users to make sure critical data are saved in department file servers. Institutional server backups are performed primarily for disaster recovery purposes. Institutional servers are backed up based on the schedule listed below. Backups are periodically tested to ensure they are sufficient and reliable

Nightly - Incremental backups will be performed to retain data until the next full backup is performed.

Weekly - Full data backups will be performed and data retained for 14 days.

Archive – 12 Monthly backups and 7 yearly backups will be retained for critical data.

Data Restoration

Shared resource data may be restored, provided the backup is within the storage timeframe as defined above. Restoration of shared resource data may be requested through the TTUHSC El Paso Information Technology (IT) Department's work order process.

Emergency Recovery:

Datacenter Operations Group will make every attempt to recover the data within one business day. For physical servers, this will apply only after the application has been reinstalled. However, in the event of a major incident (natural and human created), services and data may be unavailable for an extended period of time. Major incidents include, but are not limited to: Fire, flood, tornados, earthquake, computer crime terrorist actions and sabotage.

Non-emergency Recovery:

Shared resource data may be restored, provided the backup is within the storage timeframe as defined above. Restoration of shared resource data may be requested through the TTUHSC El Paso Information Technology (IT) Department's work order process.

Email Retention

Email is managed by Texas Tech University Health Sciences Center (TTUHSC) in Lubbock.

- Email backups are for disaster recovery purposes only. Restoration of individual email boxes is not possible.

- Email in the Deleted Items folder will automatically be permanently deleted 30 days after the email is placed in the Deleted Items folder.

- Email in the Junk E-mail folder will automatically be permanently deleted 15 days after receipt.

- Permanently deleted (either automatically because of retention dates or manually by the user) email is recoverable by the end-user with 30 days of the date of permanent deletion using Outlook Tools or Outlook Web Access.

- Disclaimer Statement. TTUHSC El Paso reserves the right to interpret, change, modify, amend or rescind any policy in whole or in part at any time without the consent of employees.