TOSM Storage Services

Memorandum of Understanding

DOCUMENT REVISION HISTORY:
10/27/2016 – added sections 3.5 and 3.6 to communicate the functional account restriction for administrative access
10/26/2016 – modified section 4.5 to include that the customer must contact TOSM to make administrative access changes
7/13/2018 – added 2.1.10 datacenter firewall, added 2.2.1.4 to address DR capabilities; updated storage offerings and prices
7/13/2018 (cont) – added 4.3 data compliance
9/16/2021 – Updated on-call link

The department of Technology Operations and Systems Management (TOSM) provides its customers with various IT-related services, including departmental storage for institutional data. This document describes the Storage Services that are available to Texas Tech University (TTU) and Texas Tech University System (TTUS) departments and colleges and serves as a Memorandum of Understanding (MOU) for this service between TOSM and its Customers.

1.0 Overview

This MOU is between TOSM, who is the service provider, and the Customers of this service, the department and colleges of TTU and TTUS. This document outlines the details of the Storage Services provided by TOSM as well as the roles, responsibilities and expectations of both parties while providing a framework for problem resolution and communication.

2.0 TOSM Storage Services

2.1 Service Description – The TOSM Storage Services provide the Customer with a network-accessible data storage for their departmental needs. In all cases, the storage infrastructure resides in a secure datacenter location with the following:

2.1.1 Raised floor space
2.1.2 Network/Internet connectivity
2.1.3 Redundant cooling
2.1.4 Redundant power with maintenance bypass
2.1.5 24x7 monitoring of power and cooling infrastructure
2.1.6 Diesel Generator with automatic transfer switch that engages during primary power loss
2.1.7 Closed-circuit video surveillance
2.1.8 Biometric readers for data center entry for approved personnel
2.1.9 Network Intrusion Detection System (IDS) managed by TTU Telecommunications
2.1.10 Datacenter Firewall managed by TTU Telecommunications

2.2 Service Types, Descriptions and Costs

2.2.1 File Share Storage (Isilon)

2.2.1.1 High performance file storage

2.2.1.2 Primary data resides in the TOSM data center

2.2.1.3 Includes real-time replication to offsite facility for minimal downtime during a disaster

2.2.1.4 Uses snapshot technology for backups and allows customers the ability to restore their own files. Snapshots are available for 30 days.

2.2.1.5 Cost is $.20/GB per year

2.2.2 File Share Storage (no replication)

2.2.2.1 Single-instance storage with no offsite copy.

2.2.2.2 No backups of the data are included.

2.2.2.3 Used primarily as a backup target for data that can be easily reproduced or for data that is already backed up by other means.

2.2.2.4 Cost is $.10/GB per year

2.2.3 Archive Storage (FileFly/Caringo)

2.2.3.1 Combination of Block/Object storage solution to provide better price point

2.2.3.2 Archive/Object data is replicated between TOSM and our offsite datacenter for disaster recovery.

2.2.3.3 Uses traditional backup methodologies (nightly full backups with daily incremental; 30-day retention) for block data. Uses object versioning for archive data protection and file recovery (Caringo).

2.2.3.4 Used most commonly as a backup and/or replication target for large amounts of departmental data

2.2.3.5 Cost is $.10/GB per year

2.2.4 Onsite FC Storage (CML/MD)

2.2.4.1 Onsite single-Instance fiber channel storage

2.2.4.2 No backups of the data are included

2.2.4.3 Primarily used to simulate large amounts of local storage

2.2.4.4 Can also be used as a replication target for FC storage originating offsite

2.2.4.5 Costs are $.10/GB per year

2.2.5 Offsite FC Storage (CML/MD)

2.2.5.1 Offsite single-Instance fiber channel storage

2.2.5.2 No backups of the data are included

2.2.5.3 Primarily used to simulate large amounts of local storage to offsite systems

2.2.5.4 Can also be used as a replication target for FC storage originating onsite to satisfy disaster recovery requirements

2.2.5.5 Costs are $.10/GB per year

3.0 TOSM Responsibilities

3.1 TOSM will provide all storage infrastructure, including the maintenance and lifecycle replacement costs of the software and hardware used to deliver the Storage Services.

3.2 TOSM will provide all storage backup infrastructure, where applicable, including the maintenance and lifecycle replacement costs of the backup software and hardware.

3.3 TOSM will monitor infrastructure for system availability.

3.4 TOSM will perform system upgrades, when possible, during our normal maintenance windows. The windows are Saturday evening from 6:00pm to Sunday 6:00am, and Sunday, 6:00pm to Monday, 12:00am.

3.5 TOSM will work with designated departmental storage administrators (2 per department) to ensure that only authorized personnel can modify permissions.

3.6 TOSM will monitor permissions to ensure that only authorized individuals (not functional accounts) have the ability to modify folder and file permissions. Neither functional accounts nor nested groups will be allowed administrative access in an effort to prevent the circumvention of TOSM security controls.

4.0 Customer Responsibilities

4.1 Customers are responsible for compliance with all TTU Information Technology Security Policies. The TTU Information Technology Security Policies may be found by visiting http://www.depts.ttu.edu/infotech/security/.

4.2 Customers are responsible for providing TOSM with up-to-date contact information of technical contacts within the department, including name, email address and phone number. If contact information changes, the Customer is responsible for notifying TOSM of the change.

4.3 Customer is responsible for notifying TOSM of any and all data stored on these storage platforms that fall under specific compliance guidelines. This includes, but not limited to, PII, PCI, FERPA, HIPPA and DFARS. Depending on the type of compliance required, TOSM may or may not be able to provide a compliant on-premise storage option. These requests will be handled on a case-by-case basis and TOSM, in conjunction with the appropriate ISO, will work with the customer to find a suitable solution.

4.4 Customer is responsible for accepting the MOU for each Storage Service provided to the Customer and covered under this MOU.

4.5 Although TOSM will assist when possible, the Customer is responsible for application troubleshooting that utilizes a TOSM Storage Service for data storage and will remain the primary contact for their end users for application-related issues.

4.6 The Customer is responsible for managing the permissions and access to their Storage Service using eRaider account credentials. Permissions will be assigned and managed using TTU Active Directory accounts and groups. Up to 2 storage administrators may be designated from each department to manage the permissions of each Storage Service. If the storage administrator needs to be changed, the Customer must contact TOSM to make the change.

4.7 Permission issues that pose a threat, as determined by the institution’s ISO, the Security Operations Center (SOC), or TOSM Security personnel must be rectified by the Customer within a reasonable amount of time or the storage will be disabled and removed from the network until the issues are resolved. If a security breach is suspected on a Storage Service, the Customer is required, by campus policy, to immediately report the incident to their institution’s Information Security Officer (ISO). As a courtesy, we’d also appreciate an email to TOSM at security.tosm@ttu.edu with the details of the incident to help us ensure the integrity of other systems within the data center.

4.8 The Customer is financially responsible for annual Storage Service fees.

5.0 Problem reporting and issue resolution

5.1 TOSM will provide assistance to address issues involving the accessibility of the data residing on TOSM Storage Services. The resolution of application issues not related to the accessibility of the data residing on TOSM Storage Services will be the sole responsibility of the Customer.

5.2 TOSM Storage Service accessibility, availability or performance issues identified by the Customer should be reported to TOSM as soon as they are identified via email addressed to serversupport.tosm@ttu.edu. Issues of an emergent nature where production systems critical to the University are not available should be reported using our on-call procedures. This information can be found at https://www.texastech.edu/offices/information-technology/tosm/contact/oncall.php or by visiting our website at http://www.tosm.ttu.edu and clicking on the Contact Us link. Other issues will be handled during business hours unless other arrangements have been previously coordinated with TOSM.

5.3 TOSM Storage Service issues identified by TOSM will be communicated to the Customer via email and/or phone.

5.4 Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the Customer is responsible for immediately notifying their institution’s Information Security Office (ISO). As a courtesy, we’d also appreciate an email to TOSM at security.tosm@ttu.edu with the details of the incident to help us ensure the integrity of other systems within the data center.