TOSM Managed Systems

Memorandum of Understanding

The department of Technology Operations and Systems Management (TOSM) provides its customers with various IT-related services, including server management. This document describes the Managed Systems service that is 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 departments and colleges of TTU and TTUS. This document outlines the details of the Managed Systems service 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 Managed Systems service

- 2.1 Service Description – The TOSM Managed Systems service provides the Customer with a physical location for their rack-mount servers and storage while providing full support of the hardware, operating system, and standardized applications installed on the system. In addition to the rack space, the data center provides the following features:
  - 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

3.0 TOSM Responsibilities

- 3.1 TOSM will provide physical rack space to the Customer for rack-mount servers and storage.
- 3.2 Ample, redundant power will be made available to meet system requirements
- 3.3 Ample cooling will be made available to maintain proper operating temperature and humidity
- 3.4 TOSM will be responsible for addressing issues related to the data center infrastructure, including server racks, power, and cooling infrastructure. TOSM will also provide hardware, operating system support and standardized application support for systems that maintain a current hardware warranty.
- 3.5 Network access will be provided in coordination with the appropriate network personnel.

3.6 Access to the loading dock for delivering or removing servers and storage devices from the TOSM data center

3.7 24x7 physical access to the data center for essential personnel when necessary

3.8 TOSM will provide the monitoring of general system health and availability and alerts and notifications will be directed to the appropriate TOSM staff.

3.9 TOSM will provide hardware support provided the server has a current hardware support warranty.

3.10 TOSM will be responsible for ensuring that operating system patches are applied in a reasonable amount of time, to be determined by our Server Security team. When possible, operating system patch maintenance will be communicated to the Customer 72-hours in advance via announcements to TechAnnounce, Network Site Coordinator (NSC) notifications and email distributions. The updates will be applied during one of the normal maintenance windows. The windows are Saturday evening from 6:00pm to Sunday 6:00am, and Sunday, 6:00pm to Monday, 12:00am.

3.11 TOSM will be responsible for firewall configurations and anti-virus installation updates to ensure system integrity.

3.12 If a security breach of the system is suspected, TOSM is required by campus policy to immediately report the incident to the TTU Security Operations Team (SOC).

3.13 TOSM will assist the Customer with troubleshooting standardized applications, but the Customer must remain the primary contact for their end users for application-related issues.

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 coordinating hardware and software purchases and acquisitions with TOSM personnel for systems that will reside at TOSM as early in the process as possible. Systems acquired without the guidance of TOSM personnel are subject to approval and may not be candidates for the TOSM Managed Systems service.

4.3 Customers are responsible for providing TOSM with up-to-date contact information of persons responsible for the server(s), including name, email address and phone number. If contact information changes, the Customer is responsible for notifying TOSM of the change.

4.4 Customer is responsible for completing an MOU Assessment each fiscal year for servers covered under this MOU.

4.5 Customers are financially responsible for all software licensing, software maintenance and upgrades.

4.6 Customers are financially responsible for all hardware upgrades and hardware maintenance contracts for their systems and are strongly urged to keep hardware maintenance contracts current. Systems with expired maintenance contracts may experience significant delays in hardware troubleshooting and hardware issue resolution. The Customer is financially responsible for hardware replacement parts for their systems not covered by their hardware maintenance contracts.

4.7 Customer must not disable or uninstall any application or process that has been installed by TOSM according to TOSM best practices. Please see Server Configuration Requirements for more information.

4.8 In the event that a security breach is suspected, the Customer will be required to fully cooperate with the TTU Security Operations Team (soc@ttu.edu) and TOSM security personnel until the incident has been resolved. Failure to cooperate will result in the system being removed from the network until the incident has been resolved.

4.9 No equipment is to be brought into the data center, removed from the data center or moved within the data center without explicit consent and coordination with the TOSM Data Center Operations group. This includes adding or removing any connection to any device within the data center.

4.10 The TOSM Managed Systems service DOES NOT INCLUDE disaster recovery or business continuity. Disaster recovery options may be available for an additional fee. Contact TOSM Server Support (serversupport.tosm@ttu.edu) for additional information regarding disaster recovery options for your systems. Business continuity planning, testing and implementation are the sole responsibility of the Customer.

4.11 The Customer is financially responsible for network connection costs. TOSM will work with the Customer to coordinate the purchasing of network ports with TTU Telecommunications staff.

5.0 Server Requirements

5.1 System must reside in the data center.

5.2 System must be configured according to TOSM best practices.

5.3 The system firewall will be enabled and configured per TOSM best practices.

5.4 System logs will be sent to the TOSM centralized logging destination.

5.5 TOSM personnel will have exclusive administrative access to the system. Customer access to the system will be limited to the point where system security and integrity cannot be compromised by the Customer.

5.6 All Microsoft Windows servers under this MOU must also comply with the following:

5.6.1 All systems must be configured as member servers on the ttu.edu Active Directory domain and the computer accounts must reside in the TOSM Active Directory Organizational Unit (OU).

5.6.2 System will have anti-virus installed and must be managed by the TOSM anti-virus server.

5.6.3 System will have the Microsoft security updates applied by TOSM during the normal TOSM maintenance windows.

5.6.4 Microsoft's passprop.exe program will be installed with the /adminlockout directive to prevent repeated administrator tries from network sources

5.6.5 All applications installed on the system are standardized applications that involve minimal customization, configuration and maintenance. Examples of standardized applications include Microsoft Internet Information Server and Windows File Sharing.

5.7 All Red Hat Linux systems under this MOU must also comply with the following:

5.7.1 All systems must have a computer account in TOSM Active Directory domain, residing in the TOSM Active Directory Organization Unit (OU).

5.7.2 System must have file integrity checker installed (Aide) as per TOSM best practices.

5.7.3 Systems must have an active RHEL subscription. The Customer is financially responsible for the procurement of support subscriptions.

5.7.4 Systems will have the Red Hat security updates applied by TOSM during the normal TOSM maintenance windows.

5.7.5 All applications on the system are standardized applications that involve minimal customization, configuration and maintenance. Examples of standardized applications include Tomcat and Apache.

6.0 Problem reporting and issue resolution

6.1 Data center infrastructure, server hardware, operating systems, or standardized application issues identified by the Customer should be reported to TOSM as soon as they are identified via email and 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 http://www.texastech.edu/it/tosm/oncall.aspx 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.

6.2 Data center infrastructure, server hardware, operating system, or standardized application issues identified by TOSM will be communicated to the Customer via email and/or phone.

6.3 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) per the IT Security Policies as well as the TOSM Server Security Team (security.tosm@ttu.edu).

7.0 Costs for TOSM Managed Systems service

7.1 Rack space under 10U will be provided to the customer at no cost. Additional rack space beyond 10U will be handled on a case-by-case basis. Availability and costs will vary based on the amount of rack units requested and related infrastructure requirements.

7.2 Ample power will be provided to the customer at no cost as long as the server or storage device can operate on 208v power, requires less than 1KW of peak power and can utilize a C13 power outlet. Specialized power requirements may or may not be possible. If the request can be accommodated, the Customer will assume all costs associated with the request.

7.3 Ample cooling will be provided to the Customer at no cost.

7.4 1 gigabit and/or 10 gbE ports are available to our Customers. The Customer is responsible for network port charges. For current network port costs, please contact TTU Telecommunications.