

Mobile Device Management Service

Service Level Agreement

Table of Contents

- 1 General Overview 2**
- 2 Service Description 2**
- 3 Service Scope 2**
 - 3.1 Included in Service2**
 - 3.2 Service Boundaries.....2**
- 4 Responsibilities 3**
 - 4.1 Service Level Defaults3**
 - 4.2 Customer Responsibilities3**
- 5 Service Availability..... 3**
 - 5.1 Hours of Support.....3**
 - 5.2 Support Description4**
 - 5.2.1 Incident Response Targets.....4
 - 5.3 Change Management Procedure4**
 - 5.3.1 Change Management Policy4
 - 5.4 Business Continuity.....4**
 - 5.5 Dependencies List5**
- 6 Data and Security..... 5**
 - 6.1 Data Policy.....5**
 - 6.2 Security Breach Procedure5**
 - 6.3 Access Control5**
- 7 Service Pricing..... 6**
 - 7.1 Pricing Information6**
 - 7.2 Billing Information6**
 - 7.2.1 Customer Billing Information6
 - 7.2.2 Billing Cycle.....6
 - 7.2.3 Billing Contact Information.....6
- 8 Termination 6**
- 9 Document Review and Updates 7**
- 10 Glossary 7**
- 11 Revision History 7**
- 12 Signatures 8**
- 13 Service enrollment/renewal information 9**

1 General Overview

This Service Level Agreement (SLA) covers service details, expectations, roles, and responsibilities between the Service Provider and its customers and provides a framework for incident resolution and communication.

By using this service, you signify that you have read and understand this agreement, what the service provides, what the service does not provide, and your responsibilities in using the service.

2 Service Description

The Service Provider provides access to an MDM server for Apple Deployment Programs participants to manage their enrolled iOS devices. The Service Provider runs and maintains infrastructure components such as servers, storage, and network that empowers users to deploy and maintain their iOS devices. The user is responsible for the configuration, maintenance, security, and support of their University owned devices enrolled in this service.

3 Service Scope

Service Provider provides the user an MDM server that the user can use to manage their iOS devices. The user is responsible for the installation, configuration, maintenance, and support of their enrolled devices.

3.1 Included in Service

- A highly available MDM server that is accessible world-wide
- A web-based management tool for IT Admins to manage their unit/department iOS devices
- User documentation and orientation training on how to use the MDM service

3.2 Service Boundaries

General service boundaries and limits:

- Service Provider is responsible for any changes made on behalf of the customer and/or user
- Service Provider is not responsible for any changes made by the customer and/or user
- Service Provider does not guarantee that problems caused by a user-made change are repairable, or that systems damaged or lost by such changes are recoverable
- Service Provider is not responsible for supporting services used to provide the MDM service (e.g. Network services)

The following are not included as part of this service:

- Installation, configuration, maintenance, and support of enrolled devices and/or end users
- Apps and iBooks licensing
- Training on device usage

4 Responsibilities

4.1 Service Level Defaults

The MDM service will provide the infrastructure, technology, people, processes, and monitoring tools necessary to deliver this service to customers. The MDM service will:

- Clearly document services and processes
- Meet response times associated with the priority assigned to incidents and service requests
- Manage the MDM service infrastructure (servers, storage, databases, network)
- Maintain monitoring for all critical systems, which includes 24x7 support contracts with all of our vendors
- Manage system resources in order to maximize performance and reliability for all customers
- Provide backups for disaster recovery
- Post alerts for incidents that affect service security, capacity, availability, or continuity

4.2 Customer Responsibilities

The customer, in support of this agreement, agrees to the following responsibilities and/or requirements. The customer will:

- Participate and enroll all devices in the Apple Deployment Programs service.
- Provide at least two IT staff members (at least one primary, one secondary) as a Unit Contact for the service
- Install, configure, maintain, and support the operating system, applications, and security for enrolled devices
- Ensure their enrolled devices meets the Penn State OIS Minimum Security Baseline in its entirety (see: <http://security.psu.edu/training-and-awareness/the-security-series/>)
- Utilize the designated incident reporting process for any incidents

5 Service Availability

This service will be available 24 hours a day, seven days a week (24x7), except when updates are scheduled during the standard maintenance window from 5:00 a.m. to 7:00 a.m., or unscheduled emergency maintenance is required. All incidents and requests reported through the CLC's Help Request system will result in a ticket, gathering user information, and obtaining information about the incident or request needed for initial diagnosis and classification.

5.1 Hours of Support

- Support hours of operation are 8:00 AM to 5:00 PM, Monday – Friday except university holidays, and announced university closures
- Support requests and incidents via the CLC's Help Request system can be sent 24 hours a day, 7 days a week and are processed on the next business day
- Off-hours requests for support and emergency support will be fulfilled on a best-effort basis. Priorities will be determined by the Service Provider based on urgency and level of impact

5.2 Support Description

This service follows the incident management policy, processes, and procedures as described in the Penn State Service Management Program Incident Management Policy, Process, and Procedures document available at smo.psu.edu/documents. Please refer to that document for a detailed description of the policy, processes, and procedures.

5.2.1 Incident Response Targets

This service will operate under the Bronze service level as defined in the Response Targets section of the incident management process document.

5.3 Change Management Procedure

This service implements the change management policy, processes, and procedures as described in the Service Management Program Change Management Policy, Process, and Procedures document available at smo.psu.edu/documents. Please refer to that document for a detailed description of the policy, processes, and procedures.

5.3.1 Change Management Policy

5.3.1.1 Change Calendar

The blackout periods (dates and times the service is prohibited from performing normal maintenance) for this service will be:

- The week before Spring and Fall academic semesters
- The first week of Spring and Fall academic semesters

Exact semester dates can be found on the Penn State's academic calendars found here:

http://registrar.psu.edu/academic_calendar/calendar_index.cfm

5.3.1.2 Communication

All services changes will be announced regardless of the risk level. If a change results in a scheduled service outage, an announcement will be sent to customers at least one week before the implementation of the change. Service change announcements will be sent to customers via regular ITS notification channels. Outages will be announced via the ITS Alerts site.

5.4 Business Continuity

Data Centers

- The MDM service infrastructure (e.g., servers, storage) is located in two separate Penn State data centers

Backups

- The servers are backed up nightly
- The databases are backed up nightly

5.5 Dependencies List

The Penn State services that the Service Provider utilizes to provide its service are:

- Penn State Data Centers
- Networking services
 - Data Center Firewall
 - Core routing
 - IP Address Management
 - Domain Name Service (DNS)
 - Load balancing
- Identity and Access Management services
 - WebAccess
 - Kerberos
 - LDAP-Enterprise Directory Services
- Red Hat Satellite Server and Linux software mirrors
- Apple Provided Services
 - Apple Deployment Programs
 - Apple Push Notifications

The Service Provider has service contracts with vendors to support the equipment and software used to provide the MDM Service.

6 Data and Security

6.1 Data Policy

The disk storage systems used for the MDM service are housed in Penn State Data Centers and managed by Service Provider. The service can host public, internal/controlled, and restricted data other than PCI and HIPAA data as described by the [Penn State AD71 Data Categorization policy](#), provided the user manages the data on his or her MDM site in compliance with the policy.

6.2 Security Breach Procedure

In the event of a security incident with the MDM service, the MDM service team will work with Office of Information Security to address the incident. The Service Provider will notify service customers via regular ITS communication channels as soon as allowed by OIS and describe the nature of the incident, any impact to customers, and what actions need to be taken, if any.

6.3 Access Control

This MDM service uses multi-tenancy, which allows the Service Provider to maintain an MDM server for multiple customers. Each customer is provided a dedicated share of the MDM server to manage their own devices. To control access to this service, the Service Provider uses Kerberos/LDAP for authentication and account management. Each customer will designate at least two users (at least one primary, one secondary) as their Unit Contacts for the service

7 Service Pricing

7.1 Pricing Information

- The price for this service is \$10 per device per fiscal year
- Service rate may change year to year. By May 1st, the Service Provider will announce any rate changes for the following fiscal year
- The customer will provide device counts upon entry into the service. They will be reviewed annually by the Service Provider
 - Customers entering the service will be charged at a prorated rate.
 - The prorated amount will be determined by taking the total annual price and dividing it by 12 months and multiplying it by the number of months remaining in the current fiscal year.
- The customer will not be billed for any new devices enrolled nor will they be refunded for any device removed during the fiscal year
- Customers who terminate from the service do not receive any refunds (See section 8)

7.2 Billing Information

7.2.1 Customer Billing Information

- Users are required to provide the following information when joining the service (See section 13)
 - Budget and Fund Numbers
 - Number of devices
 - Description of Service to provide on the billing
 - Department Billing Contact Name, User ID, and Phone Number

7.2.2 Billing Cycle

- Payment is due upon entry into the service and then annually on July 1st.
- Service billing cycle would follow the fiscal year (July 1 - June 30)

7.2.3 Billing Contact Information

For billing questions:

- Email ITS Financial at: TLTFinancial@psu.edu
- Call ITS Financial at: 814-863-6821

8 Termination

- Customer participation in this service may be terminated for any of the following reasons:
 - Violation of University policy
 - Failure to pay for the service
 - Abuse of the service
 - Failure to abide by the Customer Responsibilities
- If the Service Provider terminates this agreement for any other reason, with a written notice of three-month lead-time, the customer will be supported at the existing level until the end of the active fiscal year.

- If the Customer terminates this agreement, with a written notice of one-month lead-time the following will occur:
 - Service access will be removed at the end of the active fiscal year.
 - No refunds will be given upon termination
 - Customer is responsible for un-enrolling their own devices from the service
- Upon termination all customer information and device information housed on the server will be securely erased in accordance with University policies and procedures. All programs and data located on the server will no longer be accessible by the user.

9 Document Review and Updates

This document will be reviewed once a year, at a minimum. If updates to this document are needed, customer feedback on the proposed changes will be requested before finalizing the document.

10 Glossary

Terminology associated with the service that may need clarification for the customer

Term	Definition
Service Provider	The Service Provider for this service is Teaching and Learning with Technology, a unit of Information Technology Services.
customer	Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees on the service level targets.
Mobile Device Management Server (MDM Server)	a server that remotely manages iOS devices that are accessible via network connections.
user	A person who uses the IT service on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT service directly.

11 Revision History

VERSION HISTORY			
Version #	Date	Revised By	Reason for change
1.0	8/8/2016	MDM Service Team	Initial draft

12 Signatures

This SLA is the complete agreement between Service Provider and the customer and may be amended only by written agreement signed by all involved parties.

The IT Unit’s Director, Financial officer, and Budget Administrator must sign this agreement in order to be valid.

Service Provider:

Jennifer Sparrow, TLT Senior Director

Date

Customer:

Unit Name

IT Director Signature

Date

Printed Name

User ID

Financial Officer Signature

Date

Printed Name

User ID

Budget Administrator Signature

Date

Printed Name

User ID

Please submit this completed SLA electronically to clc-mdm@psu.edu

13 Service enrollment/renewal information

The following information is required for service enrollment or renewal. Return this information with a completed SLA agreement.

Date: _____

Customer Billing Information:

Provide the following information for ITS Financial to processing billing for this service.

Budget and Fund Numbers: _____

Description of Service to use for Billing: _____

Number of Devices: _____

Cost per device per year: \$10.00

Department Billing Contact Information:

Name: _____

User ID: _____

Phone Number: _____

Customer Technical Contact:

Provide at least two IT staff members (at least one primary, one secondary) as a Unit Contact for the service

Name: _____

User ID: _____

Name: _____

User ID: _____

Additional contacts (optional):

Name: _____

User ID: _____

Please submit this completed SLA electronically to clc-mdm@psu.edu