



Texas A&M University
Enterprise Operations
Unified Apple Device Management

Disaster Recovery Plan

Table of Contents

	1
1. Overview.....	2
1.1 Purpose.....	2
1.2 The Service.....	2
1.3 The Service’s RTO and MTD.....	2
2. Personnel.....	2
3. Inventory.....	3
4. Procedures.....	3
4.1 Backup Operations.....	3
4.2 Recovery Actions.....	4
4.3 Testing the disaster recovery plan.....	4
4. Versioning.....	5

1. Overview

This disaster recovery (DR) plan is developed as part of the contingency planning process for services provided by Texas A&M University (TAMU) Enterprise Operations and outlines the procedures and protocols for restoring Jamf Pro services in the event of a disruption, ensuring minimal downtime and data loss. This plan aligns with this service's RTO indicated in the associated BIA.

1.1 Purpose

The major goals of this plan are the following:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the financial and reputational impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

1.2 The Service

Endpoint Device Management – Jamf Pro Production, Test, and Development Instances

1.3 The Service's RTO and MTD

Mission/Business Process	MTD	RTO
<i>Desktop Central Patch Management</i>	4	2
<i>Configuration Deployment</i>	4	2
<i>Reporting</i>	6	4

2. Personnel

List of Personnel Needed for Recovery

Name	Position/Group	email	Phone
Stephen Johnson	IT Manager I	stephen@tamu.edu	
Andrew Barnett	Senior IT Professional II	andrewbarnett@tamu.edu	
Oscar Reyes	System Administrator II	oscar@tamu.edu	
Danielle Narita	System Administrator II	danielle.narita@tamu.edu	
Noah Bruce	IT Professional I	brucenoa2185@tamu.edu	

Bernardo Garcia-Moreno	IT Professional I	bernardogm@tamu.edu	
-------------------------------	-------------------	--	--

3. Inventory

List all workstations, servers, appliances and software that are part of this service and would need to be in place for this service to be functional,

Computer/Software Name/IP	Vendor (if Software)	Own or Leased
Jamf Pro Production Instance	Jamf	Licensed Software
Jamf Pro Test Instance	Jamf	Licensed Software
Jamf Pro Developer Instance	Jamf	Licensed Software

4. Procedures

4.1 Backup Operations

List all files, systems, platforms that are backed up, where they are backed up to, and how often each are backed up.

Item/file Backed up	Backup location	How often
<u>Pending Jamf Services</u>		

4.2 Recovery Actions

To facilitate the rapid restoration of this service, list all items from the inventory section in order of recovery.

Order (from 1 st recovered to last)	Computer/Software
First	Production Jamf Server
Second	Test Jamf Server
Last	Developer Jamf Server

4.3 Testing the disaster recovery plan

In successful contingency planning, it is important to test and evaluate the plan regularly. Use this checklist as you conduct your test and decide what areas should be tested.

1. **Detection:**
 - a. Unified Apple Device team monitors and detects service disruptions or receives communication about stoppage of service.
2. **Escalation:**
 - a. Create new Support Ticket with Jamf Pro and communicate with Jamf Account representatives
 - b. Create IT outage alert within 30 minutes of creating support ticket with vendor.
3. **Communication:**
 - a. Internal: Unified Apple Team member updates leadership and team.
 - b. External: Notify end users via IOC IT Outage.

- 4. **Resolution:** Follow recovery procedures and document findings.
- 5. **Post-Mortem:** Conduct a review and update DR plans accordingly.

Lead Overseeing Testing	Date Tested	Location of Proof/Artifacts

4. Versioning

Name	Contact Info	Action	Date
		<i>Creation</i>	