Implementing A Mobile Device Management Solution

Jacob W. Crowder

Western Governors University

Table of Contents

Summary

We are implementing mobile device management software for a mid-market enterprise company with 2000 employees, most of whom use Apple devices provided by the company’s IT department. The company owner expressed the need for better mobile device security. Many employees had issues with lost phones, which is a security risk if no remote management capabilities were active on the device. Employees were also not required to follow device management policies like password complexity requirements or acceptable device usage. Mobile devices also needed to be updated, leaving security risks on devices across the company. The company needs policies for the proper use and security of mobile devices. They also need procedures for updating mobile devices. IT staff need a way to manage and track mobile devices to prevent devices from being lost or stolen. Implementing a mobile device management system will address the problems identified by the company.

We planned to follow a step-by-step process that starts with assessing the needs of the business. We determined that the company needed remote management software for mobile devices. Then, we implemented policies to address those needs after choosing a mobile device management solution with the required technology to solve them. We decided to implement a password policy and an acceptable usage policy. We also assigned roles and responsibilities to appropriate managers to enforce policies and train employees. Next, we chose a mobile device management solution that fit our needs. Then, we provisioned users and trained IT staff to use the software. We then trained employees to adhere to the mobile device management policies. Finally, we moved to long-term device management, where IT staff regularly wipe, lock, and locate mobile phones while enforcing company policy within the MDM software.

In our project proposal, we detailed outcomes that show the project's success. Included in these outcomes were 15-minute response times for lost and stolen phones for wiping, locking, and locating mobile devices. A 100% participation rate in both the password and acceptable use policies is required for project success. Updates will also be tested and pushed to systems within one week of release from manufacturers.

Drills will be performed to test and log the IT staff's response times. IT staff will also create and maintain an inventory system to ensure participation in corporate policies. IT staff will also log the time necessary to complete updates and patches.

Review of Other Work

The Beginner's Guide to Mobile Device Management (MDM)

The author details the current state of mobile device management. He then talks about the benefits of using mobile device management software. After, he discusses how mobile device management software works. Next, he details the challenges of using mobile device management software. Then, a comprehensive list of best practices for mobile device management is provided. Finally, he discusses the differences between software suites and recommends several choices for specific device environments.

Encouraging users to improve password security and memorability

The authors discuss the research behind password memorability and security. They go into strategies for implementing passwords that are memorable to users. Many aspects of password creation are discussed and detailed. An empirical study was done to determine a user-friendly approach to password creation. They go into the differences in user password creation when faced with strict and more open-ended password policies.

Internet acceptable usage policies

The author details the need for acceptable usage policies in today’s internet-connected world. We are given strategies for writing an acceptable usage policy. The author recommends that only one person works on the acceptable usage policy. He explains, “The department manager, or someone in his or her department, must write the **acceptable** use **policy**. It is better to have the fewest number of people possible involved in writing the **acceptable** use **policy**. The best number of authors is one.” (Gaskin, 1998) Gaskin then details the policy's necessary scope, including email, web traffic, and social media. Gaskin provides an overview of how to introduce the policy to employees and then suggests the creation of a policy committee to oversee the acceptable use policy.

Project Relation Explanation

I used the comparisons section from The Beginner’s Guide to Mobile Device Management (MDM) to choose which software to use for our project environment. “We recommend Jamf for those seeking basic Mac device management capabilities.” (Blanton, 2024) Therefore, we decided to use Jamf’s mobile device management platform.

I used section 2.1 of Encouraging Users to Improve Password Security and Memorability to design the password policy implemented in the project. I decided to use an open-ended password policy approach that focuses on the length of the password and memorability. The research supports that a 16-character minimum is a sufficient length for password security “They found that users have less difficulty to comply with creating a 16-character minimum password compared to an 8-character minimum excluding dictionary words or further restrictions. In addition, passwords with at least 16-characters provide the best security.” (Yıldırım & Mackie, 2019)

I developed our acceptable usage policy using Internet Acceptable Usage Policies. While it is dated, the advice of including email and web traffic-related rules is still relevant today. It is also a great reference tool for why we may want to implement our acceptable usage policy. This article also influenced our strategy for designing the policy; we had only one person working on the policy.

Changes to the Project Environment

Our project introduced solutions for the company's proposed needs. Included in those solutions were the ability of the IT staff to track devices, remote lock devices, and remote wipe devices, as well as enforce company policies. Before the project, the IT staff did not have these crucial device management technologies. The company also lacked policies regarding password requirements and acceptable device usage. We implemented these policies and training for employees to follow the guidelines correctly. Then, we addressed the need for devices to be regularly updated. Previously, the company had no requirements for updating devices. We implemented a schedule to check for updates and then push them to devices. Part of the implementation included designing a test device to check that updates will not affect business operations. While we did implement practical solutions for the IT staff, these changes inconvenienced staff, and many complained about the change in procedures and extra training.

Methodology

Our project utilized a standard waterfall methodology. We followed the five phases of the waterfall methodology. These are the requirements, design, implementation, verification, and maintenance phases. Below, we detail the steps we took in each phase.

Requirements Phase

We looked at the company's problems and decided which features were required and optional. Remote management of devices was a requirement. IT staff needed a way to centrally access and manage these devices to locate, wipe, and lock lost and stolen mobile devices. Policy enforcement was determined to be a requirement. The company largely followed a culture of self-policing their mobile devices. This created a landscape of devices with different configurations and software. This also created a culture of lax password management. IT managers determined that policy changes regarding password requirements and acceptable use were necessary to increase the security of mobile devices company-wide. Furthermore, user training was essential to raise awareness of the new company policies and procedures. IT management then determined that mobile devices needed central patching and update management procedures to homogenize the devices across the company.

Design Phase

During the design phase, we created policies and procedures for following proper password complexity and acceptably using the devices. We designed training to support employees in transitioning to the new procedures. We assigned roles and responsibilities to the IT manager and IT staff. The IT manager was responsible for system oversight and employee training. The IT staff were responsible for completing remote management tasks like wiping, locking, and locating the mobile device. IT staff's permission to use the software was granted only to those needing access. Next, we researched mobile device management software and decided on a Jamf platform because it supports Apple devices. We also needed a central device register or log. IT staff created the log to be used in the implementation phase. IT staff were also tasked with designing a test mobile device.

Implementation Phase

We then moved to implement the designed policies, train users, and provision devices with the mobile device management software. IT management trained the IT staff to use the mobile device management software. Management then trained all employees in the MDM policies we created. The password policy was addressed first, followed by the acceptable usage policy. Employees signed documentation in agreement with the policies. This helped the IT staff ensure that all employees adhered to the policies. We then installed the mobile device management solutions on all devices. We also registered the devices within the central device log.

Verification Phase

During the verification phase, we used our mobile device to test the Jamf MDM environment and ensure it met our needs and requirements. To start, we installed the software on the mobile device. Then, we tested the IT staff's ability to use the features of the MDM software. We tested the ability to track, wipe, lock, and enforce updates and policies. The IT staff logged the time it took to achieve these key tasks.

Maintenance Phase

The maintenance phase was the final phase of the project. We used the mobile device management software features to track, lock, and wipe mobile devices. We enforced the company MDM policies. We also decommissioned devices when they were no longer being used.

Project Goals and Objectives

Goal: Enforce best practice standards

One of our goals was to enforce best practice standards. We wanted to implement a password policy that met basic password complexity requirements. We also wanted to ensure that all devices were being used acceptably. Then, we needed to train employees to follow the policies and procedures.

Objective: Implement a Password Policy

IT staff wrote a password policy that follows best practice standards in the industry. They then designed training to teach employees how to follow the policy. They then set requirements for passwords within the mobile device management software.

Objective: Implement Acceptable Use Policy

IT staff wrote an acceptable usage policy that follows industry standards. Training for this policy was designed. Then, the acceptable usage policy was implemented within the MDM software.

Objective: Implement User and Management Training

IT management trained employees in the password policy and acceptable usage policy. Training days were scheduled and performed. However, a few employees could not attend training due to being busy. IT staff conferred with stakeholders and got approval for two more days of funding to train the employees who missed the initial training.

Project Timeline

Milestone	**Projected Duration (hours or days)**	**Actual Duration**	**Projected Start Date**	**Projected End Date**	**Actual Start Date**	**Actual End Date**
Goal 1, Objective 1	1 Day	1 Day	2/03/2025	2/03/2025	2/03/2025	2/03/2025
Goal 1, Objective 2	1 Day	1 Day	2/04/2025	2/04/2025	2/04/2025	2/04/2025
Goal 1, Objective 3	1 Day	1 Day	2/05/2025	2/05/2025	2/05/2025	2/05/2025
Goal 2, Objective 1	2 Days	2 Days	2/06/2025	2/06/2025	2/06/2025	2/06/2025
Goal 2, Objective 2	2 Days	2 Days	2/10/2025	2/12/2025	2/10/2025	2/10/2025
Goal 2,	3 Days	5 Days	2/12/2025	2/14/2025	2/12/202	2/18/2025

Objective 3					5	
Goal 3, Objective 1	365 Days / Year	365 Days / Year	2/17/2025	Ongoing	2/18/2025	Ongoing
Goal 3, Objective 2	1 Day	1 Day	2/17/2025	2/17/2025	2/18/2025	2/18/2025
Goal 3, Objective 3	1 Day	1 Day	2/18/2025	2/18/2025	2/19/2025	2/19/2025
Project Ends	1 Day	1 Day	2/19/2025	2/19/2025	2/20/2025	2/20/2025

Timeline Narrative

During the first week, everything went according to the timeline. The IT team worked hard to meet the deadlines and completed their deliverables within the given time frame. This finished our work on Goal 1. We then moved to work on Goal 2. Most of Goal 2 went smoothly. IT delivered the password and acceptable usage policy. During Objective 3 of Goal 2, we encountered some pushback from employees who insisted they were too busy for training and, therefore, did not attend the scheduled training days, which created a delay of two days. Initially, the training phase was scheduled for 3 days, but due to the employee pushback, 5 days were instead spent on employee training. With the conclusion of training, we moved to work on Goal 3. Objective 1 of Goal 3 is a continuous aspect of the project. This objective requires IT staff to continue supporting our environment's mobile devices with updates and patches. Objectives 2 and 3 were completed on time with no delays as IT staff were determined to finish the project without any delays.

Unanticipated Scope Creep

The two-day delay in the employee training deliverables caused unanticipated scope creep due to poor communication and involving users too late. The project timeline had to shift by two days for each following objective. Approval for two more days of project funding was needed, including a stakeholder meeting where the issue was discussed. Eventually, the mandatory nature of the training was adequately communicated to the employees, who then attended the required training.

Conclusion

Overall, our project was a success. IT staff can wipe, lock, and locate lost and stolen phones within 15 minutes of being notified. IT staff achieved an average response time of 13 minutes across two tests. IT can now ensure that all devices participate in the password and that there are acceptable use policies. Using the data collected about company devices, we identified all devices within the organization that don’t follow the password and acceptable use policies and enforced participation using the MDM software. IT staff tested their ability to update and patch mobile devices within our given time frame. Four days after the manufacturer's release, IT staff could update and patch our test mobile device with the released update. This fits our given time frame of one week for patching mobile devices.

References

Blanton, S. (2024, November 13). *The Beginner's Guide to Mobile Device Management (MDM)*. JumpCloud. https://jumpcloud.com/blog/mdm-mobile-device-management

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759. https://doi.org/10.1007/s10207-019-00429-y

Gaskin, J. E. (1998). Internet acceptable usage policies. *Information Systems Management*, *15*(2), 20. https://doi.org/10.1201/1078/43184.15.2.19980301/31115.4

Appendix A

Password Policy

Below is a copy of the password policy written and implemented during our project. This proves that IT staff wrote a password policy. Part of our project completion goals is 100% participation in this policy. This would not be possible without having written this policy.

By Signing below, you agree to adhere to and understand the following company policies.

1. **All Devices Must Have Passwords**
2. **Passwords Must Be 16 Characters or More in Length**
3. **Passwords Should Use a Memorable Phrase**
4. **Passwords Must Not Be Shared With Anyone Else or Written Down**
5. **Passwords Will Be Changed Annually**
6. **Passwords May Be Reset and Changed by Contacting the IT department.**

Employee Name Print:____

Employee Signature:____

Date:____

Appendix B

Acceptable Use Policy

Below is a copy of the acceptable usage policy that was written and implemented during our project. This document proves that IT staff wrote an acceptable usage policy. Our project completion goals include 100% participation in this policy. We can enforce these rules and policies by having written this document.

By Signing below, you agree to adhere to and understand the following company policies.

1. **Employees will not harass or send obscene or threatening emails using company devices and email.**
2. **Employees will not send or receive sexually explicit images, videos, or messages using company devices and email.**
3. **Employees will not transmit confidential company information without proper permission.**
4. **Employees will not use company email or devices to send personal messages.**
5. **Employees will not view, download, or display anything of an obscene or illegal nature using company devices and systems.**
6. **Employees will not use company devices to view social media or other off-topic sites during work hours.**

Employee Name Print:____

Employee Signature:____

Date:____

Appendix C

Company Policy User Training

I attached a copy of our training presentation, which was used during the training part of our project. It reviews the policies and then directs employees to sign our acknowledgment forms. This proves that IT staff administered training regarding company policies. One of our project objectives was to train staff in associated MDM policies.