Implementing A Mobile Device Management Solution

Jacob W. Crowder

Table of Contents

Proposal Overview

Problem Summary

A midsize company has been experiencing issues with employees losing their corporate-owned cell phones. The company owner has expressed concerns about the security of corporate-owned mobile devices. Lost or stolen phones are a security risk if someone can access the corporate data on the device. Employees are not required to implement any security or passwords on their phones, nor are they required to update their phones regularly. Devices require the most up-to-date software and operating system versions for the best security. Unpatched devices may be susceptible to known vulnerabilities that an attacker can exploit. Enforcing password and security policies ensures employees have the best device settings. Not implementing these policies leaves gaps in the security of every employee’s mobile device.

IT Solution

Implementing a mobile device management platform and associated policies will mitigate these issues and allow the company greater control over its devices while addressing the owner's security concerns. The key features in mobile device management software, such as remote wipe and lock, enforced updates, and password rules, directly address the issues identified with corporate-owned devices. Remote wipe and lock technology will help mitigate the effects of lost and stolen phones. Enforcing updates ensures mobile devices are running secure software. Requiring employees to follow password policies ensures that only the assigned employee can access the device.

Implementation Plan

Implementing MDM software can be achieved by following a step-by-step process. My plan follows this step-by-step format and allows the business to develop its policies and procedures regarding mobile device management. We start by assessing the needs of the business. Here, we determine the specific technology requirements the business needs to implement.

We determined that the company needs a way to control and track mobile devices remotely. The Owner Identified the need for better security. Then, we identified the lack of company policy surrounding mobile devices. After determining the needs of the business, we move to implement the policies identified as a need.

Now, we address the policies regarding the mobile device management system that must be implemented at an organizational level. We must assign roles and responsibilities, such as who controls the management software, enforces the policies, and is responsible for training users and managers. We then assign permissions based on the decided roles and the appropriate level of access needed for their role. Finally, developing an acceptable usage policy ensures employees know the acceptable use of mobile devices. Next, we choose a mobile device management solution.

When choosing a mobile device management solution, we must ensure that the enterprise MDM solution fits the organization's needs. Once we determine the appropriate solution, we will move to the next step: provisioning and training users.

During the provisioning and training of users stage, we install software on devices and set up user accounts and profiles. By implementing a training program for the software for management staff, we ensure they can train new IT staff in the management software. We also want to ensure that policies are followed by implementing a training program detailing the need to adhere to the MDM policy. We are then left to manage the devices long-term using the chosen technology.

When managing devices, we use the implemented software to manage the mobile devices by enforcing password policies, enforcing the acceptable use policy, remotely wiping and locking phones, GPS tracking devices, continual patch management, and de-provisioning unused devices. This is the final and longest step of the process, as it requires ongoing adherence to the implemented policies and procedures.

Review of Other Work

Summary of Four Works

5 Steps for Implementing Enterprise Mobile Device Management

Mark Desautelle explains a 5-step process for implementing an enterprise mobile device management solution. Desautelle describes why managing mobile devices is critical: “MDM solutions are essential in helping IT tighten security while lightening the workload.” (Desautelle, 2024) Desautelle introduces the benefits of enterprise device management. He then describes the five steps followed by recognizing the changing landscape of businesses and security.

Business sizes: Classifications and characteristics

The Indeed editorial team talks about the differences in business sizes. They detail the main classifications of businesses and their characteristics, such as the number of employees, locations, and specialized roles. Size is a primary determining factor in how a business is classified. Recognizing these differences is important in developing a project that suits our environment.

The other MDM: Why “my device matters.”

Joe McKendrick interviews several business leaders, IT professionals, and CEOs to comprehensively explain why mobile devices matter in today's business world. Industry leaders describe how and why they use mobile devices in their businesses. McKendrick then goes into the changing landscape of mobile access to data. Employees can access data from anywhere they have a device and become much more efficient from that quick and easy access. Mobile devices have also increased the amount of data created in business environments, creating a need to protect even more data. McKendrick then details the need for "a comprehensive, unified endpoint management approach solution" (McKendrick, 2017). This helps businesses manage their devices and secure communications to those devices.

Waterfall methodology for project management

Atlassian explains the details of the waterfall project management methodology. They answer the question, "What is the Waterfall Methodology?". The five stages of the waterfall methodology are then explained: "In a waterfall process, you must complete each project phase before moving to the next." (Atlassian, n.d.) Atlassian then talks about the benefits and limitations of using the waterfall methodology. Then, the differences between waterfall and agile methodology are highlighted. Atlassian finishes with an FAQ, enabling the reader to see commonly asked questions regarding the waterfall methodology.

Relation of Works to Proposal Design

I used 5 Steps for Implementing Enterprise Mobile Device Management to design my Step-by-Step Implementation Approach. The article is also an excellent resource detailing why a company should adopt this technology.

My project rationale is supported and influenced by The Other MDM: 'Why My Device Matters.' (McKendrick, 2017) Many of the talking points in the article support the need for implementing a solution to managing mobile devices. The professionals quoted in the article make a genuine case for why this technology matters.

When detailing the company's current project environment, I referred to Business Sizes: Classifications and Characteristics when deciding on the company's classification. I determined that our company is a Mid-market enterprise. Mid-market enterprises "generally employ between 1,500 and 2,000 people." (Indeed, 2025) This fits our project environment.

My project methodology uses information from the article "Waterfall Methodology for Project Management." I used the five stages of the waterfall methodology to design my project methodology.

Project Rationale

The company needs a way to track and manage their mobile devices. Employees consistently have issues with lost phones. Providing the IT staff and employees with ways to locate, lock, or wipe their phones increases the security of company mobile devices. Unlocked phones are susceptible to data breaches. Lost phones provide little use to the company and have associated costs. Stolen phones may be used for nefarious purposes like impersonation and data theft. The need for the owner to feel secure about their investments was influenced by the

number of phones being lost by employees. Utilizing the remote wipe, lock, and tracking capabilities will ensure that every measure has been taken to manage these devices properly.

The owner identified a need for better security. A company stakeholder (the owner) has recognized the need for better security. The needs of stakeholders should be considered, as they may have projects that rely on mobile devices. Properly addressing the wants and needs of the stakeholders means taking comments about increasing security seriously. Implementing policies to increase security will help stakeholders feel more secure doing business with the company.

The company needs policies in place to enforce proper security. Employees are not required to adhere to any policies, posing a security risk. This organizational issue can be addressed by enabling IT staff to enforce these policies on mobile devices.

Current Project Environment

In the current project environment, we are supporting a mid-market enterprise. The company has 2000 employees, most of whom are using Apple mobile phones provided by the company. Employees also use a mix of Apple and Microsoft operating systems on corporate-owned laptops. These devices have no way for IT to track, lock, wipe, or enforce corporate policies. The company has many specialized roles, including CISO and CIO. These roles enable the owner to delegate responsibility to others. The company has multiple locations within its state and thus needs a solution that will work in a remote environment.

Implementing mobile device management software and policies allows IT staff to track, lock, wipe, and enforce updates to mobile devices enrolled in the management software. This technology also allows IT staff to manage devices that may not be in the main office. The mixed software environment for laptops requires a chosen solution to support that diversity of devices.

Methodology

Our project will be using the waterfall methodology. The waterfall methodology follows five stages of development, each of which must be completed before the next stage. Using our implementation plan, we follow this methodology very closely. The stages are requirements, design, implementation, verification, and maintenance. During the requirements phase, we are assessing the needs of the business. During the design phase, we will write policies and choose which software to implement. The implementation phase will begin by enacting the training and policies for the mobile device management software. In the verification phase, we will test the environment and ensure it meets the business's needs. Then, during the maintenance phase, IT staff can push updates to mobile devices and enforce security policies.

Project Goals, Objectives, and Deliverables

Goals, Objectives, and Deliverables Table

	Goal	Supporting Objectives	Deliverables Enabling the Project Objectives
1	Mitigate the effect of lost or stolen mobile devices.	Enable GPS Tracking in MDM Software.	IT staff can track the location of mobile devices.
			IT staff can locate lost or stolen devices.
		Enable Remote Wipe Technology.	IT staff can remotely wipe data from devices.
		Enable Remote Lock Technology.	IT staff can remotely lock devices.
2	Enforce best practice standards.	Implement a Password Policy.	IT staff have developed a password policy.
			IT staff have implemented the password policy.

			IT staff enforce the password policy.
		Implement Acceptable Use Policy.	IT staff have developed an acceptable use policy.
			IT staff have implemented the acceptable use policy.
			IT staff enforce the acceptable use policy.
		Implement User and Management Training.	Management has developed software training for the IT staff.
			IT staff have been trained in using the software.
			Employees have been trained in MDM-related policies.
3	Ensure devices are updated and patched.	Regularly Check for Manufacturer Updates.	IT staff developed a schedule for checking on available updates and patches.
			IT staff adhere to the check schedule.
		Develop Testing Platform.	IT staff developed a test mobile device.
			IT staff tests all updates on test systems before pushing them out.
			IT staff determine if an update interferes with business operations before updating devices.
		Implement Patch and Update Management Technology.	IT staff enabled patch management on mobile devices.

Goals, Objectives, and Deliverables Descriptions

Goal 1: To mitigate the effect of lost or stolen corporate-owned cell phones and mobile devices.

- We choose technology that reduces the risk and effects of lost and stolen mobile devices.
- GPS tracking, remote wipe, and remote lock will be implemented and enforced on mobile devices.

Objective 1: IT staff will enable GPS tracking in the chosen mobile device management software.

- GPS tracking technology will be enabled on all mobile devices.
- GPS tracking will be enforced on all mobile devices.
- IT staff will utilize GPS tracking technology within the mobile device management software.

Deliverable 1: IT staff can track the location of mobile devices.

- IT staff will be able to use GPS data retrieved from the phone remotely to track the locations of devices.
- This allows IT staff to ensure that devices are with whom they are supposed to be.
- This allows IT to determine if a mobile device appears in a suspicious location.

Deliverable 2: IT staff can locate lost or stolen devices.

- Using tracking capabilities within the mobile device management software, IT staff can locate lost devices.
- IT staff can also locate the device's last location before shutdown.

Objective 2: IT staff enable remote wipe technology on devices.

- Remote wipe technology will be enabled on devices.
- Remote wipe technology will be usable through the mobile device management software.
- Remote wipe technology will be used to wipe the contents of lost and stolen mobile phones

Deliverable 1: IT staff can remotely wipe data from devices.

- Using remote wipe technology within the mobile device management software, IT staff can access the device’s file system and safely delete its contents.
- Lost and stolen mobile devices will have the data wiped to maintain confidentiality of the data.

Objective 3: IT staff enable remote locking technology.

- Remote locking technology will be enabled on mobile devices and the mobile device management software.
- IT staff will use this technology to lock lost and stolen devices so they may not be used unless returned or found.

Deliverable 1: IT staff can remotely lock devices.

- Using remote locking functionality, IT staff can ensure that devices are locked and secure until they are found.
- Using remote locking technology, IT staff can lock stolen devices to mitigate the chances of unwanted access to the device.

Goal 2: Enforce best practice standards when implementing policies, including password complexity and length, acceptable usage, and design training to inform employees about these important policies.

- Policies regarding password requirements will be implemented and enforced using the mobile device management software.
- Using mobile device management software, complexity requirements for passwords will be enforced.
- Using the mobile device management software, password length requirements will be enforced.
- Using the mobile device management software, the acceptable use policy will be enforced.
- User training will be designed and implemented to provide adequate knowledge of company policy.

Objective 1: Implement a Password Policy.

- IT staff must design and implement a password policy that includes complexity and length requirements.

- Using the mobile device management software, IT staff will enforce the password policy on mobile devices.

Deliverable 1: IT staff have developed a password policy.

- A password policy has been written and approved by multiple stakeholders and management staff.
- The policy addresses complexity requirements, including password length and special character use.

Deliverable 2: IT staff have implemented the password policy.

- The password policy has been implemented into the company policies.
- Employees are made aware of the change in policies.

Deliverable 3: IT staff enforces the password policy.

- The password policy is enforced by IT staff using the mobile device management software.
- Employees adhere to the password policy.

Objective 2: Implement an Acceptable Use Policy.

- An acceptable use policy will detail what employees can and cannot do with the devices provided to them.
- The policy will be implemented using mobile device management software.

Deliverable 1: IT staff have developed an acceptable use policy.

- The acceptable use policy has been written and approved by stakeholders and managers.
- The acceptable use policy addresses what employees can and cannot do with company devices.

Deliverable 2: IT staff have implemented the acceptable use policy.

- The acceptable use policy has been implemented into the company policy.
- Employees are made aware of the change in company policy.

Deliverable 3: IT staff enforce the acceptable use policy.

- The IT staff enforces the acceptable use policy using the mobile device management software.

Objective 3: Implement User and Management Training.

- Employees and managers need training to follow the policies and procedures.
- Training will be developed and given to all employees to ensure compliance with the company policies.

Deliverable 1: Management has developed mobile device management software training for the IT staff.

- Managers design training for IT staff to use the mobile device management software.
- IT staff will be provided knowledge of the relevant technologies needed to manage mobile devices enrolled in the software appropriately.

Deliverable 2: IT staff have been trained in using the software.

- IT staff must be trained to use the mobile device management features.
- IT staff will be proficient in using the mobile device management software.

Deliverable 3: Employees have been trained in MDM-related policies.

- Employees have received training in the password policy and acceptable usage policy.

Goal 3: Ensure devices are updated and patched with the latest releases for the best security on corporate-owned devices.

- IT staff will develop procedures for updating and patching devices.
- IT staff will maintain a schedule for routine updates and patches.
- IT staff will develop a testing platform to check updates before pushing them to devices.

Objective 1: Regularly Check for Manufacturer Updates.

- IT staff will check for updates for devices from the associated manufacturers.
- IT staff will design and implement a schedule to check for updates and updating devices.

Deliverable 1: IT staff developed a schedule to check available updates and patches.

- IT staff have designed a schedule to check for manufacturer updates.
- IT staff have been notified about and have access to the schedule.

Deliverable 2: IT staff adhere to the check schedule.

- IT staff adhere to the schedule and check for patches regularly.

Objective 2: Develop a Testing Platform.

- IT staff set up a mobile device to test updates and patches.
- IT staff check all updates and patches for stability before pushing them to devices.

Deliverable 1: IT staff developed a test mobile device.

- A mobile device has been provisioned.
- The mobile device can be separately updated and maintained.
- The mobile device represents a baseline mobile device in the company.

Deliverable 2: IT staff tests all updates on test systems before pushing them out.

- Updates and patches are tested for stability.
- Updates and patches are applied upon completion of testing and analysis.

Deliverable 3: IT staff determine if an update interferes with business operations before updating devices.

- IT staff will check using the mobile testing platform whether the update will cause a service disruption before updating devices company-wide.
- IT staff will determine if the update interferes with business before updating devices.

Objective 3: Implement Patch and Update Management Technology.

- Patch and update management features have been enabled on the mobile device management software and connected devices.

Deliverable 1: IT staff enabled patch management on mobile devices.

- Patch management features are enabled on company-owned devices.
- Update management features are present and enabled on the mobile device management software.

Project Timeline with Milestones

Milestone	Duration (hours or days)	Projected Start Date	Anticipated End Date
Goal 1, Objective 1	1 Day	3/31/2025	3/31/2025
Goal 1, Objective 2	1 Day	4/01/2025	4/01/2025
Goal 1, Objective 3	1 Day	4/02/2025	4/02/2025
Goal 2, Objective 1	2 Days	4/03/2025	4/04/2025
Goal 2, Objective 2	2 Days	4/07/2025	4/08/2025
Goal 2, Objective 3	3 Days	4/09/2025	4/11/2025
Goal 3, Objective 1	365 Days / Year	4/14/2025	Ongoing
Goal 3, Objective 2	1 Day	4/14/2025	4/15/2025
Goal 3, Objective 3	1	4/15/2025	4/16/2025
Project Ends	1	4/16/2025	4/16/2025

Outcome

IT staff will be able to locate phones within 15 minutes of receiving a notification of a lost or stolen phone. IT staff can lock lost and stolen phones within 15 minutes of notification. IT staff can wipe the contents of lost or stolen phones within 15 minutes of receiving notification. IT staff can ensure 100% participation in the password policy. IT staff can ensure 100% participation in the acceptable use policy. IT staff will test and push the updates or patches to mobile devices within one week of manufacturer updates.

A monthly lost phone drill will be done to time the IT staff's ability to respond by locating, locking, or wiping the phone. IT staff will log the time it takes to perform the drill. All mobile devices used for business will be logged into an inventory system and then provisioned with the mobile device management software when being used. This data will be used to monitor and ensure 100% participation in password and acceptable usage policies. When manufacturer updates are available, IT staff will log the time necessary to test and push the updates and patches.

References

Atlassian. (n.d.). *Waterfall methodology for project management*. https://www.atlassian.com/agile/project-management/waterfall-methodology

Business sizes: Classifications and characteristics | indeed.com. (2025, January 29). https://www.indeed.com/career-advice/career-development/business-sizes

Desautelle, M. (2024, May 24). *5 steps for Implementing Enterprise Mobile Device Management*. Tangoe. https://www.tangoe.com/blog/5-steps-for-implementing-enterprise-mobile-device-management/

McKendrick, J. (2017b, April 18). The other MDM: Why “my device matters.” Database Trends and Applications. https://www.dbta.com/Editorial/Trends-and-Applications/The-Other-MDM-Why-%E2%80%98My-Device-Matters-117411.aspx