**To: Chief Information Officer of XYZ**

# From:

# Date:

# Subject: Information System Proposal

# Introduction

A mobile device management guideline defines guidelines for the use and security of mobile devices inside an organization (Wall Street Journal, 2020). Due to the lack of mobile usage standards, our employees expose the organization to cybersecurity dangers, theft, and attempts at corporate espionage. Mobile gadgets are among the most susceptible and unregulated technologies XYZ workers utilize. Immediately a device leaves the bounds of our business; it exposes our sensitive data and equipment to the potential of security breaches. MDM policies apply to various devices, including laptop and notebook computers, all cellphones (Android and iPhone), portable media players, and tablets. MDM policy will apply to all of our workers, involving contractors, full-time and part-time employees, and anyone who uses a mobile phone to obtain corporate data. Regular contractors should be trained on MDM policies and, if necessary, should sign non-disclosure agreements (NDAs).

# Implementation of Proposed Information System

Discovery.

It will entail documenting and visualizing critical company information and operations to utilize shared data to identify and describe all data sources. The process will begin by defining the most vital subject area. Furthermore, an IT designer will build the MDM design in this phase based on the institution's intended methodology and goals for master data management and the organization's present business architecture.

Analysis.

The section will identify authorized information sources for the selected topic area, analyze transformation rules and data flows, enhance metadata descriptions, and specify master data quality standards. Individuals from an approved data management program must participate in this step. It is the most challenging process because it is iterative and involves a range of responsibilities.

Construction.

Constructing the MDM database per the design we defined.

Implementation.

The database is populated with the master data and related metadata for the first subject area, access permissions are defined and implemented, change management mechanisms are designed, and data standards levels for MDM are assessed. The operation will be carried out with the assistance of IT specialists.

Sustainment

Internally managing change for the prototype while developing and launching the next — and then going in the same steps until the MDM program is fully implemented.

**Additional Resources**

Sponsorship by an Executive

MDM implementation is a time-consuming procedure in the firm. Suppose a company is thinking about implementing MDM. In that case, it very definitely already has numerous systems collecting, processing, and reporting on client data, all of which suffer from the consequent volume, diversity, data quality difficulties, and duplication. It took time to create the problem, and it will take time to fix it. The program's success is dependent on a strong executive sponsor. Many organizations are project-based, and funding is sometimes distributed on a project-by-project basis. MDM and other long-term efforts require longer-term support and vision to thrive, which an executive can only provide (*Mobile device management,* 2016). Many businesses function in silos. The concept of master data suggests that it is a collection of information that is shared and of common interest, which is incompatible with a siloed organization. Executive sponsorship allows stakeholders to work together.

An Owner

Application ownership is unclear to XYZ company. Successful MDM implementations have an application owner whose primary responsibility is to keep the MDM program up to date and running smoothly. Due to its central role in a company, MDM's business value and function are intimately linked to its customers. Each of our client applications will have a specific use for our customer data, and MDM is an actual application that all of them can utilize. MDM application decisions can be made in the application owner's best interest of all stakeholders.

# Project Risks and Scope Creep

### During the implementation process, workers will be constantly trained, mentored, and coached on carrying out their tasks according to the MDM policies (Prasetyaningtyas et al 2021).  Securing your mobile devices means preventing security risks from getting into your device from outside sources (shadow IT use). It also means making sure these risks can't get into the company's network if they do. In addition to endpoint security solutions, the company should require that all mobile devices used by the company be installed with a native security app before they can be used.

### “Scope creep is one of the most common project management risks. Generally, scope creep occurs when new project requirements are added by project clients or other stakeholders after the project execution has started” ([ProjectMnager](https://www.projectmanager.com/blog/5-ways-to-avoid-scope-creep)). To avoid scope creep at MDM implementation, we need to define the statement of work clearly, assume there will be change, educate the employees, and filter simple adjustments from new tasks.

Risk Business Environment is **Low Little** or no impact to existing business processes.

Technical Environment is **Medium** Previously implemented technologies with new aspects and/or new requirements.

# Change Management Strategy

Change management must always accompany master data management (MDM) systems. Indeed, it is a vital component determining how successful (or unsuccessful) an organization is with MDM. While change is a natural part of any information management effort, it is more evident with MDM, particularly end-users. Businesses are becoming increasingly data-driven, which means that data is used and managed regularly by staff ranging from analysts to marketing to sales experts. Individual data management methods in a business without MDM (or in a company that is new to MDM) range from simple to sophisticated (Prasetyaningtyas et al., 2021). Spreadsheets abound, and essential data items are shared as users contribute to or manipulate them to address business concerns or manage the operations of their separate groups.

Applications and Resources

AWS Cloud Storage

Databases are critical components of data storage, organization, and retrieval. Additionally, they must create an eCommerce system (*Chapter 7 master data management,* 2020). A good database facilitates e-Commerce and centralizes the management of all correlations. AWS Cloud Storage is more cost-effective for businesses. XYZ eCommerce is built on high performance, an intuitive database design, and excellent scalability and availability. These characteristics will dictate the database type, either interrelated, NoSQL, or a mix.

Diagram

Description automatically generated

Figure . Title ([AWS-Metadata](https://w84iit.wordpress.com/2020/04/19/system-design-dropbox/))

# Evidence of Feasibility

## "Feasibility is the measure of the tangible and intangible benefits of an information system"

## There are five types of feasibility: Economic, Operational, Technical, Schedule, and political. According to Mange Engine, MDM allows personal cluster devices into groups after which specific policies and apps can be distributed easily. In addition, the new system must conduct. Although drafting a BYOD policy and educating employees about the best practices can reduce the chances of data breaches and unauthorized data access, organizations must also consider personally owned devices' overall management. The easiest way to manage a BYOD setup is using BYOD management solutions (BYOD MDM).

## The feasibility and costs of establishing and implementing the new policy and purchasing MDM plus for eCommerce employees' devices are:

XYZ eCommerce has 10,000 employees

MDM Plus annual price per 10,000 on Cloud $39,195 with one technician.

Additional technicians (50): $ 5,995

Total annual Cost for purchasing and implementation of MDM Plus is:

$39,195 + 5,995 = $45,190

Herning IT stuff for Auditing and monitoring network and devices activities:

4 IT specialist 1 Security specialist

IT specialist salary: $125,000 x 4 = 500,000

Cybersecurity specialist: $140,000

Total new stuff salary = $500,000 + $140,000 = $640,000

Total feasibility Cost= $640,000+ 45,190 = $685,190

# Sources

1. Chapter 7 master data management. (2020). Big Data Management, 80–98. <https://doi.org/10.1515/9783110664065-007>
2. Mobile device management. (2016). Security and Auditing of Smart Devices, 121–129. <https://doi.org/10.1201/9781315369372-15>
3. Prasetyaningtyas, S. W., Heryanto, C., Nurfauzi, N. F., & Tanjung, S. B. (2021). The effect of work from home on employee productivity in banking industry. Jurnal Aplikasi Manajemen, 19(3), 507–521. <https://doi.org/10.21776/ub.jam.2021.019.03.05>
4. Wall Street Journal. 2020. How Apple and Google Formed one of Tech's Most Powerful Partnerships. https://on.wsj.com/2JXutjv.