Radboud Universiteit

Faculty of Science

MSc Information Sciences

Master's Thesis

Human-Centered Information Security: Mobile Device Management and Mobile Application Management in Higher Education

How insights into employees' perception of enterprise mobility management can lead to accepted and adopted security policies

Paolo Maggioni

Student Number: 1113737

Supervisor: Dr. Hanna Schraffenberger

Second evaluator: Dr. Ilona Wilmont

External supervisor: Joost Gadellaa

Date: 21st of October, 2025

Word count: 29851

Table of Contents

Abstract

This thesis investigates how Dutch Higher Education Institutions (HEIs) can foster greater acceptance of Mobile Device Management (MDM) and Mobile Application Management (MDM) solutions among their employees while maintaining robust information security controls. Thus, the study addresses the balance between security requirements and employees' usability needs.

Adopting a Design Science Research (DSR) approach, the research combined desk research**,** unstructured interviews with Chief Information Security Officers (CISOs)**,** and semi-structured interviews with employees to identify acceptance factors, find the aforementioned balance, and formulate actionable recommendations. The findings constituted a set of seven policy recommendations that would likely result in good user acceptance while maintaining adequate security levels.

From a theoretical perspective, the study extends the Technology Acceptance Model (TAM) by incorporating communication as a key determinant influencing perceived usefulness and ease of use. Practically, it contributes to the field of human-centered security design by translating abstract principles into practical, risk-based, and awareness-oriented measures.

The results indicate that communication, proportionality, and usability are decisive for increasing user acceptance of MDM–MAM systems and thus higher compliance with the policies. In fact, instances of shadow IT were primarily linked to poor usability and lack of clear risks and security communication rather than deliberate policy avoidance. Hence, transparent explanations of why security measures need to be implemented, which security risks they cover, and how they affected users' daily work should significantly increase policy acceptance levels.

Chapter 1: Introduction

This thesis addresses a pressing challenge in today's IT landscape: the limited acceptance and adoption of security policies and solutions among employees, and the consequent rise in shadow IT. Shadow IT is defined as 'hardware, software, or services introduced and used for work without the explicit knowledge or approval of the organization' (Gadellaa, 2022, p. 20). This research delivers strategies to foster employee acceptance and reduce resistance against Mobile Device Management (MDM) and Mobile Application Management (MAM) solutions in the context of Dutch Higher Education Institutions (HEIs).

The core argument of this research is that successful adoption depends on an organization's ability to balance its security requirements with usability, with users being consulted about their considerations, needs, and concerns around security matters. In fact, previous research has shown that the more users feel they are involved, the more effective the security measures will be (Ki-Aries & Faily, 2017). Furthermore, this study highlights communication as a critical enabler of trust: when security measures are clearly explained and transparently justified, employees are far more inclined to comply (Vedadi et al., 2024).

Choosing HEIs as scope for this research delivers findings useful and impactful for an important sector in Dutch society. In fact, HEIs have become prime targets for cyberattacks (Fouad, 2021; Masaryk University, 2023), making it essential to improve the adoption of MDM and MAM solutions. The goal of this research is to develop policy recommendations that are user-friendly, security-compliant, and effective in increasing security. This objective leads to the following research question (RQ):

"How can higher education institutions increase acceptance of Mobile Device and Mobile Application Management among their employees, considering both employee perceptions and security requirements?"

In this study, *employee perceptions* include their experiences, opinions, and needs regarding security policies.

To answer this question, the research employs Design Science Research (DSR), which combines abduction and deduction phases (Fischer & Gregor, 2011; Brocke et al., 2020). Abduction involves gathering insights from both security departments and end-users through literature reviews, unstructured interviews with security professionals, and semi-structured interviews with employees. Afterwards, deduction uses these insights to design potential MDM/MAM policy solutions that create a balance between usability and security.

The methodological approach of DSR also includes a validation phase, in which the proposed designs are evaluated. Given the scope of a master's thesis, it was not possible to delve into the validation phase in depth. Due to lack of time, as well as contextual complexities, validation occurred during the SURF Security and Privacy conference, where the proposed designs were validated with security professionals and a small number of users. Further validation of the design *with more users* is left for future work. In fact, it is strongly suggested to pursue further research to achieve a deeper level of validation within the education sector, as well as to establish the usefulness of these designs in other sectors.

Nevertheless, this thesis comes with a concrete deliverable, namely a set of recommendations for HEIs on the security controls around MDM/MAM that foster higher acceptance and reduce reliance on shadow IT. From an industry perspective, this research offers actionable guidance for improving organizational security. From

an academic perspective, this work employs the Technology Acceptance Model (TAM) as theoretical framework (more in chapter 3), thereby contributing to the expansion on the body of knowledge around this model. Specifically, this thesis tests the TAM in the context of higher education, offering insights into the role of trust and communication in security policy adoption.

This thesis is structured as follows. The remainder of this introduction clarifies the research problem, the scope of the study, definitions of MDM and MAM, and the rationale for focusing on HEIs. Subsequent chapters present: a literature review, detailing the research gap and relevant security controls (Chapter 2); the theoretical framework, based on an extended version of the Technology Acceptance Model (Chapter 3); the methodology and research methods, including the DSR approach described in detail (Chapter 4); the research process, including sub-findings and the policy design Chapter 5). Then, the findings and the final policy recommendations follow (Chapter 6). Afterwards, the reader will be confronted with a discussion of the proposed design and a critical reflection on the research process, its quality, and limitations (Chapter 7). Lastly, the conclusions highlight both practical implications for SURF members and contributions to academic knowledge (Chapter 8).

1.1 The Problem

In today's organizational landscape, employees are frequently provided with laptops and mobile phones to perform their work activities. These devices are often used for both work and personal purposes, leading to situations where corporate and private accounts and files coexist on the same device. This creates a complex security environment in which sensitive organizational data is potentially exposed beyond the controlled infrastructures. Similarly, users sometimes use different IT tools than

those scoped by the organization. For instance, it is not uncommon in higher education that personal accounts are used for work-related communication and purposes.

Another example is using applications or software that have not been assessed by the organization. During the interviews with security officers of HEIs institutions, the use of tools such as ilovepdf for pdf editing was mentioned as a concern: while this may seem an innocent action, the pdf uploaded to this tool might contain sensitive information, which is now shared with an untrusted third-party. However, during the users interviews for this research, one user mentioned how they never saw warnings when using ilovepdf as a tool for editing pdfs. This shows how the user was not aware of their action possibly being a security risk, demonstrating a lack of proper communication in that specific case.

In response to these security risks, many organizations attempt to secure information and systems through technical tools that block certain unsecure activities, formal security policies for the employees, and awareness campaigns. Despite the efforts, users often show some degree of resistance to stricter policies, as they often perceive security tools and policies as intrusive or disruptive to their daily tasks, resulting in low acceptance and limited adoption (Hwang et al., 2017; Merhi & Ahluwalia, 2018; Khan & AlShare, 2019). This reluctance not only undermines the effectiveness of security measures but also constitutes a security threat in itself, as non-compliance creates further vulnerabilities within the organization's IT ecosystem.

The issue is further exasperated by the phenomenon of shadow IT, defined as 'hardware, software, or services introduced and used for work without the explicit knowledge or approval of the organization' (Gadellaa, 2022, p. 20). For instance, if

an organization mandates the exclusive use of Outlook for official communication but an employee chooses to use a personal Gmail account instead, this activity constitutes shadow IT. Because these tools operate outside the organization's security perimeter, they expose data to a higher risk of being compromised. From a confidentiality and integrity perspective, as described by Samonas and Coss (2014, p. 24), data processed through shadow IT is more susceptible to breaches or disclosures to unauthorized parties. When shadow IT is used, critical security mechanisms such as phishing detection and network monitoring may be circumvented entirely, creating blind spots that could be exploited by malicious parties. Furthermore, in cases where employees handle personal data of colleagues, students, or research participants, the use of shadow IT can lead to violations of data protection regulations such as the GDPR, with severe legal and financial implications.

Mitigating these risks requires more than the implementation of technical security solutions: it is crucial to build a security culture among the employees. To do so effectively, a deep understanding of the human factors that influence employee behavior is needed, including the reasons behind their acceptance of, or resistance against, organizational security policies. Consequently, the challenge is not only to secure the infrastructure but also to balance organizational security requirements with employees' usability needs and concerns, attempting to build trust between the organization security department and the users. This tension between security enforcement and user acceptance constitutes the central focus of this thesis.

The context of this research, HEIs, was chosen for three reasons: despite being critical for society, the education sector often has less resources to use for improvements in their security maturity; it was an easy sector to access thanks to the connections of the researcher; and it offers unique challenges that make the work

more interesting: in fact, universities and large applied-science institutions have a specific organizational structure, as they are typically organized into faculties, schools, and research institutes, each with its own IT landscape, risk profile, and operational needs. For instance, a medical faculty handling sensitive patient-related research data may require stricter security controls than a humanities faculty with primarily open-access data. Central IT departments often define security policies, but implementation is often decentralized, relying on local IT support within faculties or departments. This federated structure can lead to fragmented adoption of MDM and MAM tools, as well as varying levels of compliance across faculties. Understanding this heterogeneity is crucial for designing security solutions that are both effective and acceptable to end users. Hence, HEIs are structurally complex to defend, while they are also particularly vulnerable to security risks due to their open digital environments and diverse user base. Unlike more centralized organizations, HEIs must support a broad range of users, including administrative staff, researchers, and teaching personnel, each of whom interacts with institutional data in different ways and with varying levels of security awareness. Research data, financial records, and personal information about students and staff often coexist in the same digital ecosystem, making HEIs attractive targets for cyberattacks.

1.2 The Scope

This section defines the scope of the present research and clarifies the concepts of Mobile Device Management (MDM) and Mobile Application Management (MAM) as used in this thesis. It also delimits the organizational, institutional, and user context in which the research is conducted.

1.2.1 MDM & MAM

Mobile Device Management (MDM) and Mobile Application Management (MAM) are both components of the broader category of Enterprise Mobility Management (EMM), which also includes Identity and Access Management (IAM) and Mobile Content Management (MCM) (Madden, 2013). In the context of this thesis, the term EMM refers to the combination of MDM and MAM, deliberately excluding IAM and MCM.

MDM primarily regards the security, configuration, and control of the entire mobile device, while MAM focuses on the management and security of specific applications installed on that device. For example, an MDM tool might restrict a laptop's connection to only approved Wi-Fi networks or push mandatory system updates to all devices. A MAM solution, in contrast, would apply security controls only to work-related applications, such as allowing emails to be sent from Outlook only when the device is connected to the institution's secure network. This distinction is particularly relevant in environments where devices are used for both personal and professional purposes.

In Higher Education Institutions (HEIs), two main categories of devices require security management: mobile phones and laptops. Each of these can be either corporate-owned devices (COD), issued to the employee for work purposes, or Bring Your Own Device (BYOD), owned by the employee but used for professional tasks (see Table 1).

Mobile Phones	Laptops	
Definition: mobile phones owned by the employees	Definition: laptops owned by the employees	BYOD
Definition: mobile phones owned by the organization, issued to the employee mainly for business purposes.	Definition: laptops owned by the organization, issued to the employee mainly for business purposes.	COD

[Table 1] – Definitions of BYOD and COD in relation to mobile phones and laptops

Traditionally, security-sensitive organizations, such as banks, preferred to issue both laptops and mobile phones to employees and to enforce strict MDM controls on these COD devices. In the current landscape, however, the cost of supplying and managing two devices per employee is often prohibitive. Consequently, many organizations, including HEIs, permit employees to use their personal phones—and, in some cases, personal laptops—for work purposes (Pierer, 2016).

This change has significant implications for security management. Implementing MDM on BYOD devices introduces further complexities: employees often perceive MDM on personal devices as intrusive because it grants the organization extensive control, such as the ability to monitor usage or remotely wipe the device. This has led to resistance and raised concerns regarding privacy and proportionality (Warner, 2023; Jimshith & Bai, 2024; Silva, 2012). In response, the industry has increasingly started adopting MAM as a less intrusive alternative, since it allows organizations to

secure only the work-related applications without controlling the device as a whole (Silva, 2012; Preus, 2015; Hayes et al., 2020).

Security officers from Dutch HEIs confirm that MDM and MAM are complementary. MDM is most suitable when the organization needs control over the device and its installed software, whereas MAM is particularly useful for protecting data on personal devices. In practice, combining MDM for COD devices and MAM for BYOD devices often provides the best balance between organizational security requirements and user acceptance (Silva, 2012; Khellaf et al., 2022). Table 2 summarizes the key differences between the two approaches. Both MDM and MAM are within the scope of this research.

	MDM	MAM
Definition	Management, security, and control of the mobile device	Management and security of specific applications
Description	Allows for control, monitoring, and management of applications through control of the device. Administrators can make changes to the device settings.	Controls applications, the features of which can be managed by administrators, but it does not control the device itself.

Aim	Protection of the organization's data and devices	Protection of the organization's data
BYOD/COD	Best suited for COD	Best suited for BYOD, useful for COD too
Example	Your device's access code must be at least eight digits.	When adding your work account to Outlook on your device, you have to add a code when accessing Outlook.

[Table 2] – MDM and MAM comparison. Table based on research [Silva (2012), Khellaf et al. (2022), Scarfo (2012), Everphone (2024), Liu et al. (2015)] and on conversation with the Security Department of some Dutch HEIs.

1.2.2 Current Landscape in HEIs

Unstructured interviews with security departments of Dutch HEIs reveal the current distribution of mobile devices (Table 3). COD laptops are nearly universal across institutions, whereas COD mobile phones are relatively uncommon. Conversely, BYOD mobile phones are very common, and BYOD laptops appear with moderate frequency.

Mobile Phones	Laptops	
Very common	Common	BYOD
Uncommon	Very Common	COD

[Table 3] – Mobile devices scope of HEIs' Security Departments

This discovered pattern shapes the scope of this thesis. In fact, the primary focus of this study lies on BYOD mobile phones, for which MAM is the typical management approach, and COD laptops, for which both MDM and MAM are considered. BYOD laptops remain within scope, though they are less prevalent, whereas COD mobile phones are of marginal relevance. Consequently, the semi-structured interviews with employees will focus on the devices most commonly in use; COD mobile phones will only be discussed if raised by participants.

1.2.3 Dutch HEIs

The research is restricted to Dutch Higher Education Institutions, as it is conducted in collaboration with SURF, a cooperative association comprising over 100 research and higher education institutions. These include university hospitals (UMCs), research universities (WO), universities of applied sciences (HBO), and vocational education and training institutions (MBO).

Only research universities (WO) and large universities of applied sciences (HBO) are within scope. This choice is motivated by several considerations. First, these institutions share similar characteristics to the extent that in many countries they would collectively be referred to as "HEIs," which ensures that relevant literature

and theoretical models are more readily applicable. Second, WO and large HBO institutions exhibit greater organizational complexity and diversity of roles compared to MBOs or UMCs, including professors, researchers, teaching assistants, IT staff, and administrative personnel, each with distinct security needs and levels of authority. Third, high mobility among academic staff—such as PhD candidates and postdoctoral researchers—across these institutions justifies considering them as a single context. Finally, practical constraints related to time and feasibility prevent the inclusion of all institution types.

1.2.4 Employees

Within the selected HEIs, the users in scope are employees and PhD researchers. Bachelor's and master's students are excluded, as they typically handle less sensitive data, rarely receive institutional devices, and including them would significantly broaden the research scope. Among employees, only those whose work requires the use of a computer are considered relevant for this study. This includes academic staff (professors, researchers, teaching assistants), administrative staff (e.g., HR, finance, admissions), and IT personnel, but excludes employees whose tasks do not involve access to digital systems, such as facilities support staff.

1.3 The Research Question

As already mentioned earlier, the research question (RQ) guiding this master's thesis is:

"How can higher education institutions increase acceptance of Mobile Device and Mobile Application Management among their employees, considering both employee perceptions and security requirements?"

As explained in the previous sections, there is a clear rationale for focusing on Higher Education Institutions (HEIs), particularly research universities (WO) and universities of applied sciences (HBO). These institutions are characterized by open digital environments, diverse user groups, and federated organizational structures, all of which pose unique challenges for the implementation of security measures.

The scope of this research includes only employees and PhD researchers who actively use computing devices for their work, as outlined in the scope section, while excluding bachelor's and master's students. Within this context, the key components of the RQ, user perception and acceptance, need to be further clarified. The term user perception in this thesis refers to the combination of user experiences, attitudes, and opinions regarding MDM and MAM, as well as the way these influence their willingness to comply with or resist the introduction of such tools. This conceptualization emerged during the unstructured interviews with security departments of Dutch HEIs, which revealed that many institutions are still in the early stages of implementing Enterprise Mobility Management solutions and would benefit from practical insights into how users perceive such measures.

The second key concept, acceptance, is discussed in the theoretical framework section, where it is linked to the Technology Acceptance Model (TAM). Explaining

the concept of acceptance is key for a better understanding of how user perception influences acceptance. This is central to the development of security policies and tools that are both technically robust and organizationally adoptable, thereby addressing the core challenge of this research.

1.4 The Academic and Research Context

1.4.1 Information Sciences

Information Sciences is a multidisciplinary field concerned with the creation, management, security, and use of information in organizational and societal contexts. It encompasses both the technical and managerial dimensions of information technology, including the study of how information systems support organizational goals and how organizations can manage the risks associated with these technologies (ASIS&T, 2023). A central theme within this discipline is the tension between information security and privacy: on the one hand, organizations aim to protect sensitive data and ensure operational continuity, while on the other, they must respect individual privacy and comply with legal requirements (Radboud Universiteit, n.d.). This dual focus makes Information Sciences a particularly relevant field, from which perspective MDM and MAM should be studied.

1.4.2 SURF

This research is conducted in collaboration with SURF, a cooperative association of more than 100 Dutch research and higher education institutions (HEIs), including research universities (WO), universities of applied sciences (HBO), university medical centers (UMCs), and vocational institutions (MBOs). SURF facilitates

collaboration among its members to develop and procure secure digital services, tackle complex innovation challenges, and share knowledge and best practices.

Similar to other organizations, SURF and its members face the challenge of strengthening information security while ensuring that employees adopt the security measures provided. Shadow IT, previously studied within SURF (Gadellaa, 2022), exemplifies this issue.

Consequently, SURF's Security Awareness and Organization division aims to support member institutions in implementing MDM and MAM solutions that achieve both technical security and user acceptance. This thesis contributes to that goal by investigating employee experiences and perceptions of MDM and MAM, ultimately providing practical recommendations for improving policies, tools, and communication to foster higher adoption rates. Greater user adoption is expected to reduce security vulnerabilities and strengthen the overall IT resilience of the participating HEIs.

1.4.3 Dutch Universities

The research context presents unique organizational challenges. Unlike corporate environments where policies are more readily enforced, universities operate in highly decentralized, autonomy-driven structures (Castro & Nyvang, 2018). Faculties and research groups often have distinct technological needs and cultures, and in Dutch society, which places a strong emphasis on individual freedom and academic autonomy, imposing top-down IT policies is particularly challenging (Hisgen, 2016; Khalil, 2013). Security solutions that fail to account for these

organizational and cultural factors risk low adoption, potentially leading to an increase in Shadow IT rather than a reduction.

1.4.4 Academic and Societal Relevance

This research offers both societal and academic contributions.

From a societal perspective, the study directly supports efforts to enhance the information security maturity of Dutch HEIs, which are central assets for society. In fact, universities and applied-science institutions do not merely deliver education; they drive research and innovation, and their operational continuity affects entire generations of students and researchers. Strengthening security in these institutions mitigates the risk of operational disruptions, cyberattacks, and data breaches, including those that could involve sensitive personal or research data (Fouad, 2021; Masaryk University, 2023).

In practice, the findings of this research can guide CISOs and IT security teams in designing Enterprise Mobility Management (EMM) strategies that balance security, privacy, and usability. By incorporating user perceptions and organizational realities, the study aims to reduce resistance, increase acceptance, and consequently limit the prevalence of Shadow IT.

From an academic perspective, the research contributes to the field of Information Sciences in several ways. First, it applies and extends the Technology Acceptance Model (TAM) to the specific context of MDM and MAM adoption in higher education, a domain where empirical research remains scarce. Second, by combining insights from TAM with interviews and validation exercises (including surveys and discussions with CISOs), the study explores new dimensions of user trust and

privacy perception in security policy adoption. Third, it provides practical insights for designing user-centric security measures in decentralized and autonomy-driven organizations, which may inform future research beyond the higher education sector.

Chapter 2: Literature Review

This chapter examines literature relevant to the management of mobile devices and applications in organizational environments, with particular attention to higher education institutions (HEIs). The analysis of the literature available is organized into four sections: Bring Your Own Device (BYOD); company-issued devices (COD); Mobile Device Management (MDM); and Mobile Application Management (MAM). For each topic, the discussion integrates both technical dimensions and human-centered considerations, providing a holistic understanding of the interconnections between technological implementation and user behavior. Also, each section synthesizes findings on security controls and user acceptance, and concludes by identifying the research gap within that subtopic. The chapter concludes with a critical analysis that highlights significant research gaps, thereby marking the rationale for this study.

The goals of this chapter are: to establish a robust theoretical and empirical foundation for this research; to reinforce the definition of the problem explained in Chapter 1; to trace the evolution of research and methodologies in this field; to identify the status quo of knowledge about these four paradigms (BYOD, COD, MDM, and MAM); and to identify what is still missing.

2.1 Bring Your Own Device (BYOD)

The Bring Your Own Device (BYOD) paradigm, where employees use their personal smartphones, tablets, laptops, or other computing devices to access organizational resources, has become a defining trend in contemporary workplaces, regardless of the industry. This is caused by the organizational necessity of enhancing workforce

flexibility, reducing hardware acquisition and maintenance costs, and increasing employee productivity and satisfaction (Cheng et al., 2016; Del Vecchio, 2024). By enabling users to work on devices they already own and are comfortable with, BYOD initiatives can streamline work processes and increase productivity (Naveed et al., 2023).

2.1.1 BYOD: Attack surface and risks

While BYOD presents clear business advantages, it inherently broadens the cybersecurity threat landscape that the organization needs to control. Unlike corporate-issued devices, rigorous control over hardware, software, and security updates can be enhanced, personal devices vary widely in their configuration, security hygiene, and patch levels (Miller et al., 2012; Downer & Bhattacharya, 2015). The nature of BYOD complicates centralized security management and increases exposure to malware, credential theft, data leakage, and compliance violations (Alotaibi & Almagwashi, 2018). For example, users may delay critical operating system updates or install unapproved applications, thereby creating vulnerabilities exploitable by sophisticated attackers.

Systematic reviews of BYOD security risks catalogue these technical vulnerabilities and advocate policy solutions, as access control rules, device enrollment, secure authentication protocols, and data encryption standards (Halim et al., 2024; Ayedh et al., 2023). In line with these solutions, this thesis' recommendations balance the aforementioned technical solutions with user needs, all in order to achieve higher policy compliance.

2.1.2 BYOD in Higher Education

Research focusing specifically on higher education institutions (HEIs) reveals that successful BYOD adoption depends not solely on technical defenses but also significantly on institutional readiness factors such as governance, infrastructure, and user training (Naveed et al., 2023). Unlike commercial enterprises with hierarchical command chains, HEIs must navigate complex faculty cultures, diverse device usage patterns, and varying sensitivity levels. This environment demands adaptive security policies that are flexible enough to accommodate differing risk tolerances while maintaining baseline protections.

Throughout this research, much attention was paid to ensuring that the level of intrusion in personal devices used for work purposes matches the level of risk, and users' non-work-related information on the device is not affected by the security measures adopted.

2.1.3 BYOD: Evolving Threat Landscape in BYOD Environments

Cyber adversaries have adapted their tactics to exploit BYOD's weaknesses. Recent studies highlight ransomware campaigns specifically targeting personal devices used for work, spear-phishing attacks exploiting less-secure personal email and social media accounts, and data exposure risks through cloud synchronization services integrated with BYOD devices (Ratchford et al., 2021; Slonopas, 2024). These trends underscore the necessity of dynamic risk management approaches that extend beyond technical controls to include organizational policies on incident response, role-based access control (RBAC), and the principle of least privilege.

Furthermore, cloud computing integration complicates the security posture by blurring boundaries between personal and corporate data. As users increasingly rely on personal cloud storage and collaboration platforms, organizations face heightened challenges in enforcing data loss prevention (DLP) controls while respecting user autonomy and privacy. The balance between DLP controls and user privacy has been included in this work's research, and the recommendations delivered aim at achieving this balance.

2.1.4 BYOD and The Human Factor: Privacy, Fairness, and Acceptance

A critical dimension emerging from the BYOD literature is the recognition that technical solutions alone cannot ensure security compliance. Employees' perceptions of privacy, fairness/proportionality, and trust in organizational governance fundamentally shape their willingness to adhere to security policies (Boyle et al., 2012; Miller et al., 2012). The tension between organizational control and individual autonomy becomes particularly salient in BYOD contexts, where employees retain ownership of their devices and expect protection of their personal information.

Studies document that when device management tools or policies are perceived as invasive, such as excessive monitoring, forced app installations, or remote wiping without clear consent, employees may resist compliance or engage in "shadow IT" behaviors. Shadow IT includes the unauthorized use of unsanctioned devices, applications, or cloud services to bypass restrictive security controls, which paradoxically increases organizational risk (Boyle et al., 2012; Miller et al., 2012; Ayedh et al., 2023).

Transparent communication, clear privacy policies, and involving users in policy development foster perceptions of procedural fairness, which correlates positively with security compliance. Conversely, ambiguous policies, unilateral enforcement, and lack of user input can fuel distrust and reduce acceptance, undermining security objectives.

2.1.5 BYOD Privacy Models and BYOD Policy Design

The application of privacy models such as the Privacy Calculus Theory is insightful in understanding BYOD adoption dynamics. This theory explains that users weigh the perceived benefits of disclosing personal information (or submitting devices to monitoring) against perceived risks to privacy. Organizations that succeed in BYOD deployment effectively minimize perceived privacy risks through technical and procedural safeguards, thereby encouraging user acceptance (Smith et al., 2011).

However, the concept of privacy is highly subjective, and models as the Privacy Calculus Theory are far from perfect: critiques to this model, specifically for IT products, are frequent. In fact, research explains how there might be a difference between what users mention in conversations (e.g. interviews) and their real inner thoughts about privacy (Norberg et al., 2007). Moreover, Acquisti and Grossklags (2005), Plangger and Montecchi (2020), and Kokolakis (2015) all stress how privacy thoughts and behaviours often do not align with a clear rational and are subject to emotions and biases, leading to a deviation from the Privacy Calculus Theory. Lastly, Meier and Krämer (2022) argue that people don’t always weigh risks and benefits in a rational way.

In practice, while including privacy in this thesis scope is important, it needs to be acknowledged that the findings about privacy may not be applicable on a large scale, due to the high subjectivity of the topics. Nevertheless, designing BYOD policies that respect user boundaries remains important from both an ethical and compliance standpoint. For example, this could mean limiting monitoring to work-related data, providing users with clear visibility into what data is collected, and enabling opt-in mechanisms where possible. Privacy-preserving technologies exist to isolate corporate data from personal data on the same device, promising tools to align organizational security needs with general privacy expectations (Ketel & Shumate, 2015).

2.1.6 BYOD Organizational Culture and Security Behavior

Beyond technical and privacy considerations, the broader organizational culture exerts a profound influence on BYOD security outcomes. HEIs' culture of autonomy and academic freedom contrasts with the approach of rigid device controls (Naveed et al., 2023). Leadership styles that emphasize participatory decision-making, continuous education, and empowerment foster greater buy-in for security policies. Security awareness training tailored to BYOD contexts, highlighting real-world risks and clear instructions for safe device usage, also enhances compliance.

Interdisciplinary studies combining information systems, organizational psychology, and communication theories suggest that integrating social influence mechanisms, such as peer role models and champions within faculties, can amplify positive security behaviors and mitigate resistance (Vance et al., 2014).

2.1.7 BYOD Research Gaps

Despite increasing interest from both organizations and academia, research gaps persist in understanding BYOD acceptance and governance within HEIs. BYOD acceptance studies are rooted in commercial or corporate environments, whose hierarchical, controlled settings differ fundamentally from the distributed, participatory governance models of academia. There is limited research into how decentralized decision-making, faculty heterogeneity, and the other conditions unique to HEIs affect security policy design and user acceptance.

Moreover, there is insufficient attention to the lived experiences of users balancing security demands with personal privacy. The interplay between procedural fairness, proportionality, trust-building, and communication strategies remains underexplored, especially for the scope of HEIs.

2.2 Company-Issued Devices (COD)

Company-Issued Devices (CODs), typically laptops, desktops, or other hardware provisioned, configured, and managed by an institution, represent a well-established strategy in managing information security and operational efficiency within Higher Education Institutions (HEIs). In contrast BYOD, CODs allow for greater standardization and administrative control (Quintanilla, 2025; Goad & Steele, 2023). This section explores the multifaceted nature of COD deployment, the benefits and challenges of such usage, and the current research around organizational culture, human factors, and security governance of COD.

2.2.1 COD Standardization and Technical Control: Strengths and Evidence

The literature consistently underscores that COD adoption enables HEIs to enforce uniform security baselines. Through centralized configuration management, IT teams can implement standardized patching schedules, encryption protocols, endpoint protection, and remote management capabilities (Butkovskiy, 2023). These capabilities translate into tangible operational benefits: uniform hardware and software environments reduce troubleshooting complexity, enhance compatibility, and expedite the deployment of new enterprise tools (Goad & Steele, 2023; Quintanilla, 2025). Empirical studies employing mixed methods, including IT helpdesk metrics and qualitative interviews, confirm that institutions with COD policies report lower device downtime and increased IT support efficiency (Goad & Steele, 2023).

Also, CODs facilitate compliance with data protection regulations, such as GDPR, by enabling enforceable data governance and audit capabilities (Quintanilla, 2025). From a risk management perspective, this level of control reduces the attack surface compared to BYOD models, where device heterogeneity complicates enforcement and control. Quantitative risk assessments frequently highlight reduced vulnerability scores and incident rates post-COD deployment, making COD a go-to solution from a security perspective (Butkovskiy, 2023).

2.2.2 COD: Financial and Resource Trade-offs

Despite technical benefits, COD programs entail substantial financial commitments. Total Cost of Ownership (TCO), including procurement, licensing, maintenance, repairs, and timely device replacement, can hit limited IT budgets (Schall, 2019).

Studies made use of cost-benefit analyses to indicate that while CODs reduce troubleshooting costs and security incident expenditures, these savings do not always offset the upfront capital and ongoing operational costs. Budgetary pressure may lead to deferred device replacement cycles, increasing security risks (Schall, 2019; Abun et al., 2022).

Moreover, COD standardization efforts must reconcile with the diverse needs across faculties. For example, research-intensive departments might require high-performance machines with specialized software, complicating efforts to apply a one-size-fits-all device policy (Abun et al., 2022). This heterogeneity can result in policy exceptions or parallel systems, which dilute the benefits of typical COD standardization. This is a key consideration for security, as even security cannot be exempted from dealing with financial and budget limitations.

2.2.3 COD Technology Acceptance and User Behavior

In the context of CODs, the Technology Acceptance Model (TAM) has seen wide applications. The TAM will be explained more in depth in Chapter 3. For the purpose of the literature review, the applications of the TAM found in the literature suggest that perceived intrusiveness and lack of control are critical barriers to adoption and compliance (Cheng et al., 2016; Glavin et al., 2024). TAM studies often deploy survey instruments measuring constructs like perceived usefulness, ease of use, trust in IT governance, and privacy concerns. Results indicate that employee trust and clear communication about monitoring significantly moderate acceptance levels.

Where trust is low or policies lack clarity, employees may resort to shadow IT practices, undermining organizational security (Boyle et al., 2012). Shadow IT risks

are particularly salient in HEIs, where academic freedom and research autonomy complicate strict enforcement. Qualitative case studies underscore the importance of engaging academic staff in policy co-design to build buy-in.

2.2.4 COD Research Gaps

Although COD policies are extensively studied from technical, financial, and psychological perspectives, significant gaps remain, particularly regarding acceptance and compliance variation across different HEI organizational units. Faculty cultures, discipline-specific technology needs, and research sensitivities introduce complexity that is poorly understood (Naveed et al., 2023). Existing research tends to treat HEIs as homogeneous entities, overlooking nuanced intra-institutional differences.

Additionally, the role of communication strategies and fairness in shaping acceptance has received insufficient empirical attention. How can transparency and participatory governance be operationalized in complex academic settings? Mixed-method longitudinal studies could shed light on how perceptions evolve and how compliance behaviors change over time.

From these gaps, the research learns that possible tailoring of the security policies to each environment within HEIs and the risk it poses, could lead to a supported, risk-based approach, which could lead to higher user policy compliance.

2.3 Mobile Device Management (MDM): status quo and limits

Mobile Device Management (MDM) systems have emerged as a cornerstone technological response to the security challenges posed by mobile endpoints. With mobile endpoints, security research indicates smartphones, tablets, laptops, and any other device used by end-users, such as university staff. Within HEIs, the proliferation of mobile devices has introduced complexity in MDM. The scholarly and industry literature collectively documents the core functionalities of MDM: device enrolment, policy enforcement (such as password complexity and encryption), application whitelisting/blacklisting, remote wipe capabilities, and compliance monitoring. Reseearch also traces their progressive evolution in tandem with the evolving world of endpoint devices (Redman et al., 2011; Disterer & Kleiner, 2013; Joch, 2020; Smith, 2020).

2.3.1 The Technical Evolution and Functional Landscape of MDM

Early MDM solutions were largely reactive, focused primarily on the ability to remotely lock or wipe lost or stolen devices to mitigate data breaches. However, as mobile device adoption expanded rapidly across sectors—including education—MDM tools matured substantially. Contemporary systems now provide integrated policy enforcement that governs password policies, device encryption standards, application control (via whitelisting or blacklisting), and detailed compliance reporting (Joch, 2020). Reviews by Yamin and Katt (2019) and industry analyses (Mindanao, 2025) chart the transition of MDM from standalone device management toward inclusion in broader Unified Endpoint Management (UEM) frameworks,

which seek to consolidate control over diverse endpoint types (mobile, desktop, IoT devices) through a centralized console.

This progression reflects an important recognition: device diversity and user heterogeneity in HEIs necessitate flexible, yet comprehensive management architectures. UEM architectures afford institutions the ability to enforce baseline policies across device classes, while layering contextual, role-based, or device-specific exceptions. For example, a researcher's tablet might have different app restrictions compared to an administrative staff member's laptop, reflecting distinct operational needs and threat models.

2.3.2 MDM Critical Limitations: Ethical, Privacy, and Social Constraints

Despite increasing technical sophistication, the literature converges on two critical and enduring limitations of MDM:

2.3.2.1 Intrusiveness and Privacy Concerns in BYOD Environments

The device-centric design of MDM systems inherently focuses on device control, which can conflict with personal privacy, especially under Bring Your Own Device (BYOD) schemes. Multiple empirical studies have documented that when personal devices are enrolled under organizational MDM policies, users often perceive monitoring, remote control, and data access features as invasive (Boyle et al., 2012; Miller et al., 2012; Alotaibi & Almagwashi, 2018). These perceptions translate into ethical concerns about surveillance, especially in the relation to academic freedom.

Research employing a wide array of methods, from quantitative surveys measuring acceptance and trust to qualitative interviews exploring user narratives, reveals a

consistent pattern: the greater the monitoring capabilities, the lower the acceptance rates and compliance intentions (Toperesu & Van Belle, 2017; Díez, 2023). This is particularly pronounced in HEIs, where academic freedom and privacy are valued highly, complicating the adoption of intrusive security controls. This suggests that users strongly value privacy and would resent tools or policies that monitor their activities.

2.3.2.2 Emphasis on Technical Metrics over User-Centred Outcomes

Another key limitation is that much of the MDM literature remains technology-centric. It predominantly focuses on deployment best practices, technical efficacy, and compliance metrics, such as number of enrolled devices, patch levels, or incident reductions. However, relatively fewer empirical studies engage deeply with the user experience post-rollout (Hayes et al., 2020; Yamin & Katt, 2019).

Where user-focused research exists, it reveals a complex interplay between acceptance, behavioral adaptation, and security outcomes. For instance, perceived invasiveness, lack of transparency about data collection, and insufficient communication significantly undermine adoption and encourage the proliferation of shadow IT workarounds (Díez, 2023; Toperesu & Van Belle, 2017). Such behaviors not only jeopardize organizational security, as previously explained, but also complicate IT incident response and undermine the organization's compliance efforts.

This thesis' core element is the user involvement in the policy design, thereby attempting to overcome particularly this second limitation.

2.3.3 MDM and The Human Factor: Trust, Transparency, and Communication

The literature increasingly frames MDM effectiveness as contingent not only on technical capability but on social legitimacy and user trust. Empirical research drawing on the Technology Acceptance Model (TAM) and trust theory highlights that perceptions of intrusiveness and lack of trust in organizational IT governance critically reduce willingness to enroll devices and comply with MDM policies (Cheng et al., 2016). Trust emerges as a composite construct, involving beliefs that the organization will protect user privacy, use collected data ethically, and minimize disruptions to personal autonomy.

Proper communication and transparency about what data is collected, how it is used, and who can access it are pivotal in shaping these trust perceptions. Studies employing longitudinal surveys and focus groups reveal that poor communication fosters suspicion and fear, leading employees to resist MDM or engage in covert workarounds (Hayes et al., 2020; Glavin et al., 2024). Conversely, transparent governance, where employees participate in policy formation and receive clear, timely information about device management, correlates with higher enrollment rates and better compliance (Siegel et al., 2022). This suggest that communication efforts play a pivotal role in fostering acceptance.

2.3.4 Emerging Practices: Role-Based and Hybrid Approaches

Responding to the limitations of device-centric MDM, vendors and researchers have begun to explore more nuanced and context-sensitive approaches. Role-based policies, which tailor device restrictions and monitoring levels to user roles or job functions, have gained attention for their ability to balance security needs with user

privacy and autonomy (Yamin & Katt, 2019). For example, administrative staff handling sensitive financial data might be subject to stringent controls, while faculty members engaged in less sensitive activities could enjoy more relaxed policies.

Hybrid management paradigms also seek to combine device-level controls with application-level governance or containerization, enabling separation between personal and institutional data on the same device. This approach aims to mitigate privacy concerns in BYOD contexts by limiting organizational oversight to work-related environments (Smith, 2020). However, such models increase complexity for IT management and may require enhanced user education and support.

For this research, role-based policies are particularly relevant, and these will be included in the interview questions to users.

2.3.5 MDM Research Gaps

Despite growing sophistication, the MDM literature presents several notable gaps, particularly if looked within HEIs.

Firstly, user acceptance variability across organizational units. Few studies examine how acceptance of MDM policies varies by faculty culture, research sensitivity, or administrative roles. Given the diverse technological needs and autonomy expectations across academic departments, more granular research is needed to understand these intra-institutional differences (Naveed et al., 2023).

Secondly, longitudinal and mixed-methods studies on behavioral adaptation are lacking. Few longitudinal research track how user attitudes and behaviors evolve post-MDM rollout. Mixed-method designs integrating quantitative compliance

metrics with qualitative user narratives would produce richer insights into adaptation processes (Díez, 2023).

Thirdly, integration of trust, communication, and organizational structure into predictive models. Existing acceptance models often treat communication as add-ons rather than core components. Future theoretical work should embed communication into the theoretical frameworks around acceptance (Cheng et al., 2016; Siegel et al., 2022).

Of these three gaps, only the third falls within the scope of this thesis: proper communication is a critical pillar of the recommendations proposed as a result of this research and of the improved version of the Technology Acceptance Model proposed in Chapter 6.

2.4 Mobile Application Management (MAM)

In recent years, Mobile Application Management (MAM) has gained increasing attention as either a privacy-sensitive alternative or a complementary strategy to traditional Mobile Device Management (MDM). Unlike MDM's device-centric approach, MAM focuses explicitly on securing specific applications and the data therein contained or accessible. This enables organization to obtain application-level information security without necessitating full device control. The core aspect of MAM, thus, shifts from device protection to *data* protection: the priority of organizations has become security the information, and MAM offers a perfect solution to do so. This has positively consequences, particularly for users making use of BYODs.

2.4.1 MAM Functional Overview and current tooling

MAM provides a range of controls targeted specifically at corporate applications, such as OneDrive, Outlook, or other comparable applications from a different provider. These controls include strong encryption of application data at rest and in transit, app-specific conditional access rules, such as multi-factor authentication triggers based on app sensitivity, and selective remote wipe capabilities that can remove the organization's data without affecting personal content on the device. For example, Microsoft Intune offers well-documented implementations of MAM that support unenrolled devices, effectively enabling organizations to protect sensitive institutional data residing in apps on personal devices, while minimizing intrusion into employees' personal digital lives (Microsoft, 2025a).

Microsoft Intune is one of the most prominent enterprise mobility management platforms, with strong focus on MAM. Therefore, most research and online documentation concentrated on this tool, resulting in several organizations across the world employing Intune. In the context of reducing dependencies on US-based tools, this means that EU-based companies and researchers should expand research on and development of European alternatives, in order to offer organizations alternatives, which, currently, are lacking.

2.4.2 Academic and Practitioner Perspectives on MAM's suitability

Scholars characterize MAM as especially suitable for organizational settings where BYOD is prevalent and employee tolerance for device-level controls is low (Batool & Masood, 2020; Ketel & Shumate, 2015; Madden, 2013). Early empirical and practitioner reports indicate that MAM adoption has been most pronounced in

regulated industries, such as finance and insurance, where the sensitivity of data and regulatory compliance imperatives demand robust protections (Batool & Masood, 2020). However, higher education is culturally very different from financial institutions. This means that, to increase security within HEIs, addressing culture and strengthening awareness should be the first step for security departments.

2.4.3 MAM Security Controls, User Acceptance, and the Human Factor

Because MAM tackles applications rather than entire devices, it effectively addresses many privacy concerns linked to device-level monitoring, which have been mentioned in the MDM literature. Empirical studies suggest that MAM policies strike a more effective balance between organizational security needs and user autonomy, resulting in better employee acceptance and reduced perceptions of intrusiveness (Batool & Masood, 2020). This balance fosters higher levels of trust in IT governance, a key predictor of compliance with security policies.

The modularity inherent in MAM frameworks also allows for flexibility in the implementation, with controls being adjustable to the necessities and the risks (Cheng et al., 2016; Yamin & Katt, 2019). For example, by applying stricter controls only on applications handling personal data or sensitive research data, institutions can demonstrate respect for privacy while maintaining robust protection for confidential information. This is very different from the typical one-fit-all MDM solutions, and might enhances user perceptions that security policies are justified, thereby improving compliance.

Nevertheless, despite these theoretical advantages and early practitioner enthusiasm, systematic empirical evaluations of MAM acceptance—especially in higher

education contexts—remain limited. Most published work continues to focus on technical features, deployment models, or vendor case studies rather than independent, user-centred research examining behavioural responses, user experience, or acceptance across organisational subunits (e.g., faculties with different cultural norms or data sensitivities).

2.4.4 MAM Research Gaps

The relative scarcity of empirical research on MAM acceptance in HEIs constrains understanding of its real-world effectiveness and limits evidence-based policy design. However, research in other sectors have provided some useful insights that could be applicable in the HEI context too. Despite this, some gaps have emerged.

The first gap regards organizational communication and transparency: while it is widely accepted that transparent communication about data collection and use enhances trust and compliance (Siegel et al., 2022), how such communication should occur in the context of HEIs is less clear. Also, little research is available on EMM communication, even outside of HEIs. However, there are studies in the field of communication that provide some insight into communication options for EMM tools, and security communication is a well-researched topic.

Secondly, MAM research has not properly established the different needs and cultural differences, not across countries and cultures, nor across organizations and types of organizations, nor across departments within a certain organization. For instance, in the case of HEIs, we already mentioned that they are complex institutions with diverse organizational subcultures. Comparative studies that

explore how acceptance of MAM varies across such subunits would form a research body of factors influencing possibly adoption across said different contexts.

Lastly, the methodology used has not varied: most existing studies are cross-sectional or vendor-driven, limiting insights into how user attitudes and compliance behaviors evolve over time post-implementation. Other approaches, such as a longitudinal mixed-methods research, could provide a richer understanding of adoption dynamics, particularly in institutions with fluctuating personnel and shifting threat landscapes, such as higher education.

Due to the scope of this study, it is not possible to delve properly into specific communication methods across different populations, but general approaches of how to improve EMM communication are explored and delivered in the recommendations.

2.5 Chapter Conclusions

The literature consistently demonstrates that BYOD offers flexibility and user convenience but also elevates security risks; COD mitigates some of these risks while introducing higher costs and managerial complexity. MDM delivers comprehensive, device-level technical control but can provoke significant privacy concerns and reduce user acceptance, whereas MAM provides an application-centric alternative that preserves greater personal autonomy while still protecting institutional data. Recent systematic reviews and vendor documentation indicate a trend toward hybrid, role-based Enterprise Mobility Management (EMM) strategies that combine device and application controls, tailoring them to regulatory requirements and specific use cases.

Despite this progress, three significant research gaps remain. First, the empirical evidence base is dominated by technical evaluations and vendor case studies, with relatively few independent, user-centered investigations. While MDM acceptance has received some scholarly attention, the findings are fragmented and often sector-specific. Research on MAM acceptance is even more limited, particularly studies comparing its behavioral impact to MDM in complex, federated organizations such as universities.

Second, the distinctive organizational characteristics of higher education—decentralized governance, heterogeneous faculty needs, strong norms of academic autonomy, and high mobility of research staff—are under-represented in current acceptance studies. Although recent HEI research has begun to explore BYOD attitudes, few studies compare acceptance across faculties or directly link perceptions to specific policy choices, such as implementing MAM-only strategies for BYOD devices versus MDM for COD endpoints. This gap reduces the transferability of findings and hinders evidence-based policy formulation for HEIs.

Third, while the Technology Acceptance Model (TAM) and its extensions are widely employed, empirical work integrating trust—as a composite construct encompassing both security and privacy—with organizational communication practices and governance structures (centralized vs. federated) remains scarce. Consequently, we lack robust, context-sensitive models explaining when and why employees accept application-level controls (MAM) versus device-level controls (MDM), and how perceived proportionality and communication quality shape these decisions.

Addressing these gaps, this thesis empirically examines MDM and MAM acceptance within Dutch HEIs, focusing on three dimensions: (a) employee perceptions, including prior experience, trust, and privacy concerns; (b) the

comparative suitability of MAM for BYOD mobile phones and MDM for COD laptops; and (c) the moderating influence of organizational structure and communication strategies across faculties. Methodologically, it applies a Design Science Research (DSR) approach, combining artefact design with qualitative interviews and validation exercises. Differently from previous studies, this approach allows for participation in the design process by both security professionals and end-users. Furthermore, very little research has applied DSR to Enterprise Mobile Management solutions, let alone in the context of HEIs. More on the DSR will be explained in Chapter 4.

The analysis resulting from this research aims to produce policy-relevant recommendations that align security requirements with user acceptance, contributing to a nuanced understanding of how EMM strategies can be tailored to the socio-technical realities of higher education. In this way, the policy choice between BYOD and COD is shown to be more than a technical matter—it shapes the range of feasible security controls and fundamentally influences how employees perceive, respond to, and comply with them.

Chapter 3: Theoretical Framework

3.1 The Technology Acceptance Model (TAM)

With the rapid advancement of technology, particularly information and communication technologies (ICT), and their increasing integration into both private and professional spheres, understanding the factors that influence technology acceptance has become increasingly critical. Throughout the years, scholars have developed various theoretical models aimed at explaining and enhancing acceptance by balancing key determinants identified through empirical research (Marangunić & Granić, 2014). Among these, prominent are the unified theory of acceptance and use of technology (UTAUT) and the Technology Acceptance Model (TAM). Both saw different versions of the core model being developed throughout the years, and both are widely used. For this thesis, both were initially considered and their key differences were analyzed. While the TAM is straightforward and, in its core version, focuses on perceived usefulness and ease of use, the UTAUT offers a broader, more nuanced approach by including additional constructs and moderators. The UTAUT is deemed to have more explanatory powers, but its complexity is not suitable for all studies (Rondan-Cataluña et al., 2015; Greener, 2022).

Given the context of a master's thesis, the straightforwardness of the TAM give this model an edge. To still account for good explanatory capabilities, an extended version of the TAM is chosen for this research. Nevertheless, the basic version of the TAM, introduced by Fred Davis in the 1980s, remains one of the most widely applied frameworks, although more recent research has developed extended and newer versions of the TAM. In fact, the relevance of the core TAM components is evidenced by extensive use across diverse domains over several decades

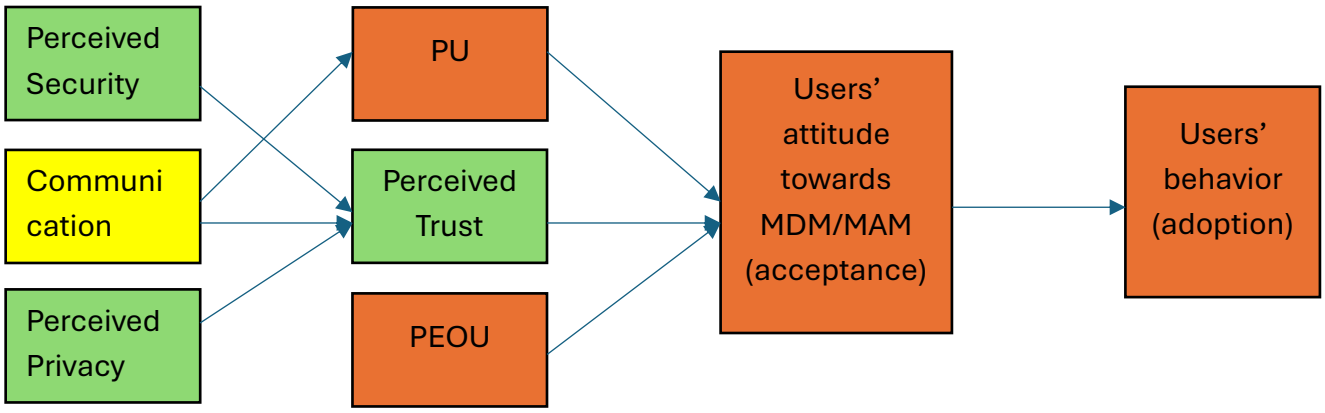
(Marangunić & Granić, 2014). Moreover, authors as Marikyan and Papagiannidis (2024), highly value TAM's core assumption: external variables, such as design features, influence cognitive user responses, namely perceived ease of use (PEOU) and perceived usefulness (PU). In the context of technology, PU refers to how a technology is viewed as contributing to the users' life: the higher the contribution to life perceived, the higher the acceptance. PEOU, instead, looks at how that technology is easy (or difficult) to use: the easier to use, the higher the acceptance. In fact, Davis (1989, 1993) explains that these cognitive perceptions shape the user's attitude or behavioral intention toward the technology, which ultimately determines actual usage behavior.

Expanded versions of the TAM include other cognitive responses, but still keep PEOU and PU in the framework. Even newer versions of the TAM, including TAM2 and TAM3, assert the centrality of PU and PEOU (Marikyan & Papagiannidis, 2024). Consequently, much of the research attention has focused on identifying the external factors that impact PU and PEOU (Marangunić & Granić, 2014; Lai, 2017). However, some attempts have been made to explore the TAM beyond PU and PEOU. For example, Panicker (2020) examines the role of organizational culture and grit as external factors within the higher education context, demonstrating that university culture can directly foster negative attitudes towards technology adoption among staff, thereby influencing their behavioral responses.

For this thesis, of very high relevance is the work of Zhang (2024), which extends the TAM framework by incorporating perceived trust as a determinant influencing PU, PEOU, and user behavior. Zhang's findings indicate that perceived trust has a stronger direct effect on user behavior than on cognitive perceptions of usefulness or ease of use. In her model, trust is constructed through perceptions of security and privacy. Building upon Zhang's augmentation (highlighted in green in Graph 1), this

research further integrates communication (highlighted in yellow), the importance of which was identified beforehand in the literature review, and confirmed during initial unstructured interviews with Chief Information Security Officers (CISOs). These interviews, which will be presented in section 5.3, stress the critical role of effective communication from IT security teams to end-users in fostering technology acceptance.

Accordingly, the adapted Technology Acceptance Model employed in this research, as depicted in Graph 1, serves as the conceptual framework guiding the investigation. This version explicitly includes PU, PEOU, perceived trust (PT), and communication as key constructs. Data collection through user interviews and subsequent validation stages are designed to elicit insights related to these variables.



[Graph 1] – Version of the TAM used in this research, original TAM in orange, TAM + Trust (green), Communication element added (yellow).

Thus, this theoretical framework was built on the concepts explained in the literature review, specifically the findings from sections 2.1.4, 2.1.5, 2.2.3, 2.3.2, 2.4.3, and the overall research gaps highlighted across Chapter 2. This contextualizes the

choice of this specific version of the TAM and creates a foundational structure that delineates the core assumptions and constructs that will be elaborated on throughout this research: PU, PEOU, PT, and Communication. In fact, this theoretical framework functions as an analytical lens through which research question is approached, data is interpreted, and the overall research trajectory is shaped. By grounding the research in this framework, the study ensures that proposed security solutions are also well perceived by the user pool. Lastly, this thesis offers the opportunity of a small-scale test of this framework in the context of HEIs.

3.2 Theoretical Assumptions: from user experience to increased security

This section aims to clarify the key concepts for this research: what constitutes acceptance, how it relates to adoption, and how these processes contribute to increased security.

3.2.1 From User Perception and Acceptance…

Within the domain of technology, acceptance represents a crucial determinant of successful implementation, particularly in workplace settings. Without adequate acceptance, technological advancement and integration in professional environments would face significant barriers. Extensive scholarly work has explored various facets of technology acceptance in the workplace, including acceptance among older employees (Tsertsidis et al., 2019), strategies for promoting responsible acceptance (Toft et al., 2014), and the interplay between acceptance and user emotions (Beaudry & Pinsonneault, 2010).

A growing body of literature highlights the importance of incorporating user experience (UX) considerations into technology acceptance models. Hornbæk and Hertzum (2017), for instance, provide a comprehensive review examining the intersection between the Technology Acceptance Model (TAM) and UX frameworks. They argue that most existing research neglects this critical overlap and advocate strongly for integrating UX dimensions, particularly users' emotional responses, into acceptance studies. This perspective is reinforced by Mlekus et al. (2020), who developed the User Experience Technology Acceptance Model, a hybrid framework combining TAM constructs with insights from UX theory. Moreover, Misron et al. (2011) employed the TAM to empirically investigate the relationship between user perceptions and acceptance of a specific technological tool. Collectively, these studies underscore that user perception and experience are pivotal components of technology acceptance that warrant rigorous examination.

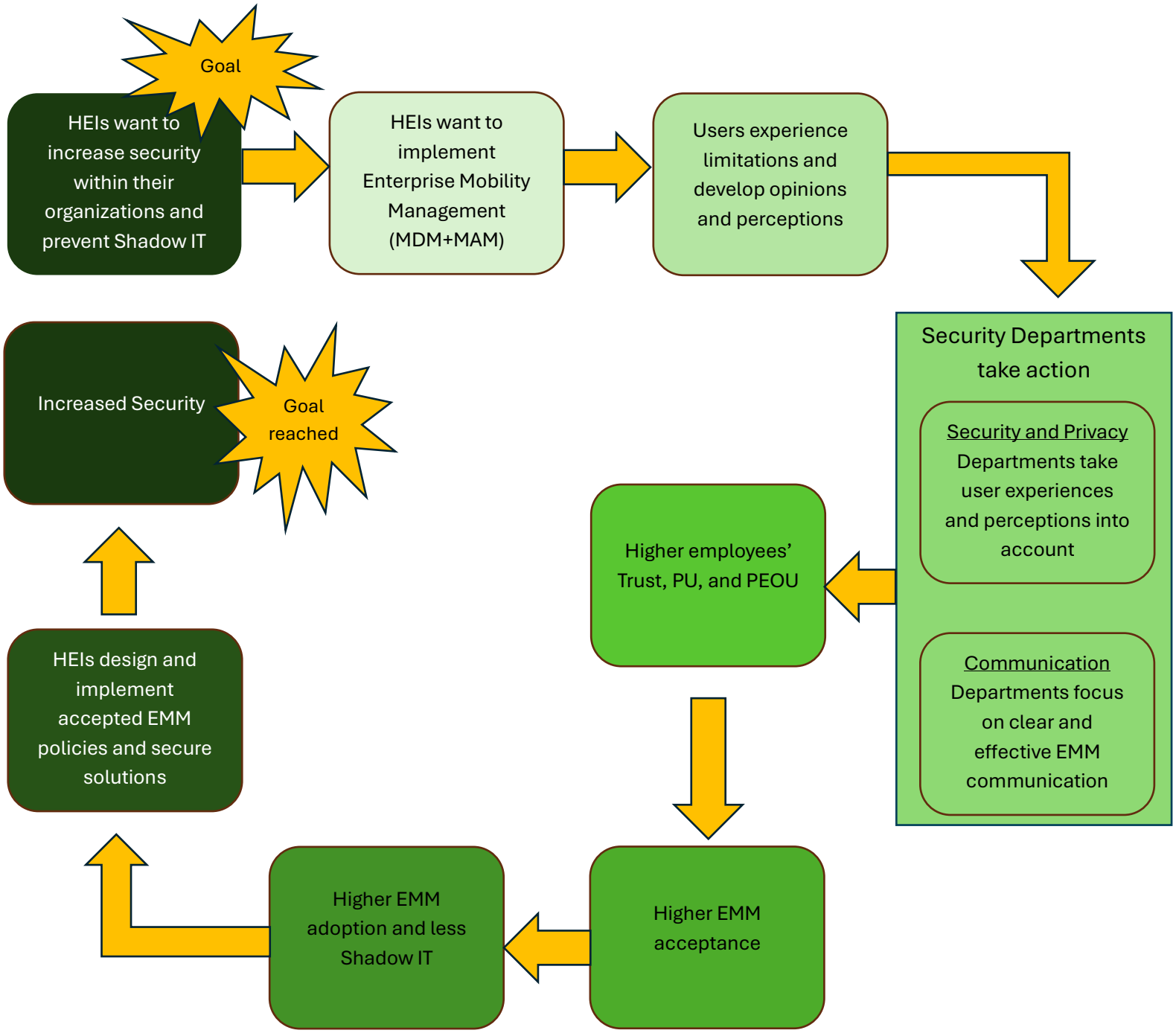
In this thesis, user experience plays a crucial role. In fact, this work puts UX at the center of the design science research process (more on this in Chapter 4): UX is a key aspect to consider when wanting to foster technology acceptance, as better described in Graph 2. In fact, there is strong theoretical and empirical support for the notion that incorporating user experience and user perception insights into the selection of technological solutions and policy development can lead to more adoption, thereby mitigating these challenges. Coupled with clear and effective communication approaches about the rationale behind policies and technological implementations, this approach can significantly enhance acceptance levels.

3.2.2 … to Technology Adoption and Increased Security

Earlier discussions introduced the concept of "shadow IT" and its associated security risks. One significant factor contributing to shadow IT is the lack of user acceptance and, consequently, adoption of officially sanctioned technologies (Raković, 2020). This deficiency often stems from factors such as user dissatisfaction, and poor usability. These issues that can be effectively addressed through careful analysis of user experiences and perceptions. This, as described in section 3.2.1, leads to higher technology acceptance.

At this stage, it becomes important to clarify why acceptance constitutes an essential element for true adoption. In fact, it is not uncommon that employees adopt technology without genuinely accepting it (Renaud & Van Biljon, 2008; Aratovskaya, 2024). This is a problem, as this kind of adoption tends to be effective only in the short term: adoption without acceptance is inherently unstable, with employees being likely to seek opportunities to discontinue the use of a tool they do not endorse or circumvent its use, thereby reintroducing potential security vulnerabilities, as in the case of shadow IT (Aratovskaya, 2024). Consequently, mere adoption is insufficient; genuine, sustained adoption is fundamentally dependent on acceptance (Bürgy, 2023). For this reason, the present research prioritizes the study of acceptance, given its strong tendency to lead to adoption and, ultimately, to enhanced long-term security.

Furthermore, looking at acceptance makes sense when thinking that, generally, acceptance does tend to translate into adoption, especially when external pressures are present. So, when users accept a technology, understand how to use it effectively, there is good communication about it, and there are the conditions to employ it, adoption is highly probable. This process is illustrated in Graph 2 below.



[Graph 2 – Graphic explanation of the connection between user experience and increased security]

This research is drive by the actions in the fourth step of Graph 2: what security departments can do to increase trust, PU, and PEOU.

Chapter 4: Methods and Methodology

4.1 Methodology

To address the central research question—““How can higher education institutions increase acceptance of Mobile Device and Mobile Application Management among their employees, considering both employee perceptions and security requirements?”—the study employs a Design Science Research (DSR) methodology. DSR is a problem-solving paradigm rooted in engineering, aimed at generating knowledge on how artefacts can be constructed or organized to achieve specific objectives, which depend on the research scope and context (Brocke et al., 2020). DSR is well suited to these objectives: prior studies have, in fact, demonstrated its effectiveness in enhancing technology acceptance (Williams, 1996; Kim, 2015; Behne et al., 2021). Notably, Behne et al. (2021) applied DSR to the design of a COVID-19 tracing application. This is a case with large privacy and intrusiveness considerations, not too different from those found in MDM and MAM.

Within the Information Systems discipline, DSR has been widely used to support design of a range of IT tools (Peffers et al., 2007; Horváth, 2007; Teixeira et al., 2016), further supporting its suitability for this study. Despite it not being often use to write policy recommendations, its structure and applicability in Information Science suggest that this methodology should fit this thesis’s research process.

DSR is a well-established methodology. The first formal DSR framework was introduced by Hevner et al. (2004). They positioned DSR within the broader information systems research, highlighting its base in both design science and behavioral science. While the former aims to extend human and organizational capabilities through the creation of innovative artifacts, the latter focuses on

developing and validating theories to explain or predict human and organizational behavior. According to Hevner et al. (2004), these two paradigms are complementary and foundational to information systems, which operate at the intersection of people, organizations, and technology. DSR, in particular, is helpful to advance understanding and solving of problem in the field of information systems by building and using artifacts. In fact, artifacts are its primary means of generating knowledge and producing actionable solutions. In the case of this thesis, the artefact is a security policy, and the objectives are maximizing user acceptance and ensuring security feasibility. The policy-artifact generates knowledge particularly on users' perceptions of MDM and MAM solutions.

Building on the seminal work of Hevner et al. (2004), Peffers et al. (2007) advanced Design Science Research (DSR) by providing a structured process to guide researchers in its practical application. Hevner et al.'s conceptual framework positioned DSR at the intersection of people, organizations, and technology: they claim this methodology is well-suited for studies aiming at designing technological tools that people need to use in an organizational context. In their framework, stakeholders' goals, tasks, and needs are central and they are positioned within the constraints of organizational contexts, structures, and existing technological infrastructures. This ensures that research addresses real user needs and places them centrally in the study without forgetting about the requirements and objectives, for instance security-wise.

Peffers et al. (2007) operationalized Hevner's work into a Design Science Research Methodology consisting of six iterative steps: (1) problem identification, (2) definition of objectives, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication. The first two activities establish the context and the feasibility of the research by defining the problem and setting objectives. The

subsequent design and development phase involves creating the artifact, which may take different forms depending on the objectives. Demonstration and evaluation test the artifact's utility in addressing the problem, while the final communication step disseminates results to relevant audiences, ensuring both scholarly and practical contributions to the relevant industry.

The traditional DSR saw some refinements throughout the years. In fact, the traditional approach often treated evaluation as a discrete, post-design activity. However, this risks overlooking valuable insights during the development process, that would shape and correct the design before its completion. To address this limitation, Sonnenberg and vom Brocke (2012) introduced the concept of concurrent or formative evaluation, emphasizing the need for ongoing assessment throughout the entire DSR cycle. Their framework integrate ex ante (before design completion) and ex post (after design completion) evaluations, This is a viable approach that provided excellent results (Venable, vom Brocke, & Winter, 2019). This is very useful in this thesis: ex-ante evaluation saves time and allows the researcher to address concerns earlier in the process. Hence, in this research, the ex-ante evaluation is done through internal validation across interviews, building later interview questions integrating points made or topics raised in earlier interviews.

Together, Hevner et al.'s foundational framework, Peffers et al.'s structured process model, and Sonnenberg and vom Brocke's iterative evaluation approach have shaped modern DSR into a rigorous, context-sensitive, and impact-oriented methodology. This evolution enables IS researchers to develop artifacts that are not only theoretically sound but also demonstrably effective in addressing complex organizational and technological challenges.

4.2 Methods

This thesis adopts an exploratory applied research approach to investigate potential Mobile Device Management (MDM) and Mobile Application Management (MAM) solutions suitable for higher education institutions (HEIs). The research is primarily qualitative and inductive in nature: semi-structured interviews with diverse stakeholders generated observations from which patterns emerged. These patterns, along with general conclusions, are presented in later sections. However, to ensure the wider validity and applicability of these findings, they require subsequent testing. This validation stage integrates qualitative and quantitative deductive methods: during the SURF Security Conference, quantitative polls and qualitative discussions with both end-users and security experts were conducted to assess whether the proposed policy would be perceived as effective by a broader audience. By confirming that solutions identified through desk research and user interviews are acceptable to a representative segment of employees, this validation process enhances the practical relevance of the study for security departments.

The study combines primary and secondary research methods. Primary data were gathered through interviews, while secondary data were obtained via a systematic review of relevant literature. Regarding primary data, this thesis employs three types of conversations: informal conversations with four SURF employees from the security team; unstructured interviews with six (Chief) Information Security Officers; semi-structured interviews with eight employees. For secondary data, research was conducted by mean of the Radboud University online library and other reputable libraries such as Google Scholar. Preference was given to peer-reviewed sources as far as possible. In some circumstances the use of grey literature was needed as it added value, for instance by presenting cases of MDM usage in the

business world. Also, sources from Microsoft were critical to present some of the technical possibilities available for implementation of MDM and MAM.

4.3 Applied Design Science Research

This section presents how DSR is applied to this study drawing on the steps of this methodology as explained in the literature. In order to provide overview, the table below [Table 4] summarizes the steps of Design Science Research (DSR) as described in Peffers et al. (2007). Each step will be then described in detail. Peffers' approach has been validated by other researchers (Lapão et al., 2014; Teixeira et al., 2016; Brocke et al., 2020). Then, this section explains in detail every step of DSR and maps them to the actions taken in this research.

DSR (Peffers et al., 2007)	**My Steps**	**How**	**Where**
#1: Problem Identification	Understand the status quo of MDM/MAM and where the issues with acceptance of technology in HEIs lie	This was mainly achieved through conversations with SURF employees, literature review, and the unstructured interviews with (C)ISOs.	Sections 5.1, 5.2, and 5.3

#2: Objectives of a solution	Determine what the goal is: increasing security within HEIs through a security policy that accounts for both the security requirements and the users' perception of MDM-MAM	This was mainly achieved through conversations with SURF employees, literature review, and the unstructured interviews with (C)ISOs. Particularly important was the desk research done to establish solid theoretical framework (TAM).	Chapter 2, and Sections 5.1, 5.2, and 5.3
#3: Design and Development	Design a proposal for a security policy that aligns with the objective of the solution. The design is based on the technical possibilities understood through desk research, on the institutions' security requirements, and on the users' needs,	Next to the desk research, critical were the unstructured interviews with (C)ISOs to understand the technical possibilities, and the requirements. Likewise, essential were the semi-structured interviews with users, to understand their perspective.	Sections 5.3, 5.4, and 5.5

	concerns, and tolerance level.	Combining these three elements resulted in the design of a policy. In short, this step draws from the interviews to design user-friendly MDM/MAM policies and solutions	
#4: Demonstration #5: Evaluation	Validation of the policy proposal	Polls and discussion during SURF Conference with both end-users and security experts The validation verifies whether the security controls in the designed policy would see wider acceptance and whether security professionals see the policy as implementable	Section 5.6

#6: Communication	Recommendations for SURF's members	A brief explaining the policy recommendations.	Appendix 8

[Table 4 – Thesis steps mapped to DSR steps)

#1 Problem Identification

In Design Science Research (DSR), the problem identification stage is foundational, as the relevance and clarity of the problem directly determine the significance of the resulting artifact (Peffers et al., 2007). This stage lies on the principle that design efforts must be grounded in a well-defined problem space that reflects both practical needs and theoretical gaps (Gregor & Hevner, 2013). According to Simon's 1996 notion of the "sciences of the artificial", effective problem formulation requires understanding the environment in which an artifact will operate, including organizational context, stakeholder expectations, and technological constraints (Simon, 2019, cited in Peffers et al., 2007). By thoroughly exploring this context, researchers ensure that subsequent design efforts are not only technically sound but also aligned with the realities of the domain in question.

In this study, problem identification consists of a proper understanding of the current EMM issues in higher education: security controls around EMM, while essential for organizational security, often generate tension between the security objectives and individual user concerns and usability needs, which directly affects adoption and compliance (AlHogail & Mirza, 2014; Almuhimedi et al., 2015). Addressing such a multifaceted problem required an approach that could capture both the technical and socio-organizational dimensions of MDM/MAM implementation.

To achieve this problem understanding, data collection was conducted through informal discussions with security experts at SURF and unstructured interviews with Chief Information Security Officers (CISOs) from six institutions. The use of purposive sampling ensured the inclusion of participants with deep domain expertise, consistent with the DSR emphasis on contextual relevance (Hevner, 2007). Unstructured interviews were particularly appropriate at this stage due to the exploratory nature of the inquiry. Since the researcher knew little about a phenomenon, he opted for open-ended questions, which normally facilitate the identification of issues, perceptions, needs, and concerns that might otherwise remain hidden (Myers & Newman, 2007).

Beyond the purpose of understanding the problem, these early engagements also served a strategic function: building trust and fostering ongoing stakeholder involvement. As DSR literature emphasizes, early and sustained collaboration with stakeholders enhances problem relevance, supports richer problem framing, and increases the likelihood of eventual artifact adoption (Prat et al., 2015; Sein et al., 2011). By embedding the research process within the realities of Dutch HEIs, this stage laid a rigorous and practice-oriented foundation for defining solution objectives and guiding the subsequent design of a user-centered MDM/MAM policy framework.

#2 Objectives of a Solution

The second step of the Design Science Research (DSR) process, defining the objectives of a solution, is rooted in Simon's (1996) *sciences of the artificial*, which emphasize the need to establish the long-term goals as the basis for artifact design. Within DSR, this stage does not merely serve the purpose of listing requirements:

instead, it represents a critical translation of stakeholder needs, environmental constraints, and theoretical insights into actionable design objectives. In this thesis, grounding these objectives in both theory and industry insights, the researcher ensured that the resulting artifact not only addresses an immediate problem but also covers long-term security goals.

During this research, the objectives emerged from the problem identification phase and were shaped by insights from security departments within Dutch HEIs and from SURF. The core aim was to develop recommendations for MDM-MAM policies that explicitly incorporate user perspectives. This orientation reflects the DSR principle of *utility-driven design*, where the effectiveness of a solution is measured not solely by its technical adequacy but also by its ability to foster stakeholder acceptance and sustained use (Prat et al., 2015). This research's emphasis on user-centered objectives acknowledges illustrates the socio-technical nature of the design problem, where technical configurations and human factors are deeply intertwined (Baskerville et al., 2018).

By defining objectives in such a structured way, the research provided high-quality operationalization of DSR's commitment of producing artifacts that are both useful in practice and grounded in research. The defined objectives served as a blueprint for the subsequent design and development phase, ensuring that the resulting policy framework was grounded in empirical evidence, aligned with stakeholder priorities, and capable of advancing knowledge on user-centered security policy in higher education contexts.

#3 Design and Development

The design and development stage represents the core of Design Science Research (DSR) and is grounded in the principle of constructive research, which emphasizes the iterative creation and refinement of artifacts as a means of generating knowledge (Gregor & Hevner, 2013). In DSR, artifacts, be they models, methods, or policy frameworks, serve as vehicles for both solving real-world problems and advancing theoretical understanding of the topic (March & Smith, 1995; Peffers et al., 2007). This dual mission stressed the importance of integrating academic rigor with industry relevance.

Hence, the design process in this research was constituted by two complementary methodological approaches. First, the rigor cycle connected the study to the existing knowledge base through an extensive desk review. This review synthesized prior research on MDM, MAM, and Bring Your Own Device (BYOD) adoption, as well as studies on user acceptance in information security. Incorporating established theoretical constructs ensured that the design was anchored in recognized drivers of technology adoption (Davis, 1989; Bélanger & Crossler, 2011). Second, the relevance cycle engaged directly with the industry thanks to the semi-structured interviews with employees from multiple HEIs. These interviews captured nuanced perspectives on user concerns, acceptance barriers, and contextual factors that purely technical analyses often overlook.

The sampling used for the interviews is convenience sampling, a pragmatic choice given the constraints of a master's thesis. However, attention was paid to have enough diversity within the sample to mitigate potential biases and enhance generalizability. Participants were drawn from at least three institutions and represented both academic and administrative roles, providing a spectrum of

viewpoints relevant to policy implementation. This inclusion of multiple perspectives aligns with DSR's emphasis on contextual validity: by considering heterogeneous user needs, the resulting artifact is more likely to be applicable across different organizational settings (Baskerville et al., 2018).

A notable feature of this stage was the integration of vignette-based inquiry within the interviews. Vignette studies, which present participants with brief, hypothetical scenarios to elicit context-specific judgments (Atzmüller & Steiner, 2010; Martin et al., 2024), were used to probe employee reactions to potential MDM/MAM policies. This method allowed participants to engage with realistic, possible depictions of policy use. The theoretical and methodological value of vignette studies, as well as practical examples in this research, will be presented in detail in the next section.

Digression: Vignette Studies

Within Step 3 (Design and Development), this research incorporated vignette studies as a methodological tool to enhance the depth and validity of the data collected, particularly during semi-structured interviews with HEI employees and, to a lesser extent, during unstructured interviews with (Chief) Information Security Officers. Vignettes are short, carefully constructed descriptions of a hypothetical scenario, or event designed to elicit participant reactions, judgments, and decision-making processes. As explained by Atzmüller and Steiner (2010), vignettes present respondents with contextually relevant yet fictionalized situations that allow them to engage with sensitive or complex topics in a non-threatening, depersonalized manner. This characteristic makes them particularly valuable for exploring perceptions and behaviors in areas where direct questioning might lead to defensiveness or socially desirable responses.

In practice, this was applied to all user interviews uniformly: based on what learnt from the literature and in previous steps of the research, the researcher included potential scenarios in the user interviews. Specifically, this meant considering the controls that the security officers had mentioned (e.g. document labeling), and place them in a scenario where the implementation of such MDM and MAM controls occurred at the user's institution. The user was then confronted with the situation where they had to comply with these controls. They were then asked to describe their perspective, feelings, and opinions.

To ensure academic rigor, the scenarios were built using both the desk research and insights gained during the earlier problem identification stage, ensuring contextual accuracy and relevance to Dutch HEIs. The design of these vignettes was guided by Skilling and Stylianides' (2019) framework, which outlines three interdependent elements of vignette construction: conception, design, and administration. Conception involved identifying the critical dimensions of MDM/MAM implementation that could influence acceptance. Design focused on embedding these dimensions into coherent and plausible narratives that were both accessible to participants and reflective of institutional realities. Administration referred to the way these vignettes were integrated into the interview questions, allowing space for participants to respond spontaneously while enabling the interviewer to probe specific aspects of their reasoning.

The use of vignettes in this study served two main purposes. First, providing a clear scenario allowed the user to immerse into the situation and ponder which reactions or emotions such situation may cause. Second, by using similar scenarios for all the participants, it provided a structured yet flexible means to use across interviews. In fact, institutions differ in structure and security maturity, and using vignettes,

allowed the researcher to build a similar structure beforehand, while still being able to swiftly adjust the scenario during the interviews.

The use of vignette studies in interviews is nothing new: this approach is well established in academia. For instance, Martin et al. (2024) demonstrated how vignettes can improve the validity of qualitative interviews within realist evaluation. They argue that vignettes help setting boundaries and elicit the imagination of the person being interviewed by allowing them to live the situation in their mind. This, in turn, delivers richer and more grounded participant responses. In the context of this study, vignettes encouraged participants to articulate not only what they might do or feel in a given MDM/MAM scenario, but also the reasoning for such reaction or emotion, thereby revealing core aspects of the user's motives. Furthermore, following Martin et al.'s (2024) recommendations, the vignettes were crafted to be sufficiently specific to prompt effective engagement, while remaining open enough to allow for the emergence of unanticipated responses. This approach supported the study's broader goal of identifying acceptance drivers and barriers that could inform both policy design and communication strategies.

Hence, by using interviews and vignette studies, this stage built the artifact of this thesis: a set of preliminary policy recommendations, which were then demonstrated to a larger pool of security professionals and users, in order to evaluate and amend the recommendations.

#4 and #5 Demonstration and Evaluation

The subsequent stages—*Demonstration* and *Evaluation*—are treated as distinct steps in Peffers et al. (2007). Instead, in this thesis the two stages were streamlined, following Horváth's (2007) suggestion that the DSR process can, in practice, be condensed into three phases: aggregation, reflection, and confirmation. Within this adaptation, aggregation corresponds to the combined processes of problem identification and defining solution objectives; reflection aligns with the design and development stage; and confirmation encompasses both demonstration and evaluation. In the present study, demonstration took place through the presentation of proposed policy designs at the SURF Security and Privacy Conference. This presentation was followed by facilitated polls and open discussions with both end-users and security experts from Dutch HEIs. The evaluation phase consisted of analyzing the responses collected during these interactions to assess the perceived feasibility and potential effectiveness of the proposed policies within the wider HEI sector.

Validation was undertaken in three phases. The first phase involved internal cross-validation of the interview data. The second phase involved an informal focus group conducted during the SURF conference, in which participants were presented the recommendations and asked to provide direct feedback on the proposed policy designs following a brief presentation. Lastly, validation would involve the users, in order to verify if the opinions of a few are shared by a larger pool of users. This process strengthened the robustness of the findings, although it is acknowledged that definitive evaluation will require a longitudinal assessment conducted by HEI security departments after the completion of this thesis.

#6 Communication

Finally, communication in DSR is not merely a knowledge-sharing activity but a theoretical imperative to ensure *knowledge contribution* (Gregor & Hevner, 2013). Artifacts and findings should be shared with both practitioner and academic audiences, to increase usability of the artifact and continuous improvements and validation, as well as the possibility for other researchers to apply the concepts and findings in other contexts.

In this research, communication was achieved through multiple channels: a detailed report for SURF and participating HEIs, a blog post on the SURF portal to engage the wider security community, and this thesis, which serves as a comprehensive scholarly output.

However, further, long-term communication and engagement with practitioners is left to SURF, as this is outside the scope of this master's thesis.

Chapter 5: Insights from the research process

In the previous chapter, this thesis described how each step of the Design Science Research (DSR) methodology can be operationalized in practical actions. This chapter expands on that by detailing the sequence of research activities undertaken. This chapter is divided in preliminary discussions with SURF experts; unstructured interviews with (Chief) Information Security Officers; semi-structured interviews with HEI employees; systematic coding and thematic synthesis; the iterative design of a user-centered security policy recommendations; and the demonstration and evaluation stages used to validate the proposed designs. For each component, the rationale for methodological choices, data collection procedures, analytic steps and measures taken to preserve rigor and ethical integrity are explained.

5.1 Preliminary desk research

As mentioned in the introduction, this thesis' topic stems from previous research's findings (Gadellaa, 2022). His thesis concluded emphasizing the importance of the usability aspect in IT environments as a factor contributing to an institution's security resilience. This, combined with the necessity to prevent shadow-IT, led to a internship, aimed at doing the research for this thesis.

Before starting the internship, a large amount of desk research was done, in order to establish the most suitable framework and high-level approach. These have been presented in the previous chapters, with the Technology Acceptance Model as theoretical framework, and Design Science as methodology. The preliminary desk

research was also conducted to understand the status quo of the academic knowledge available on the topic. This has been presented in Chapter 2.

The main finding from this step is:

Sub-finding #1: Previous research conducted within SURF had identified the presence of shadow IT usage across Dutch HEIs.

This helps identify the high-level problem and highlights the need to delve deeper into this topic.

Primary source: Gadellaa, 2022.

5.2 Preliminary talks: SURF experts

The research internship began with exploratory conversations in February 2025 with members of SURF's Security Awareness & Organization and Technical Security teams. These informal discussions—each lasting approximately thirty minutes—served three interrelated purposes. First, they situated the phenomenon of shadow IT within the Dutch HEI landscape and clarified SURF's prior work and strategic concerns. Second, they identified high-level objectives for the project: namely, to propose MDM/MAM policy solutions that reconcile institutional security requirements with end-user perceptions and needs. Third, these talks helped define the study's scope by recommending a focus on research universities (WO) and large universities of applied sciences (HBO), and by advising the exclusion of vocational education institutions (MBO) given differences in scale, governance and data sensitivity. Notes from these conversations were collated promptly and used to shape subsequent interview guides and vignette scenarios. Methodologically, this stage

fulfilled DSR Steps 1 and 2 (problem identification and specification of solution objectives), providing the practical problem frame and initial constraint set that informed artefact design.

5.2.1 Sub-findings

From these preliminary talks, the following findings have been identified:

Sub-finding #2: SURF is working with its members towards MDM policies. While there currently is a working group on this topic, some institutions have already taken some MDM/MAM measure. This may lead to a great difference in MDM/MAM practices across institutions. The working group is trying to establish a uniformed approach.

This relates to both problem identification and objectives of a solution.

Primary source: Conversations with members of the team Security Awareness and Organization and with some of SURF's liaisons for universities and HBOs.

Sub-finding #3: SURF experts see a security risk in shadow IT and agree that good, user-friendly MDM policies might reduce the employees' temptation of turning to shadow IT.

This relates to the objectives of a solution.

Primary source: Conversations with members of the team Security Awareness and Organization

5.3 CISO-talks: Status Quo and Security Requirements

Between February and early March 2025 a series of seven unstructured interviews was conducted with security departments from Dutch HEIs—four research universities and three universities of applied sciences. Interviews lasted approximately forty-five minutes and were carried out either on campus or remotely. SURF facilitated access to participants, which produced a purposive sample of informants who possessed authoritative knowledge of institutional security strategy and operational constraints. Unstructured interviews were selected deliberately: at this stage the aim was not to test hypotheses but to elicit rich, tacit knowledge about institutional priorities, legal and organisational constraints, and the practical barriers security teams faced when attempting to implement EMM solutions in federated academic settings. The unstructured format permitted interviewees to narrate problem histories, surface political and cultural sensitivities, and propose candidate controls in their own terms—data that a more tightly structured instrument would have failed to capture.

All CISO interviews were documented through notes, which were subsequently formalized within forty-eight hours of each meeting. The decision not to audio-record these sessions reflected participant preferences in several cases and was taken to encourage candor; however, it introduced analytic limitations that were mitigated by rapid note formalization, careful cross-checking of themes across interviews, and continual researcher reflexivity. No prior personal relationships existed between the researcher and the interviewed officers. To reduce confirmation bias, invitations made explicit the study's aims but did not pre-announce detailed methodological assumptions; interview prompts were deliberately open-ended and follow-up probes were used only to clarify or extend participants' own emphases.

The substantive outcomes of these interviews were threefold. They identified the core technical and governance constraints that shape MDM/MAM policy choices in HEIs (for example, the need to accommodate faculty autonomy, research mobility and diverse software requirements); they articulated security departments' principal objectives (limiting shadow IT, protecting research data, and achieving compliance with data-protection standards); and they offered high-level input on design preferences (for instance, desire for role-based controls and delegated administration). The interview set reached a practical point of theoretical saturation: by the sixth and seventh interviews, the substantive issues being raised were recurring and no fundamentally new categories of concern appeared. This evidence of saturation supported the transition to the design phase of DSR.

5.3.1 Sub-findings

Sub-finding #4: in HEIs, academic freedom is paramount. This impacts how security practices are developed and implemented: it was often mentioned as the key obstacle to change: enforcing policies in academia works differently than in a corporate environment.

These words align with and confirm what was found in the literature.

Primary source: unstructured interviews with security officers of HEIs #1, #2, #3, #5, #6, #7

Sub-finding #5: different institutions have different maturity level and different approaches. One institution strongly restricts local-admin rights and enforces security controls with a top-down approach, using MDM for CODs, and MAM for the BYOD devices for which the institution provides a reimburse. A second

institution adopts a similar hard approach. One HEI take different approach and have few security controls: despite the hopes and work of the security departments, this "soft" approach has not delivered many results. And lastly, 4 of the 7 have tried mixed approaches: working at faculty level (2/4), offering local-admin rights (3/4), requiring software requests for most applications (2/4), and MAM in place on BYOD (2/4). Table 5 summarized the findings of the unstructured interviews with the security department, focusing on the topics that were discussed in all seven interviews.

HEI Control	#1	#2	#3	#4	#5	#6	#7
Hard approach: strongly limit users in what they can and cannot do with the device	Yes	No, mixed	Yes	No, mixed	No, mixed	No, mixed	No, soft approach

Local Admin: possibility for the users to install applications on their COD without any action from the IT department (no is in principle more secure)	No, by request only and local admin is not easily granted	Yes	No, separate account for those working with software	Yes, with limitations and software by request	Yes, but software by request, only one tool allowed among those with the same functionality	No, but clear tool picker (application and software whitelist, with clear instructions and explanations of what is allowed and what not)	Yes
MAM: controls that limit users' actions on the application used for work purposes	Yes, with enrollment, including BYOD	Pilot phase	Yes, also for BYOD that are reimbursed by the institution	Very basic	No	Yes, for BYOD	No

(either COD or BYOD)							
MDM: controls that limit users' actions on the device (either COD or BYOD)	Basic, faculty-managed	Strong	Strong	Basic	Basic	Basic	Very basic

[Table 5 – Overview of common topics emerged in the unstructured interviews with Security Dept]

Sub-finding #6: when asked about the security requirements security departments had in mind, their answers remained vague and high level, such as "increasing security", "preventing data leaks", "securing data of the institution", "be GDPR compliant". These are overall security goals. When direct questions were asked, most security officers explained how they have controls they would like to implement, but they are aware that it would not be feasible due to these controls being too restrictive, hence they use high-level goals to guide their work in EMM. However, some security controls did emerge in three conversations: document labelling (Finding 6.1), local admin based on the role (Findings 6.2), complex passwords (Finding 6.3), email forwarding (Finding 6.4) and improving communication with the users (Finding 6.5).

These topics, combined with topics from the background literature, prompted the questions for the semi-structured interviews with the end-users.

5.4 Users' interviews: user perception and acceptability

These semi-structured interviews (see Appendix 2 for the list), were conducted by the researcher between April and May 2025. The researcher is a male student, he holds a BSc and performed the interviews in the context of his MSc thesis. His previous experience in research consists of 15 ECTS in research methods during his bachelor, his BSc thesis, and 3 ECTS in research methods during his master's program.

These interviews were a one-off (no repetition) and involved eight employees of HEIs. They were conducted individually in a quiet room at their workplace or online via MS Teams, with no one else being present in the rooms during the interviews. Eleven participants were invited, and eight agreed to participate, with three mentioning lack of time to participate. No one dropped out during the study. The choice to hold *semi-structured* interviews lies in the exploratory nature of this phase: the interview was not 'locked', and it was shaped based on the interviewee's specific experience, context, and role. However, to ensure the interview remained on-point, twelve questions, and a number of sub-questions were developed prior to the interviews, also allowing for cross-validation.

The questions of the interviews can be found in Appendix 3. These were used as a baseline for all users' interviews. These questions were written based on the findings from the unstructured interviews with the security officers (Finding 6) and on the background literature, as mentioned in the literature review section.

The sampling approach chosen for these interviews was convenience sampling. While ideally random sampling would have been used, there are good reasons for this choice: firstly, time and contextual constraints limited the reach of busy individuals; secondly, many HEIs had not rolled out MDM/MAM programs to the whole institution yet, but (if anything) only to a limited number of employees: convenience sampling allowed the researcher to make use of SURF's contacts within the institutions for employees willing to be interviewed; lastly, convenience sampling still allows a solid width in the roles, jobs, and experiences of the sample: in fact, the interviews were spread out across multiple institutions and involved different types of employees (from employees involved in teaching to researchers, to support staff). This limits the bias that can occur with convenience sampling, namely that the individuals interviewed belong to the same group and therefore do not provide a broadly enough sample. After a few interviews, an attempt was made to reach further participants via snowball sampling: one succeeded. Three of the participants knew the researcher beforehand, while the others did not. These three had been professors or teaching assistants during the researcher's academic career. All participants received a detailed explanation of the research purposes, basic assumptions, and methodological approach per email, during the invitation. Some users were firstly contacted via LinkedIn and then received the formal invitation via email. In this formal invitation, they were informed about the study, the reasons for the research, and what would have happened with the information gathered through the interviews. They were also informed of who the researcher/interviewer was and what made him carry out these interviews.

Since all participants provided their consent for the interview to be recorded (Appendix 4), these interviews have been recorded, transcribed, and coded. Besides the transcripts of the recordings, no field notes were made during or after the

interviews. The reason for this is bifold: recording and transcribing interviews allows for high academic rigor in the research process, and it allows deeper insights and understanding of the interviewee's words and experience. While Rutakumwa et al. (2019), Muraglia et al. (2020), and Höpfner and Promberger (2023) explain that recording interviews does tend to have an influence on the answers interviewees provide, the context of this interviews is not deemed sensitive enough that employees might significantly alter their responses due to the recording. All participants were offered the possibility to review the transcript of the conversation, and one participant made use of this option, without reporting any correction.

The goal of the interviews is understand the users' opinion on current security controls and possible new controls and draw a mental model. If several users express discomfort or hinderance in regard to a security control, the policy design should consider alternatives that achieve similar security goals. The interviews also aimed at a better understanding of different needs across different type of employees and faculties.

This part of the research maps to step #3 of DSR In fact, by providing insights into the views of users, this step laid the first layer leading to the design of a new, user-centered policy: the findings stemming from these interviews will directly support the design of the new policy.

As mentioned in Chapter 4, this research employed vignette studies to build the internship questions. Many of these questions were scenario-based, *what-if* questions: the users were asked their opinion in a possible scenario involving implementation of MDM/MAM limitations. For example, what if the workplace of the user adopted the policy of blocking automatic forwarding of emails, or what if the workplace offered a portal with the tools approved for use, or what if a

warning/confirmation message was displayed if the user tried to forward an email to an external party. The design of these vignettes was guided by Skilling and Stylianides' (2019) framework, which outlines three interdependent elements of vignette construction: conception, design, and administration. Conception consisted of identifying the dimensions of MDM/MAM implementation, such as technical restrictions, that could influence acceptance. Vignette design focused on embedding these dimensions into coherent and plausible narratives that were both relevant to the participants and reflective of institutional realities. Administration referred to the way these vignettes were integrated into the interview process, allowing space for participants to respond spontaneously while enabling the interviewer to probe specific aspects of their reasoning.

5.4.1 Coding process

After each interview, its recording was transcribed. To ensure data protection, the recording occurred through the 'voice memo' application on the researcher's iPhone, while the transcription was done via the 'dictate' function within the Microsoft suite of SURF. The transcript was the checked for transcription errors and corrected when needed.

After holding all the interviews, the researcher coded them by himself using Atlas.ti, the approved tool of Radboud University. To perform the coding, the interviews were analyzed using thematic analysis, which consisted of identifying common themes, topic, ideas, and meaning patterns, that were (repeatedly) mentioned in the user interviews. The themes were derived from the data and not established in advance. In seven out of eight interviews, fourteen to twenty-four relevant pieces of information were found. In one transcript, seven passages with useful information

were identified. In total, sixty-six codes were identified in the first round of coding, with more than one hundred coded sections. The detailed Atlas.ti Code Manager can be found in Appendix 5. After three rounds of coding the documents, a round of grouping was performed, leading to fifteen groups, displayed in Table 6.

The grouping presented in Table 6 is based on the topic and answer to the question 'which were the topics discussed?' and affinity diagram was used during the grouping process. Affinity diagrams are a commonly used in qualitative research, particularly with interviews, as this method consists of grouping together similar findings or concepts to identify themes or trends in the data (Courage & Baxter, 2005; Lisle at al., 2019).

These choices led to the employment of bucket-themes, which deliberately group together different opinions related to the same overarching topic: for instance, it groups codes about acceptance and codes about non-acceptance of a particular security control. In this context, the use of bucket-themes is intentional: it serves a specific analytical purpose. In fact, it helps understanding *to what extent* a security control is accepted, and where the participants draw the line. For instance, when discussing their opinion on the control, participants provide reasons and more details than a simple "yes" or "no", thereby helping understand exactly what is accepted and the context under which is accepted. To provide an example: to the question about having an extra password to access the device, a respondent might say that it makes sense because the extra time spent inserting four extra numbers does significantly increase security. At the same time another participant might have a longer and more complex password in mind, which results in him expressing concerns about the 'extra password'.

As a second reason behind this choice of grouping lies a structural issue: before assessing participants' views on specific controls, it was essential to first identify which topics were mentioned and discussed. So, this thematic grouping serves as a pragmatic step to capture the areas that were most frequently addressed. Topics that were rarely mentioned are less useful for research focused primarily on users' perspectives.

Once these commonly discussed themes were established, it became possible to analyze individual controls more meaningfully by examining whether participants expressed supportive, critical, or mixed views. This analytical stage leads to key insights. For example, a control that received mostly positive feedback may indicate broad acceptance and support for inclusion in future policy. Conversely, a control that was largely criticized may warrant reconsideration or removal. Equally noteworthy are controls where participant opinions were split. Such divergence raises important questions: does the variation relate to the role or context of the participant? Does it point to underlying uncertainties or conflicting priorities? These cases may benefit from further investigation, possibly through quantitative methods, to assess the views of a broader and more representative population.

Furthermore, transitioning from these merged thematic groups to individual evaluative findings (i.e., whether feedback was positive, negative, or neutral) is straightforward: participants' stances are clearly discernible through their quotes, making the interpretation of opinion clear.

Lastly, fifteen groups is a fairly large number, which would have been even higher if the positive and negative opinions were kept separate. To reduce this number even further, and obtain higher-level groups, a second level of grouping was deemed necessary, by merging groups that covered similar topics. After three iterations the

number of groups was reduced to seven, then to six, and then to three, with two previous groups left self-standing. This final version is presented in Table 7. While the importance of identifying high-level themes is clear, this research still wants to highlight the value of the first level of grouping (Table 6) for analytical purposes: due to the choice of using bucket-themes, maintaining a level of concreteness allows more detailed analysis that catches the nuances of each opinion.

Group #1 – Communication errors	Group #9 – Opinions MDM: access control
Group #2 – Communication importance and methods	Group #10 – Opinions on whitelists for software and applications
Group #3 – Opinions on security notifications	Group #11 – Privacy
Group #4 – Opinions MAM: email forwarding	Group #12 – Prompt change with notification: offer alternatives
Group #5 – Opinions MAM: separation between private and work on a device	Group #13 – Proof: users may turn to shadow-IT (if they really need something, if security is too strict, and if communication is not effective)
Group #6 – Opinions MAM: sharing documents	Group #14 – Request process

Group #7 – Opinions MAM: access control	Group #15 – Risk Acceptance and consequences
Group #8 – Opinions MAM: information labeling	

[Table 6 – Atlas.ti, first round of grouping codes]

Group A (Groups 1 and 2) – User perception of communication around security policies and practices.	Group C (Groups 4, 5, 6, 7, 8, and 9) – Users' attitudes toward information protection
Group B (Groups 3, 10, 12, 13, and 14) –Opinions about steering users away from shadow IT and guiding them towards approved solutions through user-friendly processes.	
Group #11 – Users' concerns about users' privacy	Group #15 – Users' opinions about risk acceptance and consequences

[Table 7 – Atlas.ti, second round of grouping codes]

5.4.2 Sub-findings

These sub-findings contain directed quotes from the transcripts. These quotes are now traceable back to a specific interviewed user. These sub-findings were not shown to the participants for feedback.

Some sub-findings are sustained by direct quotes from the interviews. Some of these quotes have been translated from Dutch: the originals can be found in Appendix 10.

Group A - User perception of communication around security policies and practices

This theme captures all the concepts around the lack of proper communication, and the possible solutions to improve it. These concepts fall, on the one end, under codes such as “lack of information” and “lack of understanding”, and, on the other hand, under “communication + a method”.

Sub-finding #7 (from group 1): some users do not understand why certain security measures are needed. Because there are lacking such information their resistance level against EMM is higher. The lack of understanding seems to be related to the little communication received.

Example quotes:

“I don’t know well why that is secured in that way: that you can only open links in Edge and that you cannot copy and paste them outside of the Outlook application. I don’t know why it is secured like this. And thus I would like to be able to do it”

“So if I could understand the reason, I be more at peace with it”

Sub-finding #8 (from group 2): communication is very often (6/7 interviews) mentioned as important for the user, and it was often (5/6) mentioned that the user would gladly receive more information. Also, it was often (4/6) said that, if proper communication is carried out, this would improve their understanding of the usefulness of security measures.

Example quotes:

"that is a good moment [when people receive their device] to set a first step in that [communication]"

"Yes, I would like to receive a really short, concrete, clear checklist"

"it's also about making people aware of this"

Sub-finding #9 (from group 2): communication approaches that are positively received by the participants and might work are:

9.1 – via email (3 interviews /6)
9.2 – on Sharepoint (2/6)
9.3 – when the laptop is given (4/6)
9.4 – via newsletters or similar campaigns (2/6)

Group B – Opinions about steering users away from shadow IT and guiding them towards approved solutions through user-friendly processes

This theme captures all the opinions about what could work in practice to reduce the use of shadow IT. Group B focuses on the processes, rather than the controls: having a whitelist, giving warning signals when users are doing something potentially unsecure. Codes about notifications fall under this group.

Sub-finding #10 (from group 3): when the user performs an action that is not allowed or desired, a notification briefly explaining why the action is not secure and offering secure alternatives would be accepted

Example quotes:

“Pop-ups or something similar, a notification would possibly help a bit at that point”

“I use random websites which I am allowed to use like at least when I open it, I don't get any pop up. But if I did get a pop up and they say oh, here's it, I don't mind as long as you know. It can redirect me to something.”

Sub-finding #20 (from group 10): all users reacted positively to the scenario where the most common tools were, if approved, placed on a whitelist.

Example quote: “On the website a whitelist of the applications that can get installed or requested”

Sub-finding #22 (from group 12): Most users (6/8) expressed positive reaction to a notification system, where users get an alert that what they are doing does not conform to the policy. For instance, if a confidential document is being sent out of

the institution's environment, alerting the user and asking whether they really want to proceed would help users' awareness and understanding.

Example quote: "at least you get a message saying, hey, watch out. This is a confidential document you're exporting"

Sub-finding #23 (from group 13): the interviews confirm that users will turn to shadow-IT, such as their own devices, if they need something, and the security constraints are too strict, and proper communication has not been carried out.

Example quotes:

"…then I would quickly take my personal laptop and do it, you know, to be able to go on with the work"

"I would like say email a different e-mail address of mine"

Sub-finding #24 (from group 14): most interviewees find the current software/application request long and sometimes hampering their job. When possible, some users agree that they could consider the tools needed in advance (for instance, at the beginning of a project or of the semester) and submit the requests well in advance, but this is not always possible.

Example quote: "Yes and it would be ok for example if you needed to think about that when starting a project"

Group C – Users' attitudes toward information protection

This theme captures all the concepts around the actual controls that can be implemented. These concepts fall under all the codes about a specific control (notifications, email forwarding, extra password, sharing documents, etc.). For instance the code: "extra security for confidential documents".

Sub-finding #11 (from groups 4 through 9): users prefer MAM over MDM, especially on BYOD.

Sub-finding #12 (from group 4)**:** as long as forwarding is not blocked altogether, but just automatic forwarding, some users are fine with this block. Other users feel strongly against this policy. But if exceptions can be set when the email comes from specific people (unless label is confidential), more would be open to this solution.

Sub-finding #13 (from group 5): there is consensus of the need to keep private and work environments separate, specifically users agree that confidential documents should not be transferable from work to personal environment, if the device is company-owned.

Example quote: "Yes, I currently have a white and a blue cloud. The blue is the OneDrive of the university, the white one is my personal OneDrive".

Sub-finding #14 (from group 5): implementation of separate IT environment or a different IT network for those users that need an unmanaged laptop for research and work purposes, for instance computing scientists.

Sub-finding #15 (from group 7): extra password for environments with sensitive information would be seen as reasonable.

Sub-finding #16 (from group 6): Policy of blocking the possibility to attach confidential files, allowing only the possibility to share it via a OneDrive link, might work. It will not work if all attachments are blocked.

Sub-finding #17 (from group 7): extra password on the user account would be accepted: if users have to access their email or documents (OneDrive) on their phone, an extra password is not considered a issue.

Sub-finding #18 (from group 8): information, document, and mail labeling is described by most (6/8) interviewees as a good solution, both from an awareness point of view and from a restriction angle. This consists of assigning a level of confidentiality to the document or email created, ranging from Public to Restricted. Specific controls can then be applied to the document based on the labeling.

Example quotes:

“actually do label most of my work. I'm a big labeler”

Sub-finding #19 (from group 9): secure access to the device is seen as important, but, for mobile phones (especially if BYOD), freedom should be left to the user.

Example quotes:

"Yes, I would accept it [extra code for work-apps], I would find it a bit intrusive, but I would accept it".

"That happens often, also with banks application I have to continuously do it [insert a code]"

Other

Sub-finding #21 (from group 11): users' privacy is not seen as a major concern when it comes to MDM/MAM. Some users mention they do not feel privacy plays a role in their acceptance of MDM/MAM, or, at least, users are willing to trade it off for higher usability.

Sub-finding #25 (from group 15): if proper explanation is provided, some users find it acceptable to sign that they understand and accept the risks of their actions.

Sub-finding #26 (from several groups): the role of the user is determinant. Someone from the science faculty has certain needs, those doing research in IT have certain needs, and those accessing personal data frequently (HR, study advisors, etc.) may need stricter rules

5.5 Human-centered Security Policy: a proposal

This part of the research consists of the actual design and development of the "artifact" of DSR: a policy proposal based on the findings gathered in the previous phases, and that accounts for the user's perspective.

The policy is built as follows: the sub-findings described earlier in this chapter are divided into priority-groups, of which the high-priority ones are translated into actionable practices. This was done by using logical follow-ups rooted in the findings.

5.5.1 Design Process: policy concepts selection

The most-suitable findings for the policy are selected through a precise decision-making structure follows: the MoScoW prioritization framework: in this context, '**must-haves**' (in light-blue) are those findings that have been mentioned at least four times in the interviews and strongly align with the security requirements expressed by the security officers. '**Should-haves**' (in green) also need to be included, but they are mentioned less often in the interviews. '**Could-haves**' (in yellow) have been mentioned at least twice in the interviews but do not align well with the security requirements; and '**Won't-haves**' (in red) are less helpful, as they have been mentioned one or two times in the interviews and do not align or align poorly with the security requirements.

Finding	**Part of the policy?**	**Explanation**
Sub-finding #1: Presence of Shadow IT	Must-have	The presence of Shadow IT in HEI is the driving factor behind this policy design. It has been mentioned several times by both the security officers and the users. It is included in the policy as a background explanation of why the policy should be implemented
Sub-finding #2: a working group already exists on this topic	Won't-have	Existing work done by the institutions, if any, has been only partially considered in the discussions and was not given a central role in this research
Sub-finding #3: MDM policies needs to be user-friendly	Must-have	The user-friendly-centered approach is key for this thesis's approach, and SURF agrees it is a crucial element. This forms the high-level approach behind the policy.
Sub-finding #4: importance of academic freedom	Must-have	Academic freedom is a key constraint of doing security in academic institution: it must be addressed in the policy design. Both security officers and users mentioned this issue.

Sub-finding #5: diverse maturity levels	Could-have	The fact that different institutions have different maturity levels is a situational constraint that could be accounted for, but is not fundamental for the policy design.
Sub-finding #6: security objectives	Must-have	The security controls and topics to which several security officers draw the attention are: document labelling (Finding 6.1), local admin based on the role (Findings 6.2), complex passwords (Finding 6.3), email forwarding (Finding 6.4) and improving communication with the users (Finding 6.5). These must be part of the policy, with their extent and strictness being based on the interviews and requiring validation.
Sub-finding #7: lack of understanding of the reasons behind security policies	Should-have	Several interviewees mentioned frustration in not understanding why something hampering their job was implemented. Improvements in communication must be included in the policy design.

Sub-finding #8: importance of communication	Must-have	That communication is important forms the high-level approach behind the policy.
Sub-finding #9: communication methods	Must-have	Regarding communication methods, providing information when the laptop is handed to the user is often mentioned as an effective action from user's perspective.
Sub-finding #10 & **Sub-finding #22: Notifications**	Must-have	Notifications are an important security control, and it has been mentioned in several interviews, especially in the moment they are doing something that should not be done.
Sub-finding #11: preference of MAM over MDM	Won't-have	Too broad, may be useful as a general principle: prefer MAM over MDM, but it depends on the context.
Sub-finding #12: email forwarding	Should-have	Limiting automatic forwarding of emails is an important MAM control, mentioned by users and security officers. Some users have provided interesting insights on how to make this less hindering.

Sub-finding #13: separation of personal and work environments	Could-have	There is consensus of the need to keep private and work environments separate, specifically users agree that confidential documents should not be transferable from work to personal environment. However, it is a complex control to implement. Hence, this could be incorporated in future, larger research.
Sub-finding #14: separation of networks	Could-have	Separation of networks for those that do not have a managed laptop is a technical solution that would require conversations with the IT department. It could be mentioned as high-level control.
Sub-finding #15 **Sub-finding #17** **Sub-finding #19** **Extra passwords**	Must-have	Having an extra password for specific sections of the network, accounts, or devices could be an important aspect of this policy
Sub-finding #16: limiting attachment of confidential files	Could-have	Blocking the possibility to attach confidential files, allowing only the possibility to share it via a OneDrive link, could be an effective and balanced

		solutions, as expressed by both security and users.
Sub-finding #18: document labeling	Must-have	Labeling of emails and documents is a very important MAM solution. Some validation has already occurred, given the high agreement across the interviewees.
Sub-finding #20: whitelisting	Must-have	White-lists are important and easily implementable
Sub-finding #21: privacy	Won't have	Although there is quite some consensus that users' privacy is not a major concern, it may be risky to include this concept in the policy design
Sub-finding #23: reliance on Shadow IT	Must-have	The fact that users might turn to shadow IT is clear and must be accounted for when designing the policy. This is part of the foreword of the policy, explaining why such policy is needed.
Sub-finding #24: choose tools in advance	Could-have	Mixed feelings from the users and hard to implement: not everyone can think in advance of all the tools they may need for their research

Sub-finding #25: risk acceptance	Should-have	Risk acceptance, preceded by with adequate communication, is important to responsible and raise awareness across the users.
Sub-finding #26: role-based controls	Must-have	Role matters: someone from the science faculty has certain needs, those doing research in IT have certain needs, and those accessing personal data frequently (HR, study advisors, etc.) may need stricter rules

At this stage, it is established which topics are included in the policy design: of the twenty-six sub-findings, eighteen must or should be used as ground for actionable solutions.

5.5.2 Development Process: from findings to actionable solutions

Sub-findings #1, #3, and #23 are the basis for the policy proposal's introduction and rationale. This makes the case for a list of proposed security controls grounded in a combination of empirical insights and practical considerations derived from the sub-findings of this study. In fact, sub-finding #1 highlights the presence of shadow IT within Dutch higher education institutions (HEIs), confirming what the theory and previous research had put forward. As previously established, this finding confirms that Shadow IT emerges when users resort to personal or unapproved tools

to complete their work, often because institutional solutions are perceived as restrictive, cumbersome, or inadequate. This phenomenon alone underscores the need for a structured policy that addresses both security risks and user requirements.

Furthermore, sub-finding #23 further reinforces this need by demonstrating that users feel they have no alternative than relying on shadow IT to perform their job effectively when institutional tools or security measures prevent them from completing essential tasks. Users' adoption of shadow IT is not necessarily malicious; rather, it reflects a tension between their work needs and security constraints. Recognizing this behavior as a driving force behind policy development ensures that any proposed framework is grounded in the reality of academic work and not merely in theoretical security ideals.

Similarly, sub-finding #3 emphasizes the importance of designing policies that are account for good user-friendly. Security officers confirmed that involving users in the development and implementation process, to the extent reasonably possible, increases understanding, acceptance, and compliance. A user-centered approach acknowledges the autonomy of academic staff while providing clear guidance and support, thereby reducing the temptation to circumvent controls.

Taken together, these sub-findings establish a strong justification for the proposed MDM/MAM policy: the framework must address the risks posed by shadow IT, provide practical solutions that align with users' workflow, and be designed in a way that encourages active engagement and adherence. This rationale forms the conceptual foundation for the actionable security controls, guiding the translation of empirical insights into concrete measures that balance institutional security needs with user autonomy and usability, leading to solutions that do get adopted.

The first practical solution of the proposed security policy stems from sub-finding #4, which underscores the central importance of academic freedom in Dutch HEIs, emphasizing that staff members, particularly researchers, value autonomy and individual choices in how they conduct their work and select their tools. Imposing rigid, one-size-fits-all technological requirements risks undermining this core principle and may result in resistance to institutional policies. Sub-finding #26 further supports this by illustrating that users are more likely to accept and comply with security measures when they are presented with options rather than mandates. So, **recommendation #1** is that the security policy should use the principle of risk-based, tailored-security. This principle stresses that security controls should be reasonable based on the risk to be mitigated. In this optic, sub-findings #4 and #26 lead to the recommendation of, where possible and appropriate with the organization's risk appetite, to provide users with options. For instance, staff and researchers could be given the possibility to either use a corporate-owned device (COD) managed entirely by the institution through Mobile Device Management (MDM) or to work from their own personal device under a Bring-Your-Own-Device (BYOD) arrangement secured through Mobile Application Management (MAM). The COD option, paid for by the employer, ensures employees have the alternative to not use their own device for work purposes. BYOD, in turn, respects users' preference to integrate work into their existing digital ecosystem and preferred operating system or interface. Even with a BYOD, the application of security controls is naturally paramount. However, the policy for BYOD should focus on MAM solutions protecting institutional data and while leaving personal use largely unaffected.

Sub-finding #6 identifies the objectives deemed important by security officers in HEIs. For document labelling (Sub-finding 6.1), **recommendation #2** is to use the

information labeling option available in Microsoft Purview (sensitivity labels, Appendix 11) or a similar tool. The approach involves users selecting a label for the document they are creating or downloading, with each label corresponding to a sensitivity level, ranging from public to restricted. Based on the sensitivity label, certain actions are either not permitted or are only permitted after the user confirms their intention to perform the action. The latter approach is usually more appropriate because, from a security perspective, this security control can be circumvented without much effort by a malicious attacker. Consequently, the underlying assumption is that the user is not actively attempting to exfiltrate information. Completely blocking certain actions for confidential documents may be counterproductive, as users might circumvent restrictions by relabeling the document or copying its content into a new, less restricted file precisely due to their frustration against the security measure. Instead, the label should function as an alarm bell for the user, indicating that they are performing a potentially risky action and thereby fostering greater awareness. Labelling also facilitates the identification of documents containing personal information, supporting easier compliance with regulations. As indicated by sub-finding #18, most interviewees did not object to document labeling, and some even considered it beneficial. Therefore, it can be concluded that, while labeling requires minimal additional effort from users, it is a control that does not significantly hinder their work.

Regarding local administrative rights based on user roles (Sub-finding 6.2), this **recommendation #3** aligns with the principle of tailoring security measures to specific user categories. This principle is grounded in the well-established role-based access control (RBAC) security model. Certain groups of users legitimately require local administrative privileges, and such access should be granted to them automatically. For the majority of users, however, local administrative rights should

be restricted, with temporary access provided only when necessary. This approach shifts the challenge from a purely technical one to a communication issue: users must be clearly informed that they do not possess default administrative rights and that, should their projects require such access, they need to request it in advance. To support this, verifying application requirements should be integrated into project initiation procedures, ensuring that any necessary installations are identified early: for instance, this can be made part of the project approval process, where one of the approval requirements is that the researcher has checked whether the tools he or she aims to use are allowed. Although some users expressed frustration at their inability to install applications on short notice, the fundamental security rationale for restricting widespread administrative rights remains compelling.

Complex passwords (Sub-finding 6.3) further illustrate the need for role-based security measures. Each role or user category could have a security level assigned, with certain requirements being applicable only for higher security levels. In fact, discussions on strong passwords in the context of BYOD revealed clear user resistance from the regular user. The security necessity, for account protection, of single-sign-on or multifactor authenticator, on top of a strong password is clear and undeniable. However, in the context of passwords for access to the BYOD mobile phone or to access certain applications as part of MAM policy, the recommendation is to require complex extra authentication only for users who access highly sensitive information, such as HR personnel, board members, directors, and those involved in sensitive research. This is **recommendation #4**.

Recommendation #5 addresses the challenges associated with email forwarding, as emphasized by sub-findings #6.4 and #12. Unrestricted forwarding of institutional

emails to personal accounts poses significant security risks, yet users often view existing restrictions as barriers to productivity, particularly researchers and professors who manage multiple accounts across different institutions. Interview data indicates that many employees prefer receiving all communications into a single inbox for convenience, while others rely on forwarding specific communications to personal addresses to ensure timely responses. Although these practices are understandable, they increase the risk of data leakage, undermine compliance with data protection regulations such as the GDPR, and foster shadow-IT behaviors that bypass institutional safeguards.

Hence, the recommendation supports the security requirement of blocking email forwarding, while addressing these competing concerns. Automatic forwarding of all institutional emails to personal accounts should be disabled by default for all users. The security team should evaluate exceptions if the risk for that specific user is low and there is a valid reason. Here, security officers should weight the time and effort against the increased security: is it effective to disgruntle a perhaps older regular user who might retire in a few years? It is important to remember that users could avoid email forwarding by asking students or colleagues to email their private address directly, circumventing the control. So, the policy should provide controlled alternatives that address legitimate user needs without compromising security. For instance, emails classified as highly confidential should be non-forwardable automatically to external addresses. Furthermore, to accommodate users who need to stay informed of critical messages from specific senders, the system could implement a “notification-only” rule: instead of forwarding full email content, a brief alert would be sent to the user’s personal email, indicating that a message awaits in their institutional inbox.

Recommendation #6, which focuses on improving communication with users, is grounded in sub-findings #6.5, #7, #8, and #9. Effective communication is not only essential but also heavily dependent on timing and approach. The recommendation prioritizes engagement with new hires, ensuring that security standards are clearly conveyed to the user. The moment when new employees collect their work devices offers a valuable opportunity to explain security policies, clarify expectations, and address any immediate questions. New hires are often more receptive to such guidance, as they anticipate differences from previous workplaces and are less likely to resist changes. Establishing this foundation early supports long-term compliance and fosters a culture of security awareness.

For existing employees, conventional methods such as emails or digital campaigns proved to be less effective, especially on a large scale. Instead, direct personal interaction has greater potential to build trust and improve adherence. This does not necessarily require formal sessions; rather, informal visits by security officers can be used to show the security flag, communicate changes, address concerns, and, especially, listen to user feedback. Such interactions create a sense of collaboration rather than imposition, increasing the likelihood of acceptance.

While this approach is resource-intensive and demanding, implementing it gradually, starting with high-risk user groups, can make it sustainable and impactful. By aligning communication efforts with both user needs and institutional priorities, this recommendation offers a pragmatic strategy to strengthen security culture across the organization.

Recommendation #7, derived from Sub-findings #10 and #22, focuses on notifying users when they engage in activities that pose security risks. Interview data indicate

that users value real-time, context-specific guidance rather than abstract, retrospective rules. Participants expressed a preference for notifications that appear at the point of action, such as banners or pop-ups on sites where uploading documents is discouraged. These notifications should not merely block actions but also explain why the chosen tool or behavior is insecure and suggest safer alternatives. Users emphasized that such explanations would not only reduce frustration but also improve their understanding of security requirements.

This feedback underscores the importance of an approach that is both preventive and educational. A contextual notification system offering concise, actionable messages at critical moments can effectively guide users toward compliant behavior without creating unnecessary friction. For example, when a user attempts to upload a sensitive document to an unapproved platform, a notification could warn them of the risk, explain the policy rationale, and provide a link to an approved solution. This aligns with principles of human-centered security, recognizing that users typically prioritize convenience over malice and are more likely to comply when they understand the reasoning behind restrictions.

While it is impractical to implement notifications for every potential risk scenario, prioritizing high-impact actions, such as external sharing of confidential documents, forwarding of confidential emails, or use of unauthorized applications, ensures meaningful coverage.

Recommendation #8, based on Sub-findings #15, #17, and #19, proposes the use of additional authentication measures, particularly for network areas and resources containing sensitive information, such as confidential research data, human resources files, or personal data repositories. The interview data show that users

generally accept the need for extra passwords or authentication steps when they are proportional to the sensitivity of the information being accessed. However, thy are resistant when they think their role does not require such security measures. Addressing this concern is a great addition and could prove highly effective.

In fact, participants agree that employees with responsibilities involving highly confidential information should be subject to stronger security mechanisms than general users accessing low-risk resources.

In practical terms, the recommendation advocates the implementation of a layered authentication approach, with controls varying based on risk assessments. For instance, for institutional accounts, an additional password or PIN should be required for accessing high-sensitivity applications such as OneDrive, Outlook, or restricted shared folders. For BYOD environments, where user autonomy is an important consideration, lighter secondary authentication, such as a short PIN or biometric verification, should be applied for sensitive applications, with more stringent measures (e.g., longer PINs) reserved for high-risk roles. This balance acknowledges the importance of securing devices without imposing overly restrictive measures on personal mobile use, which could otherwise discourage compliance.

This control directly reflects the aforementioned principle of tailored security, linking authentication strength to the level of data sensitivity and user responsibility. By adopting this approach, HEIs can avoid the pitfalls of a “one-size-fits-all” security model that often generates frustration and resistance.

Ultimately, role-based extra authentication represents a pragmatic solution that operationalizes key findings from Sub-findings #15, #17, and #19, demonstrating how human-centered security measures can effectively balance institutional needs with user acceptance in a higher education context.

Recommendation #9, based on Sub-finding #20, focuses on creating a clear and comprehensive whitelist of approved tools. The primary objective is to provide users with transparency and predictability regarding which applications are secure and acceptable for use within the HEI environment. Users emphasized during interviews that such clarity would reduce uncertainty and decrease reliance on shadow-IT solutions, which often arise when approved alternatives are not clearly communicated or easily accessible.

The whitelist should explicitly indicate which tools are considered secure and, where necessary, include usage conditions. For instance, this could mean prohibiting certain tools from handling highly confidential documents. This structured approach ensures that users understand institutional expectations while being able to quickly identify approved tools. Furthermore, the policy should support streamlined processes by enabling users to install whitelisted applications independently where appropriate, or by automating the approval workflow. These measures help minimize delays and user frustration, which were recurring concerns during interviews.

To complement the whitelist, the recommendation includes the implementation of a "tool picker" feature that provides users with approved alternatives to commonly used insecure applications. For example, if a user frequently relies on services like ilovePDF for document processing, the tool picker would suggest an institutional solution offering equivalent functionality while adhering to security standards. This approach addresses two critical issues simultaneously: it guides users toward secure practices and supports their productivity by offering practical, vetted options that the user can immediately use. It also shows users that there are secure tools with similar functionality as those they are used of, but that the user may not knew about.

Recommendation #10 focuses on implementing a formal risk acceptance mechanism to emphasize individual responsibility and reinforce awareness of security requirements, as highlighted in sub-finding #25. This measure is particularly relevant for new hires and can be integrated into clauses within employment contracts or the acceptable use policy (AUP) for institutional devices, whether COD (corporate-owned devices) or BYOD (bring your own device). Ensuring that users understand both the rationale for security measures and the risks associated with non-compliance increases the likelihood of acceptance and adherence, even when these measures may partially constrain their workflow.

Sub-finding #25 indicates that users are more likely to comply with security policies when they clearly understand the potential consequences of their actions and the reasoning behind specific controls. Interview responses suggest that formal acknowledgment of these risks enhances awareness and accountability. Users reported that explicit communication of potential consequences, combined with an opportunity to agree to follow guidelines, improves their willingness to accept restrictive measures. This aligns with human-centered security principles, which recognize that informed users are more likely to act responsibly, particularly in academic settings where autonomy and flexibility are highly valued.

Building on these insights, the proposed control recommends integrating a structured risk acceptance mechanism into the institutional policy framework. This could take the form of a signed declaration, digital acknowledgment, or inclusion within the acceptable use policies. The consequences of this responsibility and how to deal with non-compliance should be decided by the single institution, but the aim is mainly to show that the institution stands behind the policy and compliance with the policy

actually matters to the organization. For new hires, the process should be embedded within onboarding procedures to ensure that users understand security rationale, potential risks, and their individual responsibilities from the start. Introducing this mechanism at the point of entry fosters a culture of accountability and minimizes confusion regarding policy requirements.

The design of this mechanism should prioritize clarity and usability over administrative complexity. It is intended as an educational and awareness-building measure rather than a punitive tool. The process may include concise explanations of key policies, examples of common risks, and practical guidance on mitigating them. For instance, it could clarify why forwarding confidential emails to external accounts is restricted or why only approved applications from a whitelist may be used.

These recommendations have been synthesized as “draft recommendations” (Appendix 6) and in PowerPoint slides to be shared for the validation process.

5.6 Validation

The proposed MDM/MAM security controls were validated using the resources and opportunities available during the study. Ideally, structured focus groups with a representative sample of users, security professionals, and other IT experts would have been conducted to systematically assess usability, acceptance, and practical challenges. Such a process would have allowed for a richer discussion of the proposed recommendations, particularly if the range of participants had included multiple institutions and a variety of roles. Due to time and logistical constraints, however, this was not possible. This limitation is acknowledged, and future research

should include such formal and thorough validation through properly organized focus groups.

Instead, for this thesis, validation relied on three main sources: internal iterative validation prior to the policy proposal, external validation with security officers, and external validation with users. While the structure of the validation is academically sound, the process was carried out informally rather than formally.

5.6.1 Iterative Validation

In order to ensure that the policy proposal was grounded in opinions shared by more than just a couple of interviewed users, an iterative approach was user when preparing the interview questions. In fact, questions in later interviews were shaped to verify the answers given in previous interviews. As a result, users across different roles consistently highlighted fairly similar challenges and opinions: for instance, some concerns, as communication, were mentioned consistently across the interviewed sample.

This results in proposed security controls that are not based on isolated individual opinions but rather reflect recurring patterns across at least a few diverse participants. The consistency that emerged through this process supports the claim that the recommended controls are appropriate, at least on a small scale. Nevertheless, this cannot fully substitute for formal testing, particularly given the limited number of interviews conducted. Hence, the human-centered security recommendations require further validation.

5.6.2 External Validation with Security Professionals

The external validation was conducted during the SURF conference, where the research was presented to participants. The audience was first introduced to the research before being shown the recommendations. Part of the talk was dedicated to discussion with the audience, which consisted mainly of security officers and other IT stakeholders. Each recommendation was explained together with its underlying rationale, and the audience provided valuable feedback.

During the discussion, the concept of tailored security presented in recommendation #1 intrigued the participants. They agreed that tailored security, in addition to a baseline applicable to everyone, could be an effective way to direct security efforts where the risks are high. The main objection, however, concerned the fact that stricter security controls might not be well received even by the institutions' leadership (such as faculty deans or executive board members), who currently enjoy little information security restrictions.

Recommendation #2, which involved labeling information, was met with some skepticism. Concerns were raised about the technical effort required to tailor actions based on sensitivity labels, and doubts were expressed as to whether users would consistently apply the labels, and if these would be applied at all. Recommendations #3 and #4 were not discussed.

Recommendation #5, which addressed email forwarding controls, received broad approval. Although participants agreed that it would not solve all user-related problems, they noted that it would make security more user-friendly without compromising protection. Recommendation #6, focusing on communication, also made sense for security professionals: they acknowledged the importance of using available opportunities to raise security awareness and of informing new users about

security policies. One professional mentioned that their organization was considering setting up a “trust center” where staff could easily access relevant security information and policies, thereby improving communication efforts. At the same time, concerns were raised about the time and resources required for communication efforts, as well as the perception that older generations are often the most resistant to security measures. The general conclusion, however, was that starting with new employees is a good and realistic tactic.

Recommendation #7, which proposed notifications or pop-ups of security-relevant events, sparked significant debate. While some praised their potential to encourage immediate corrective action, others feared that users would simply ignore them, despite the considerable effort needed to implement such systems. Recommendation #8, which proposed role-based extra authentication measures, was more positively received: in fact, the audience agreed that such a measure could effectively protect sensitive data while minimizing intrusion and disruption on users’ devices, particularly in BYOD contexts. Similarly, Recommendation #9, which concerned the implementation of whitelists and tool-pickers, was warmly welcomed. Several participants mentioned that their institutions already had such tools in place, and that they were effective in providing users with clarity about secure tools. In contrast, the audience agreed that recommendation #10 would be very difficult to implement: the idea of requiring employees to sign risk acceptance forms was seen as likely to face high resistance, not just from users but also from HR departments and other stakeholders. Additionally, concerns were raised about how to respond if influential staff members refused to sign. The consensus was that while raising awareness remains important, formalizing risk acceptance is not feasible at present.

5.6.3 Informal User Validation

To complement the discussion held during the talk, some degree of validation from the users was beneficial. This was achieved through informal talks with nine university and HBO employees from a variety of roles, including academic staff, administrative personnel, and IT support. These discussions took place during social moments and meals at the SURF conference. The recommendations were presented conversationally, with the goal of assessing whether users would accept and adopt such measures in practice. In seven of the nine conversations, the slides used in the presentation were also shown to participants.

The user feedback was generally positive but highlighted several important concerns. Many participants welcomed the concept of tailored security and felt confident that users would have no difficulty labeling documents. Some users remarked that labeling could help them avoid mistakes themselves. In contrast, recommendation #3 was met with some skepticism, especially among researchers, who explained that it is difficult to anticipate in advance which tools they might need. While they understood that local admin rights could not be granted universally, they supported the idea of a whitelist of tools that they could install independently, aligning with Recommendation #9.

Recommendation #4, concerning additional authentication measures, consistently raised doubts. Although users were not enthusiastic about the prospect of additional passwords, some acknowledged the necessity of such measures if limited to essential situations. Many expressed support for Recommendation #8, which applied extra authentication only to specific roles, and several noted that Recommendations #4 and #8 could usefully be combined. When discussing Recommendation #5, all users acknowledged that email forwarding is widely practiced and anticipated some

discontent if it were restricted. However, they also suggested that explaining the reasons behind the restriction would reduce resistance. This supports the earlier observation in the thesis that when users understand *why* a security control is being introduced, they are more likely to comply and less likely to develop workarounds.

In line with Recommendation #6, all users agreed that communication is crucial. Most also reacted positively to Recommendation #7, noting that notifications, pop-ups, and other alerts would actually help them. Recommendation #10, however, was almost uniformly rejected, with most participants expressing strong discomfort at the idea of signing a risk-acceptance document.

5.6.4 Validation Conclusion

This validation process, although informal and limited in scope, provided essential insights into the feasibility and acceptability of the proposed controls. In general, users reacted positively to the recommendations, with the exception of Recommendations #3, #4, and #10. From the perspective of security professionals, the main concerns centered on the high implementation effort required for certain measures.

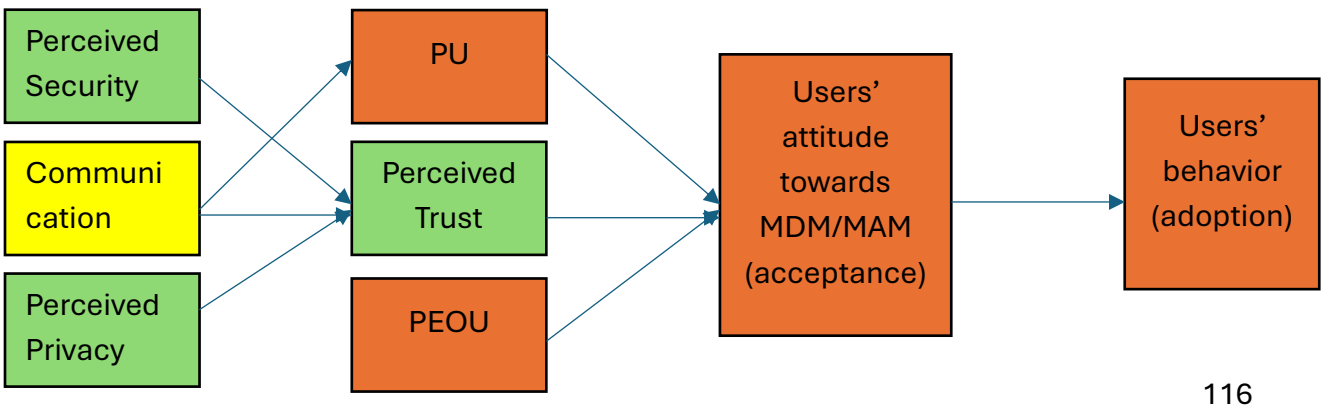
Future work should therefore employ structured focus groups and pilot implementations to assess more thoroughly the effectiveness, usability, and sustainability of these controls. Some pilot projects are already underway in various institutions, and these may provide valuable insights in the coming years.

Chapter 6: Findings & Recommendations

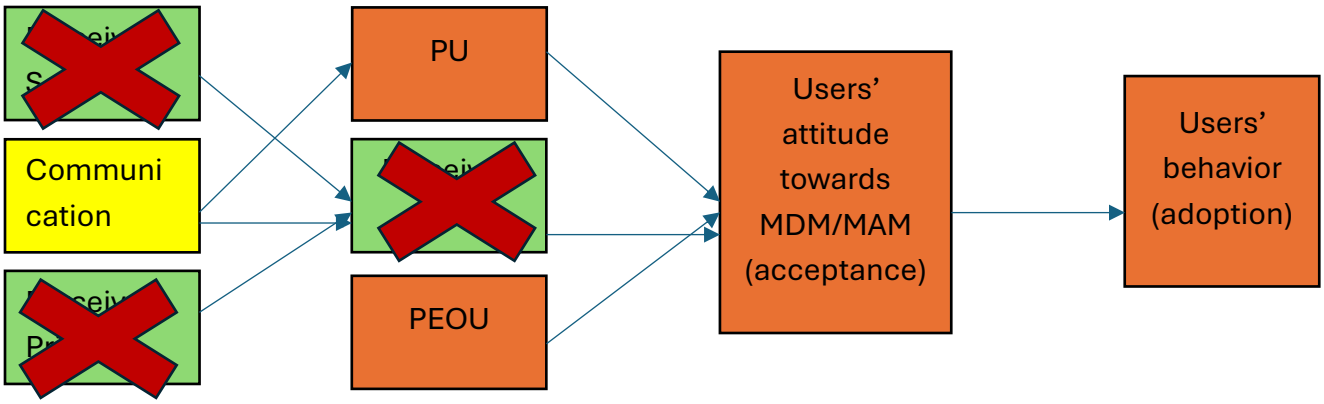
This chapter illustrates the final findings of this research, after writing a draft recommendations and going through the validation process. The findings below are based on this small-scale study and broad generalization is not possible.

This research produced two main findings. From an industry perspective, the findings have been translated into recommendations, which will be presented shortly. From an academic perspective, this research, thanks to sub-finding #21, hinted that privacy might not be a major concern among employees in higher education, at least from an MDM-MAM standpoint. Some users did mention that they wonder what IT can see from their managed devices. However, in the interviews, users did not mention privacy as a factor contributing to the acceptance of the MDM-MAM solution. Diving more into the possibility of an updated framework, it turns out perceived security of the MDM-MAM tools were also not often mentioned by the participants in the study: all the security discussions referred to how much security the MDM-MAM solutions would bring, which is, in other words, the perceived usefulness of the solution. Given the time constraints, this was not investigated further and is left for future researchers to address.

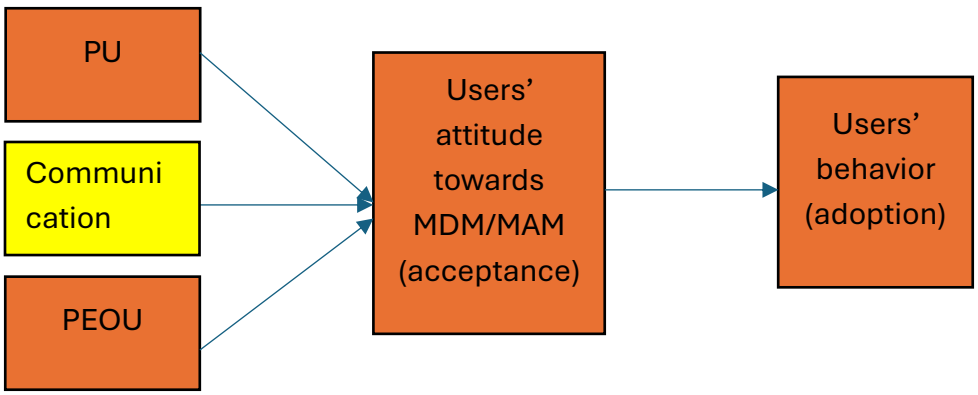
The consequences for the theoretical framework is that the version of the TAM used as theoretical framework in Chapter 3, and reported here below, is found to be not fully applicable.



From the original model, trust, should be removed: in fact, the form of trust conceptualized by Zhang (2024) does not seem to apply well to the context of MDM-MAM solutions, at least based on what could be researched in this study. Instead, as confirmed several times throughout the research, communication was observed to play a crucial role. In fact, both the interviews and the validation phase asserted that communication about the technology, its workings, and the reason for such technology play a key role in the attitude of the users towards acceptance.



The final framework for this thesis turned out to be as depicted below:



This is a new extended version of the TAM, which might be applicable to other contexts. It would be interesting for future studies to test this version of the TAM as well as reassess the value of Trust on a larger scale.

As mentioned before, several findings from the research process have been translated into practical recommendations. This is the outcome of the study and is presented below. In comparison to the pre-validation draft, recommendations #4 and #8 were combined and made more generic about applying extra access and authentication methods only to certain roles, on top of the baseline access controls that apply to everyone. Recommendations #3 and #10 were removed due to implementation complexities and lack of positive widespread reception. Recommendation #7 was not changed, despite the concerns from the security officers, since users had very positive reactions to this control, with almost all users saying that a notification would help us behave more securely. Despite the skepticism about the labeling of recommendation #2, the recommendation still stands.

Recommendation A – Risk-Based, Tailored Security

On top of a first basic layer of security controls applicable to all employees, stricter controls should be proportional to the sensitivity of the data and the role of the user. For instance, for users with access to large amount of personal data or to sensitive or confidential data, stricter security controls are legitimate and justifiable. Applying this principle is the context of higher education is critical, as it demonstrates that, where possible, freedom is left to the users. Furthermore, when possible, staff should be able to choose between corporate-owned devices (COD) managed via MDM or their own personal devices (BYOD) secured through MAM. COD provides the

option of a device fully meant for work, while BYOD respects user autonomy, integrating work into familiar ecosystems. For BYOD, security measures should focus on protecting organizational data, leaving personal use largely unaffected.

Recommendation B – Document Labeling: it's all about consciousness

Documents should be labeled according to sensitivity levels, such as public, internal, confidential, or restricted. This can be achieved using Microsoft Purview or similar tools. Users select a sensitivity label for each document they create or download. Certain actions may require confirmation depending on sensitivity, but blocking an action altogether is not recommended, as this control can be easily circumvented. Labels act as a warning to users performing risky actions and strengthen awareness among the users. Minimal additional effort is required, and users generally perceive this as helpful rather than burdensome.

Extra information about Microsoft Purview can be found in Appendix 11.

Recommendation C – Controlled Email Forwarding

Automatic forwarding of all institutional emails to personal accounts should be disabled by default. Exceptions may be granted when risks are low and justified. Emails marked as confidential should never be forwarded externally. It is recommended to weigh the time and effort against the increased security: is it effective to frustrate a perhaps older regular user who might retire in a few years? It is important to remember that users could avoid email forwarding by asking students or colleagues to email their private address directly, circumventing the control. So,

the policy should provide controlled alternatives that address legitimate user needs without compromising security. As an example, a “notification-only” option allows users to receive alerts about messages from specific senders received in their work inbox without sending full content externally.

Recommendation D – User Communication and Engagement

Clear and timely communication is critical. For new hires, device collection provides an ideal opportunity to explain security policies, clarify expectations, and answer questions. For current employees, informal personal interactions with security officers are more effective than emails or digital campaigns. Prioritizing high-risk groups and gradually extending engagement ensures sustainability. Listening to user concerns fosters collaboration and trust, improving compliance. Practical examples of mistakes from previous incidents increase awareness and reinforce secure behaviors.

Recommendation E – Real-Time Risk Notifications

Users should, where possible, receive alerts when performing risky actions. For instance, banners or pop-ups can warn users attempting to upload sensitive documents to unapproved platforms. The purpose is increasing consciousness in the users that what they are doing may not be secure. Notifications should explain the risk and suggest approved secure alternatives. Priority should be given to high-impact actions, such as sharing confidential documents externally: an alert in Outlook informing the user they are sending or forwarding a sensitive document would be effective.

Recommendation F – Extra Authentication and Access Controls

For account protection, SSO and MFA remain paramount and should be implemented for all users, where possible. Extra authentication measures, on top of the baseline applicable to all users, should be implemented based on the sensitivity of the data and the role of the user, for instance when accessing specific folders, or on the devices of high-risk users. In fact, in the context of MDM and MAM, users such as HR staff, board members, directors, or sensitive research personnel require stronger authentication, while lower-risk users may use short PINs or biometrics, whereas high-risk roles may be required to employ longer PINs or multi-factor authentication. This recommendation refers to device access (MDM) and data access on the device (MAM), for instance when opening OneDrive.

Recommendation G – (Un)approved tools list

A whitelist of approved applications would provide clear guidance of what is allowed and what is not. Likewise, a list of unapproved tools, with an explanation of why certain tools or websites have been blocked would enhance awareness. A "tool picker" would support users in choosing secure alternatives for commonly used unsecure applications. Despite the local-admin block, users should be allowed to install approved applications themselves or request streamlined approval, fastening the response time and reducing frustration.

These recommendations have been shared with SURF and its members, including the rationale behind them (Appendix 8). The policy proposal contain recommendations: it is responsibility of the HEIs to identify the recommendations

to implement first, but it is suggested to grab the “low-hanging fruits”, as they are called in the consultancy world. It refers to those low-effort actions that deliver some improvements compared to the current situation. In this case this consist of recommendations B and D.

Chapter 7: Discussion

This chapter discusses the findings of this thesis in relation to the pre-existing knowledge found in the academic literature presented in Chapter 2. Next, This chapter critically evaluates the methodological approach employed in this research by explaining why the approach used is suitable to this research; then, it assesses the concept of trustworthiness, typically used in qualitative research, to assess the quality of the research; it presents ethical considerations; and, lastly, it identifies limitations and opportunities for future research.

7.1 Relation of the findings to the existing literature

7.1.1 Alignment with existing literature

The findings of this study largely corroborate prior research on the relation between security requirements and user autonomy in an organizational context. Previous studies (Silva, 2012; Batool & Masood, 2020; Ketel & Shumate, 2015) reported that employees often perceive MDM solutions as intrusive on personal devices, whereas MAM configurations are considered less invasive, protecting corporate data while respecting individual privacy. Consistent with these insights, participants in this study expressed a clear preference for application-level protection (MAM) on BYOD devices, while accepting device-level control (MDM) primarily on corporate-owned hardware. What mentioned so far was combined in recommendation A, which proposes a layered security approach: a basic security baseline applies to all users, while stricter controls are proportional to the sensitivity of data and user roles. High-risk users handling sensitive or personal data are subject to enhanced security measures, whereas BYOD users benefit from MAM-based

protections that preserve personal autonomy and integrate work within familiar ecosystems.

Also, this research confirms prior findings about the value of role-based, risk-proportionate controls (Yamin & Katt, 2019; Smith, 2020). Security officers and users endorsed hybrid, context-sensitive approaches that allocate stricter measures to high-risk roles, supporting recommendations A and F. Recommendation F operationalizes this principle through additional authentication and access controls for sensitive roles or documents.

Finally, the interviews revealed a presence of shadow IT, which is consistent with prior literature (Boyle et al., 2012; Gadellaa, 2022). Participants indicated that they often relied on personal tools when official solutions were inaccessible or perceived as slow, obstructive, or unfunctional. So, the findings of this thesis confirm the importance of designing security measures that are both security-effective and user-friendly.

7.1.2 Extension of existing literature

While the findings support much of the existing research, they also extend existing knowledge in meaningful ways.

First, the most significant theoretical contribution lies in the reformulation of the Technology Acceptance Model (TAM) used in this study. Previous researchers (Cheng et al., 2016; Siegel et al., 2022) both mentioned that communication, although recognized as a factor influencing acceptance, has rarely been explicitly incorporated into acceptance frameworks: they argue that this is should indeed be

addressed and thus that communication should be better integrated in technology acceptance frameworks. This thesis answers their call and, in a small-case study, does exactly that. In fact, in this study, communication consistently emerged as critical factor for higher user acceptance, with almost all users interviewed emphasizing the need for proper communication: participants described understanding "why" a measure was implemented and "how" it affected their work as more influential than the technical features of the tools themselves. As mentioned in Chapter 6, this led to a revised TAM model where communication becomes the key element of this TAM extended version.

Second, this research advances the understanding of human-centred security design by providing evidence-based recommendations that operationalize user autonomy without compromising institutional protection. While previous studies have discussed balancing usability and control (Boyle et al., 2012; Ki-Aries & Faily, 2017), few have translated these principles into implementable policy mechanisms. Recommendations A and F concretize these theoretical ideas by proposing risk-based, layered security and role-dependent security controls, directly extending the literature on access management (Yamin & Katt, 2019; Smith, 2020), and demonstrating how these concepts can be applied in higher education.

Third, the study contributes to ongoing discussions about security awareness and steering users' behaviour by showing that informational, non-punitive controls can be both effective and well-received. Previous research (e.g., Parsons et al., 2014; Beautement & Sasse, 2016) highlighted user resistance to hindering policies, but few empirical studies have evaluated user reactions to softer interventions in academic environments. This thesis lays a first stone in filling that gap through recommendations B and E, which promote awareness via document labeling and real-time risk notifications. The validation phase of this research revealed that users

perceived such measures as useful. This insight support the theory that awareness is critical when aiming to enhance user cooperation and to reduce accidental policy violations.

Fourth, from earlier research (Boyle et al., 2012), we know that shadow IT is linked to frustration with official tools. This thesis adds that awareness, speed of support, and perceived fairness of restrictions are equally decisive factors in (not) resorting to shadow IT. In fact, users often circumvented restrictions not to evade policy but to maintain productivity. Recommendations C and G directly address this gap by offering pragmatic, user-friendly solutions: controlled email forwarding policies balance risk with convenience, and an approved/unapproved tools list paired with a "tool picker" offers approved alternatives.

Finally, the study provides a sector-specific contribution by contextualizing MDM–MAM adoption in HEIs, an environment where autonomy, privacy, and academic freedom are deeply valued. Most previous EMM research focused on corporate or governmental contexts (e.g., Ketel & Shumate, 2015; Yamin & Katt, 2019), where a hierarchical authority is present and supports enforcement. This thesis extends the literature by suggesting that acceptance in HEIs seems to rely less on authority and more on collaboration and perceived fairness and proportionality. The recommendations proposed, particularly recommendation D (user engagement and communication), translate abstract user-centred principles into concrete, scalable practices such as personal onboarding discussions, high-risk group prioritization, and informal engagement between users and security officers.

To conclude, these contributions to the current research suggest that security acceptance in higher education depends predominantly on communication efforts, proportionality, and usability. This insight adds both theoretical knowledge and

practical strategies for implementing MDM–MAM frameworks in user-sensitive environments.

7.1.3 Unexpected findings

The most unexpected outcome was the limited salience of trust as conceptualized in Zhang's (2024) extended TAM. While this research's participation was too limited to draw general conclusions, it was surprising that neither privacy, nor trust were mentioned as primary elements for acceptance. In fact, privacy concerns were far less pronounced than reported in the broader BYOD literature (Miller et al., 2012; Alotaibi & Almagwashi, 2018). All in all, this suggests that in HEIs communication may functionally replace trust as the key mechanism through which users decide on their acceptance of security policies and controls. This finding does not diminishes the overall importance of trust but, rather, hints that it might be built indirectly through clear, consistent communication, which, therefore, should be prioritized.

7.2 Methodological Evaluation

7.2.1 General Approach

This study adopted a Design Science Research approach, the suitability of which has been established in chapter 4. While DSR is widely recognized as a robust method for addressing complex socio-technical problems, discording voices do exist (Pello, 2023). However, this thesis' methodological choices and the approach used succeeded in delivering research-based recommendations. The approach is solid as

each step built up pieces of information to then converge into recommendations grounded in the translation of the information gathered into actionable solutions.

Despite these strengths, the methodological approach is not without limitations: mainly the use of convenience sampling for the semi-structured user interviews could have caused some bias in the responses. More importantly, the validation process strongly needs further research to reach stronger validation, especially from the user's perspective: what done in this thesis, while valuable, is not classifiable as a rigorous validation process. Lastly, the sample size, though diverse in roles, was small, limiting generalizability. Despite this, the small sample size fits with the qualitative nature of the study, and allowed in-depth investigation and research that would have not been possible with a larger sample size.

7.2.2 Preliminary talks with SURF

This first step was a perfect complementation of desk research: while desk research does provide deep academic knowledge on EMM, only the experience of professionals actively involved in these practices could allow a clear identification of the problem at hand.

These preliminary talks were carried out internally within SURF, which as advantages and disadvantages: on the one hand, these professionals were easily accessible and hold vast knowledge about the higher education context. On the other hand, professionals within SURF lacks the breadth of knowledge that I would have gained by holding primary talks with a wider array of professionals: there talks were limited in time and were primarily reflective of SURF's perspective rather than a broad cross-section of institutions. Nevertheless, these discussions were

instrumental in framing the research questions and ensuring that the study was grounded in the realities of Dutch HEIs.

7.2.3 Desk research

Desk research was paramount in providing a foundational understanding of MDM-MAM systems, security frameworks, and prior studies on human-centered security. This step enabled the researcher to map existing knowledge gaps and identify relevant information to structure the design of the interviews, and already conceptualize possible recommendations. All in all, desk research was valuable, but could not replace primary data collection.

The approach of using Google Scholar and the university library for finding papers, articles, and books is a standard practice and allowed for the finding of several peer-reviewed sources.

7.2.4 Unstructured interviews CISOs

Unstructured interviews with CISOs provided insights into organizational security policies, risk assessments, and the perceived challenges of MDM-MAM deployment. The unstructured format allowed for flexibility, enabling participants to raise issues not initially anticipated.. The richness of data these interviews provided are a major strength, as they captured organizational nuances that would have been difficult to predict. Especially, they provided unique contextual challenges of Dutch institution, for instance the current issue of reducing reliance on tools produced by

US companies, while many security tools available and used are actually from US companies.

On the other hand, these interviews, being unstructured, carry the risk of inconsistency and interviewer bias: different CISOs emphasized different topics, and the lack of a standardized script made direct comparison of responses challenging. Furthermore, the number of CISOs interviewed was limited, which may not fully reflect the heterogeneity of security practices across HEIs. Despite these limitations, the topics discussed were similar, if not the same, across many interviews, and provided critical insights for the preparation of the user interviews.

7.2.5 Semi-structured interviews employees

Semi-structured interviews with employees were designed to explore user behaviors, perceptions, and compliance patterns with MDM-MAM controls. A table mapping interview questions to research objectives (Table 8, Appendix 9) ensured comprehensive coverage of relevant topics, including shadow IT use, labeling practices, and attitudes toward extra authentication. This approach balanced structure with flexibility, allowing participants to elaborate on their experiences and concerns: fully structured interviews would have forced the discussion on topics that might have not been relevant to the context of the specific institution or to the individual user. Table 8 was also used to check that the researcher had thought of at least one question for each interview goal, hereby strengthening the research quality.

Adopting a critical eye, while the semi-structured format enhanced depth and user voice, the study's relatively small sample size and self-selection of participants limit generalizability. Ideally, interviews would have been carried out until theoretical

saturation was reached, but this proved not feasible for this research's context. Sample size is a limitation, especially if coupled with the sampling method used: convenience sampling. While this was a forced choice in this research context, it does affect the likelihood of the sample not being fully representative of the user population.

Nevertheless, interviewed users work at different institutions across the Netherlands, and these users have very different roles. This does provide enough breadth in the sample population to support a good degree of accuracy of this research. Additionally, the consistency of themes across interviews supports the credibility of the findings.

7.2.6 Validation

The three-step validation process, explained in chapter 5, supports the final recommendations for the security officers, but does miss a quantitative element and could have better rigor. In fact, a quantitative element (such as a survey) could have strengthened the validation process. Alternatively, structured focus groups or pilot implementations could have provided a more systematic evaluation of widespread usability. This was not feasible in the context of this thesis. However, considering that both security officers and the validating users reacted positively to the proposed recommendations, it can be claimed that broader acceptance is likely enough for the recommendations to be communicated to the security departments, which could investigate this further within their own institution to then discover what works best in their local context.

7.3 Quality Criteria: Trustworthiness

Ensuring trustworthiness is essential in qualitative research to ensure that the research has delivery a high-quality product. Especially important is that the findings are credible, neutral, consistent, and potentially applicable to other contexts. In line with Lincoln and Guba (1985), this study evaluated trustworthiness using four key criteria: credibility, confirmability, dependability, and transferability. This section critically explains how this research meets the trustworthiness criteria.

7.3.1 Credibility

The credibility criterion refers to the confidence that the findings accurately represent participants' experiences and perceptions. In other words, credibility assesses whether the results genuinely reflect the reality. This criterion is foundational in qualitative research because the usefulness of the findings, and any recommendations derived from them, heavily depend on how accurately participants' perspectives are captured and interpreted.

Credibility is commonly achieved through strategies such as triangulation of data sources and attention to negative or deviant cases. In the case of interviews, citation and quotes can strengthen credibility by allowing the participants' voices to be represented directly. Moreover, persistent engagement and iterative data collection help ensure that findings are grounded in thorough observation rather than impressions with little depth.

This research established credibility primarily through triangulation, combining insights from desk research, unstructured interviews with CISOs, and semi-structured interviews with employees. Persistent observation and iterative

refinement of both interview questions and interview findings ensured that emerging themes were adequately explored. The researcher worked with these themes multiple times before developing the recommendations.

Despite this, the process was not perfect: final interpretations could have been sent back to all interviewed users for verification that their claims were correctly interpreted. This was only done once upon request of the user. Nevertheless, the triangulated approach and attention to both typical and deviant cases provided a solid foundation for trustworthy findings.

7.3.2 Confirmability

Confirmability is the second trustworthiness criterion. It addresses the degree to which findings are actually shaped by participants' perspectives rather than researcher bias, preconceptions, or personal motivations. Researcher bias is hard to eliminate, but it can be reduced or, at least, acknowledged. Checking for confirmability means verifying that bias is reduced to the minimum and that the residual bias is recognized. This ensures that the conclusions drawn are firmly grounded in the data, supporting the neutrality of the research. Confirmability is particularly important in qualitative studies where the researcher is deeply and actively involved in the research, for instance in the interviews.

Confirmability can be enhanced by maintaining a detailed audit trail of research decisions, documenting the coding and analytical process, triangulating multiple sources, and practicing reflexivity. Reflexivity refers to the critical reflection of one's own potential biases and assumptions, which might have inadvertently altered the results, for instance when a selection needs to be made. Explicit disclosure of the

researcher's background and involvement helps readers contextualize interpretations.

In this study, confirmability was actively pursued to ensure that the findings were grounded in participants' perspectives rather than shaped by the researcher's own background in IT and security. Each recommendation was explicitly linked to specific sub-findings from the interviews, making it possible for readers to trace recommendations back to the sub-findings and to the participants' statements. The coding process was meticulously documented, resulting in a transparent audit trail that records decisions made during data analysis and theme development. This documentation provides a clear account of how raw data evolved into the final recommendations, supporting the neutrality of the findings. Reflexivity played a critical role throughout the research: as a security officer and a student with a background in IT security, I remained aware of my potential biases, such as the possibility to prioritized security over usability. I took deliberate steps to mitigate the risk of bias by seeking alternative interpretations during analysis, and constantly reminding myself the human-centered approach I was applying. Triangulation of multiple data sources further reduced the influence of any single viewpoint and reinforced the grounding of the results in diverse perspectives.

Although the study made significant efforts to maintain neutrality, it is not exempt from critiques. In fact, some potential bias from the researcher's prior IT experience cannot be entirely ruled out, especially considering the sample size and sample population of the interviewed users. Also, the fact that part of the process consisted of the researcher filtering content and analysing interview transcripts makes the presence of some bias possible. Nevertheless, the semi-structured nature of the user interviews, and the explicit connections of recommendations to empirical data and

the documented analytical process provide reasonable assurance that the findings are truly grounded in participants' perspectives.

7.3.3 Dependability

The third trustworthiness criterion, dependability, relates to the stability and consistency of the research process and findings. It examines whether similar results would likely be obtained if the study were repeated under comparable conditions. Dependability is crucial for establishing methodological rigor and ensuring that the conclusions are reliable. This can be obtained through strategies such as maintaining an audit trail, iterative questioning, triangulation of data sources, peer review, and self-critical reflection. It is also possible to involve external researchers to verify the coding and interpretations and ensure it is consistent.

Dependability in this research was promoted through the iterative development of the interview questions. These questions, in fact, were adapted based on previous responses, ensuring comprehensive coverage of relevant themes, particularly if mentioned by other users. An audit trail was maintained for all research stages, including data collection, coding, and recommendation synthesis.

The main limitations regarding dependability arise from the relatively small and convenience-based sample. This means that repeating the study with a different sample may report different findings. However, the iterative approach, careful documentation, and triangulation of multiple sources provided reasonable consistency and methodological rigor.

7.3.4 Transferability

Transferability assesses whether the findings can be applied or adapted to other contexts. In qualitative research, transferability relies on providing sufficient detail for readers to judge the applicability of results in their own settings. In-depth description of participants, context, and methods allows other researchers or practitioners to evaluate whether the conclusions might be relevant elsewhere. In fact, transferability is supported by rich contextual information, detailed participant demographics, purposive sampling to capture diverse perspectives, and thorough descriptions of procedures and findings. These measures allow other researchers to make informed judgments about the applicability of results beyond the immediate study context.

For this thesis, the research provided detailed contextual information about higher education institutions, participant roles, and organizational settings for MDM-MAM deployment. Clear descriptions of the interview procedures and rationale behind security controls were included and explained. Purposive sampling ensured that participants represented a variety of roles, experiences, and institutional contexts, albeit still in the educational context.

Since HEIs are a very particular context, the findings are inherently specific, which limits direct applicability to institutions in other countries or with different governance structures. Even further, the struggles themselves that led to the necessity of a balance between usability and security may be very different in other contexts.

7.4 Ethics

Ethical integrity was maintained through informed consent, anonymity, and secure handling of sensitive information. Participants could withdraw at any time, and no identifiable data was disclosed. A limitation is the informal validation during the SURF conference, which may have influenced participant responses due to social desirability. Nonetheless, overall ethical standards were upheld and the interview's plan received approval. The study complies with the ethical declaration, attached in Appendix 7.

7.5 Limitations & Further research

This study has a number of limitations that need to be considered when interpreting the findings. These have already been mentioned throughout the research process and are summarized here.

The first limitation regards the sample size of the interviews. While this was not a significant issue for the interviews with the CISOs, it is a much bigger limitation when it comes to establish employees' perception. The sample was small, with eight participants, which limits how widely the results can be generalized.

Another limitation is that the validation process was informal. Feedback was collected through discussions rather than structured focus groups or pilot implementations, which means the recommendations have not yet been tested rigorously in practice.

In addition, the study relied on self-reported potential behaviors. Participants may have provided responses that differ from their real opinions and from how they would really behave if the scenarios depicted became a reality.

Time constraints also limited the depth of exploration into certain areas, particularly users' privacy concerns and their perceptions of the security of MDM-MAM tools. As a result, trust as a combination of security and privacy was removed from the final applicable TAM model. While this is correct based on this research, more time might have made the privacy aspect emerge.

These limitations already touch upon possible improvements in future research and interesting topics to investigate. For instance, structured focus groups or pilot projects could be used to test how practical and usable the proposed recommendations are, and to explore how well they are adopted over time. Investigating privacy perceptions in relation to MDM-MAM adoption would provide a clearer picture of user acceptance. Expanding the study to include more institutions and different cultural or national contexts would make the findings more generalizable. Testing this TAM framework and the recommendations in other organizational settings and contexts would help assess its broader applicability. Finally, exploring how all of this can be combined with the desire of reducing reliance on US-based tools and services could offer innovative insights into security, compliance, and autonomy for higher education institutions.

Chapter 8: Conclusions

This thesis investigated the adoption and acceptance of Mobile Device Management (MDM) and Mobile Application Management (MAM) solutions within Dutch Higher Education Institutions (HEIs), focusing on how organizational security requirements could be reconciled with employee perceptions and their usability needs. The research was motivated by the challenges that HEIs faced against shadow-IT.

Through a combination of unstructured and semi-structured interviews with security professionals and employees, desk research, and a Design Science Research (DSR) approach, this study produced insights that extended both practical understanding and academic knowledge. The primary contribution consisted of a set of policy recommendations aimed at fostering higher acceptance of MDM and MAM tools while simultaneously ensuring the protection of institutional data.

A central aspect of this research is the critical influence of organizational culture and good communication practices. In fact, HEIs are characterized by decentralized governance, diverse faculty cultures, and strong norms of academic freedom, which collectively shaped security behavior. Chapter 6 showed that acceptance of security policies was not solely a technical issue but was deeply intertwined with organizational culture, appropriateness of the security controls, and, especially, good communication, confirming the assumptions of chapter 1 and of section 3.2. In fact, employees-users are more likely to comply with MDM and MAM policies when they perceive the security measures as justified, proportionate, and when these are clearly communicated. Participation in the policy design and engagement with the users fosters perceptions of fairness and proportionality: in fact, if users see the security controls are fair and proportionate, as suggested in recommendation A, users

should increase compliance. The same occurs if users feel listened to, and see their concerns addressed: this seems to lead to a reduction in shadow IT.

From a theoretical perspective, this research contributed to the Technology Acceptance Model (TAM) literature by integrating trust, communication, and organizational structure as moderators of acceptance. Methodologically, the research employed a Design Science Research approach, combining abduction and deduction phases to develop policy recommendations grounded in empirical insights. While the sample size and scope were limited, this approach still allowed the development of actionable recommendations based on both usability and security.

Several practical implications emerged. For academics, it was discovered that proper communication, perceived usefulness and perceived ease of use are more important to users than trust, at least in this context. For the industry, a list of recommendations for security officers has been drafted, validated, and amended accordingly. The key concept that emerges from these recommendations is to tailor security strategies, when possible, on top of a common security base-line. Communication strategies needed to be proactive, transparent, and participatory, involving users in policy co-design to enhance trust and perceived proportionality.

In conclusion, this thesis demonstrated that effective adoption of MDM and MAM in higher education is a socio-technical challenge: technical controls alone are insufficient, and user engagement and proper communication are equally crucial. The findings reinforced that security policy design needed to consider the lived experiences of employees. This, in turn, fosters higher acceptance of MDM and MAM solutions contributed to stronger information security, reduced shadow IT, and more resilient institutional IT ecosystems, offering benefits not only to the organizations themselves but to the broader academic and societal context in which they operated.

Acknowledgements

First and foremost, I would like to thank the security professionals I had the opportunity to interview and talk to throughout this research. I value greatly the insights I gained from them, and I will carry their lessons with me as I move forward in my career. Spending so much time in close contact with experts in the field has reinforced my commitment to building a future in information security.

I am deeply grateful to Joost and Hanna for their unwavering support and guidance. Their mentorship went far beyond supervision, helping me navigate challenges and steering this research in the right direction. My sincere thanks also go to the entire Security Awareness and Organization team at SURF, as well as to everyone I had the privilege of crossing path with at the Radboud University.

I am profoundly thankful to my best friends—Tommaso, Giacomo, Gabriele, Chiara, and Francesco—for always offering a listening ear and being there whenever I needed them. To my younger siblings—Sofia, Stefano, and Sara—thank you for reminding me, through the power of pure love, that life is beautiful and for making even the hardest days, days worth living. Finally, to my future children: every struggle, hardship, and setback is worth enduring if it means I can one day wrap you in the warmth of my love.

My academic journey across Leiden and Nijmegen has been truly enriching. The internships, projects, and challenges I embraced along the way have shaped me profoundly, both as a student and as a young professional. As I now take my first steps into the professional world, I do so with gratitude, optimism, and a commitment to contributing to a more secure IT ecosystem.

Responsible use of Large Language Models

Large Language Models have been used ethically and responsibly in this thesis. No content was generated by Artificial Intelligence, the use of which was limited to improving the form of this thesis. Tools such as ChatGPT and Grammarly have been used to increase writing quality, flow, and structure, and to remove grammar errors. Scribbr was used to automatically set the sources in APA for the reference list.

Appendix

Appendix 1 - Reference List

42Gears Mobility Systems. (2021). App Wrapping vs. Platform Native Containerization: Which Mobile Application Management (MAM) strategy is better? In *42gears.com*. https://www.42gears.com/wp-content/uploads/2021/08/App-wrapping-or-Platform-native-containerization_-1.pdf

Abun, D., Javier, J. P. G., Gamponia, J. I. B., Magallanes, T., & Julian, F. P. (2022). The effect of employees' computer and internet self-efficacy on job satisfaction. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(3), 130–140. https://doi.org/10.20525/ijrbs.v11i3.1727

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality. In *Springer eBooks* (pp. 15–29). https://doi.org/10.1007/0-387-28222-x_2

Alotaibi, B., & Almagwashi, H. (2018). A Review of BYOD Security Challenges, Solutions and Policy Best Practices. *IEEE*. https://doi.org/10.1109/cais.2018.8441967

Android. (n.d.). *Android Work Profile*. https://www.android.com/intl/us_en/enterprise/work-profile/

Apple. (n.d.). *About Apple device supervision*. Apple Support. https://support.apple.com/en-euro/guide/deployment/dep1d89f0bff/web?utm_source=chatgpt.com

Aratovskaya, A. (2024, October 21). *Start tracking user acceptance to enhance the ROI of your digital transformation - FOUNT*. FOUNT. Retrieved March 3, 2025, from https://getfount.com/resource/adoption-vs-acceptance-in-digital-transformations/#:~:text=Adoption%20just%20means%20employees%20are,day%2Dto%2Dday%20work.

ASIS&T. (2023, December 21). *What Is Information Science? - Association for Information Science and Technology | ASIS&T*. Association for Information Science and Technology | ASIS&T. https://www.asist.org/student-resources/what-is-information-science/

Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology*, *6*(3), 128–138. https://doi.org/10.1027/1614-2241/a000014

Ayedh, A. T., Wahab, A. W. A., & Idris, M. Y. I. (2023). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment:

State of the art and future directions. *Applied Sciences*, *13*(14), 8048. https://doi.org/10.3390/app13148048

Barbu, M. (2025, July 9). MDM vs MAM. *IBM*. https://www.ibm.com/think/topics/mdm-vs-mam

Batool, H., & Masood, A. (2020). Enterprise Mobile Device Management Requirements and Features. *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. https://doi.org/10.1109/infocomwkshps50562.2020.9162763

Beaudry, N., & Pinsonneault, N. (2010). The other side of acceptance: studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, *34*(4), 689. https://doi.org/10.2307/25750701

Behne, A., Krüger, N., Beinke, J. H., & Teuteberg, F. (2021). Learnings from the design and acceptance of the German COVID-19 tracing app for IS-driven crisis management: a design science research. *BMC Medical Informatics and Decision Making*, *21*(1). https://doi.org/10.1186/s12911-021-01579-7

Boyle, J. L., Smith, A., & Madden, M. (2012). Privacy and Data Management on Mobile Devices. In *pewinternet.org*. Pew Research Center. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf

Brocke, J. V., Hevner, A., & Maedche, A. (2020). Introduction to Design Science Research. In *Progress in IS* (pp. 1–13). https://doi.org/10.1007/978-3-030-46781-4_1

Bürgy, B. (2023, November 9). User adoption – the success of an IT project stands or falls on acceptance. *insights. magazine*. https://insights.tt-s.com/en/user-adoption-it-project-success-depends-on-acceptance

Butkovskiy, N. (2023, March 27). *Loaning laptops to employees: best practices and pitfalls to consider*. WorkTime. https://www.worktime.com/loaning-laptops-to-employees-best-practices-and-pitfalls-to-consider

Carstensen, A., & Bernhard, J. (2018). Design science research – a powerful tool for improving methods in engineering education research. *European Journal of Engineering Education*, *44*(1–2), 85–102. https://doi.org/10.1080/03043797.2018.1498459

Castro, W. F., & Nyvang, T. (2018). From professors' barriers to organisational conditions in ICT integration in higher education. *Tidsskriftet Læring Og Medier (LOM)*, *11*(18). https://doi.org/10.7146/lom.v10i18.96143

Cheng, G., Guan, Y., & Chau, J. (2016). An empirical study towards understanding user acceptance of bring your own device (BYOD) in higher education. *Australasian Journal of Educational Technology*. https://doi.org/10.14742/ajet.2792

Courage, C., & Baxter, K. (2005). FIELD STUDIES. In *Elsevier eBooks* (pp. 562–633). https://doi.org/10.1016/b978-155860935-8/50043-9

Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2024). Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. *Journal of Cybersecurity and Privacy*, *5*(1), 2. https://doi.org/10.3390/jcp5010002

Das, S., Kramer, A. D., Dabbish, L. A., & Hong, J. I. (2015). The Role of Social Influence in Security Feature Adoption. *Association for Computing Machinery*. https://doi.org/10.1145/2675133.2675225

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

Davis, F. D. (1993). User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, *38*(3), 475–487. https://doi.org/10.1006/imms.1993.1022

De Kok, A., Lubbers, Y., & Helms, R. W. (2015). Mobility and security in the new way of working : Employee satisfaction in a Choose Your Own Device(CYOD) environment. *Mediterranean Conference on Information Systems*, 31. https://aisel.aisnet.org/mcis2015/31/

Del Vecchio, L. (2024, November 27). *What is Bring Your Own Device (BYOD)?* PLANERGY Software. https://planergy.com/blog/what-is-byod/

Díez, M. (2023, May 17). Respectful MDM: Balancing privacy and device security. *Applivery | Android, Apple & Windows Device Management & App Distribution Platform*. https://www.applivery.com/blog/device-management/privacy-in-mdm-respect-employee-privacy-while-securing-mobile-devices-for-productivity/

Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. *Procedia Technology*, *9*, 43–53. https://doi.org/10.1016/j.protcy.2013.12.005

Doss, C. R. (2006). Analyzing technology adoption using microstudies: limitations, challenges, and opportunities for improvement. *Agricultural Economics*, *34*(3), 207–219. https://doi.org/10.1111/j.1574-0864.2006.00119.x

Downer, K., & Bhattacharya, M. (2015). BYOD Security: A New Business Challenge. *IEEE*, 1128–1133. https://doi.org/10.1109/smartcity.2015.221

Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N., & Saad, E. H. M. (2014). BYOD: Current state and security challenges. *IEEE*, 189–192. https://doi.org/10.1109/iscaie.2014.7010235

Everphone. (2024, October 16). *MDM and MAM: What's the difference?* https://everphone.com/en/blog/mdm-mam/#:~:text=and%20Microsoft%20Intune.-,The%20differences%20between%20MDM%20and%20MAM,corporate%20applications%20and%20their%20data.

Fischer, C., & Gregor, S. (2011). Forms of reasoning in the design science research process. In *Lecture notes in computer science* (pp. 17–31). https://doi.org/10.1007/978-3-642-20633-7_2

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Gadellaa, J. (2023). *Cyber threats of shadow IT in Dutch higher education and research* [Master's Thesis, Utrecht University]. https://studenttheses.uu.nl/bitstream/handle/20.500.12932/45731/Masters%20Thesis.pdf?sequence=1&isAllowed=y

Glavin, P., Bierman, A., & Schieman, S. (2024). Private eyes, they see your every move: workplace Surveillance and Worker Well-Being. *Social Currents*. https://doi.org/10.1177/23294965241228874

Goad, M., & Steele, C. (2023, April 3). *enterprise mobility management (EMM)*. Search Mobile Computing. https://www.techtarget.com/searchmobilecomputing/definition/enterprise-mobility-management-EMM?utm_source=chatgpt.com

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users. *Information & Management*, *20*(1), 13–27. https://doi.org/10.1016/0378-7206(91)90024-v

Greener, S. (2022). Digging for acceptance theory. *Interactive Learning Environments*, *30*(4), 587–588. https://doi.org/10.1080/10494820.2022.2062170

Halim, I. I. A., Buja, A. G., Zain, J. M., Ngah, A. H., & Bansal, R. (2024). BYOD Security Policy Model: A Systematic Literature Review. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 170–186. https://doi.org/10.37934/araset.62.1.170186

Hameed, M. A., & Arachchilage, N. a. G. (2018). Understanding the influence of Individual's Self-efficacy for Information Systems Security Innovation Adoption: A Systematic Literature Review. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1809.10890

Hanna, T. (2021, May 25). *Understanding the difference between MDM, MAM, EMM, and UEM*. Best Enterprise Mobility Management Vendors, MDM UEM EMM Software and MDM Platforms. https://solutionsreview.com/mobile-device-management/understanding-the-difference-between-mdm-mam-emm-and-uem/

Hayes, D., Cappa, F., & Le-Khac, N. A. (2020). An effective approach to mobile device management: Security and privacy issues associated with mobile applications. *Digital Business*, *1*(1), 100001. https://doi.org/10.1016/j.digbus.2020.100001

Hevner, N., March, N., Park, N., & Ram, N. (2004). Design science in Information Systems Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Hisgen, R. (2016, April 19). *The Dutch love affair with freedom*. Iamexpact. https://www.iamexpat.nl/expat-info/dutch-expat-news/dutch-love-freedom

Holtby, A. (2021, November 18). *OMDIA Market Radar: Unified Endpoint Management, 2021-22*. Omdia. https://omdia.tech.informa.com/om019339/omdia-market-radar-unified-endpoint-management-202122

Höpfner, E., & Promberger, M. (2023). The Elephant in the Room-Recording Devices and Trust in Narrative Interviewing. *International Journal of Qualitative Methods*, *22*. https://doi.org/10.1177/16094069231215189

Hornbæk, K., & Hertzum, M. (2017). Technology acceptance and user experience. *ACM Transactions on Computer-Human Interaction*, *24*(5), 1–30. https://doi.org/10.1145/3127358

Horváth, I. (2007). Comparison of three methodological approaches of design research. *Guidelines for a Decision Support Method Adapted to NPD Processes*. https://iced.designsociety.org/download-publication/25512/Comparison+of+Three+Methodological+Approaches+of+Design+Research

Howell, G., Franklin, J. M., Sritapan, V., Souppaya, M., & Scarfone, K. (2023). *Guidelines for managing the security of 34 mobile devices in the enterprise*. https://doi.org/10.6028/nist.sp.800-124r2

Huang, D., Rau, P. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870–883. https://doi.org/10.1016/j.ijhcs.2011.07.007

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2–18. https://doi.org/10.1108/oir-11-2015-0358

Jimshith, T., & Bai, M. A. (2024). An Evaluation of the Proposed Security Access Control for BYOD Devices with Mobile Device Management (MDM). *International Journal of Electrical and Electronics Research*, *12*(1), 276–284. https://doi.org/10.37391/ijeer.120138

Joch, A. (2020, February 14). *The evolution of mobile device management*. Technology Solutions That Drive Government. https://fedtechmagazine.com/article/2014/10/evolution-mobile-device-management

Ketel, M., & Shumate, T. (2015). Bring Your Own Device: Security technologies. *SoutheastCon*, 1–7. https://doi.org/10.1109/secon.2015.7132981

Khalil, S. M. (2013). From resistance to acceptance and use of technology in academia. *Open Praxis*, *5*(2), 151. https://doi.org/10.5944/openpraxis.5.2.5

Khan, H. U., & AlShare, K. A. (2019). Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 4–23. https://doi.org/10.1080/10919392.2019.1552743

Khellaf, R., Boudouda, S., Hacini, S., LIRE Laboratory, & Abdelhamid Mehri- Constantine2, University Constantine, Algeria. (2022). *MAM Security Enhancement: Proposed control mechanism*. https://ceur-ws.org/Vol-3176/paper7.pdf

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, *70*, 663–674. https://doi.org/10.1016/j.cose.2017.08.001

Kim, H. (2015). Acceptability Engineering: The study of user acceptance of Innovative technologies. *Journal of Applied Research and Technology*, *13*, 230–237. https://www.scielo.org.mx/pdf/jart/v13n2/v13n2a8.pdf

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lai, P. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*, *14*(1), 21–38. https://doi.org/10.4301/s1807-17752017000100002

Lapão, L. V., Gregório, J., Mello, D., Cavaco, A., Da Silva, M. M., & Lovis, C. (2014). Using Design Science Research to develop Online Enhanced Pharmaceutical Care Services. *Studies in Health Technology and Informatics*. https://doi.org/10.3233/978-1-61499-432-9-266

Lincoln, Y., & Guba, E. G. (1985). Lincoln, Yvonna, and Egon G. Guba, Naturalistic Inquiry. Beverly Hills, CA: Sage, 1985. *SAGE*. https://stars.library.ucf.edu/cirs/690/

Lisle, A. H., Merenda, C., & Gabbard, J. (2019). Using affinity diagramming to generate a codebook: a case study on young military veterans and community reintegration. *Qualitative Research*, *20*(4), 396–413. https://doi.org/10.1177/1468794119851324

Liu, H., Zhang, W., & Gao, T. (2015). A comparative study of dynamic analysis methods for structural topology optimization under harmonic force excitations. *Structural and Multidisciplinary Optimization*, *51*(6), 1321–1333. https://doi.org/10.1007/s00158-014-1218-4

Madden, J. (2013). *Enterprise Mobility Management: Everything You Need to Know about MDM, MAM, and BYOD*.

ManageEngine. (n.d.). *Mobile Device Management (MDM) software for enterprises - ManageEngine Mobile Device Manager Plus*. https://www.manageengine.com/mobile-device-management/

Marangunić, N., & Granić, A. (2014). Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society*, *14*(1), 81–95. https://doi.org/10.1007/s10209-014-0348-1

Marikyan, D., & Papagiannidis, S. (2024, December 2). *Technology Acceptance Model - TheoryHub - Academic theories reviews for research and T&L*. Retrieved March 3, 2025, from https://open.ncl.ac.uk/theories/1/technology-acceptance-model/#:~:text=According%20to%20TAM%2C%20technology%20acceptance,%2C%20influencing%20use%20behaviour%20(Davis%2C

Martin, É., Bergeron, D., & Gaboury, I. (2024). The use of vignettes to improve the validity of qualitative interviews for realist evaluation. *Qualitative Health Research*. https://doi.org/10.1177/10497323241237411

Masaryk University. (2023, April 24). *Why are universities increasingly being targeted by cyberattacks?* Cybersecurity at MUNI. Retrieved February 28, 2025, from https://security.muni.cz/en/articles/why-are-universities-increasingly-being-targeted-by-cyberattacks

MDM Settings. (2025, March 13). Cisco Meraki Documentation. https://documentation.meraki.com/SM/Profiles_and_Settings/MDM_Settings

Meier, Y., & Krämer, N. C. (2022). The Privacy Calculus revisited: An empirical investigation of online privacy decisions on Between- and Within-Person levels. *Communication Research*, *51*(2), 178–202. https://doi.org/10.1177/00936502221102101

Merhi, M. I., & Ahluwalia, P. (2018). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, *92*, 37–46. https://doi.org/10.1016/j.chb.2018.10.031

Microsoft. (2025a, March 4). *Mobile Application Management (MAM) for unenrolled devices in Microsoft Intune*. Microsoft Learn. https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/deployment-guide-enrollment-mamwe

Microsoft. (2025b, March 4). *Mobile Application Management (MAM) for unenrolled devices in Microsoft Intune*. Microsoft Learn. https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/deployment-guide-enrollment-mamwe

Microsoft. (2025c, March 4). *What is app management in Microsoft Intune?* Microsoft Learn. https://learn.microsoft.com/en-us/intune/intune-service/apps/app-management

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: security and privacy considerations. *IT Professional*, *14*(5), 53–55. https://doi.org/10.1109/mitp.2012.93

Mindanao, K. (2025, July 14). Mobile Device Management: What Is MDM and Who Needs It? *Intelligent Techincal Solutions*. https://www.itsasap.com/blog/mdm-services

Minihan, C., & Lanusse, A. (2022, November 14). Introduction to Workspace ONE UEM device management modes. *VMware End-User Computing Blog*. https://blogs.vmware.com/euc/2022/10/introduction-to-workspace-one-uem-device-management-modes.html

Misron, M. M., Shaffiei, Z. A., & Hamidi, S. R. (2011). Measurement of User's Acceptance and Perceptions towards Campus Management System (CMS) Using Technology Acceptance Model (TAM). *International Journal of Information Processing and Management*, *2*(4), 34–46. https://doi.org/10.4156/ijipm.vol2.issue4.4

Mlekus, L., Bentler, D., Paruzel, A., Kato-Beiderwieden, A., & Maier, G. W. (2020). How to raise technology acceptance: user experience characteristics as technology-inherent determinants. *Gruppe Interaktion Organisation Zeitschrift Für Angewandte Organisationspsychologie (GIO)*, *51*(3), 273–283. https://doi.org/10.1007/s11612-020-00529-7

Muraglia, S., Vasquez, A. L., & Reichert, J. (2020, August 16). *ICJIA | Illinois Criminal Justice Information Authority*. https://icjia.illinois.gov/researchhub/articles/conducting-research-interviews-on-sensitive-topics

Naveed, Q. N., Choudhary, H., Ahmad, N., Alqahtani, J., & Qahmash, A. I. (2023). Mobile Learning in Higher Education: A Systematic Literature review. *Sustainability*, *15*(18), 13566. https://doi.org/10.3390/su151813566

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Panicker, P. (2020). Embedding culture and grit in the Technology Acceptance Model (TAM) for higher education. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2005.11973

Parente, S. L., & Prescott, E. C. (1994). Barriers to technology adoption and development. *Journal of Political Economy*, *102*(2), 298–321. https://doi.org/10.1086/261933

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2007). Design Science Research Process: A model for producing and presenting information systems research. *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology*, 83–116. https://doi.org/10.48550/arxiv.2006.02763

Pello, R. (2023, November 21). Design science research — a short summary - Rauno Pello - Medium. *Medium*. https://medium.com/@pello/design-science-research-a-summary-bb538a40f669

Pierer, M. (2016). Mobile Device Management (MDM). In *Springer eBooks* (pp. 27–28). https://doi.org/10.1007/978-3-658-15046-4_2

Plangger, K., & Montecchi, M. (2020). Thinking beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, *50*(1), 32–44. https://doi.org/10.1016/j.intmar.2019.10.004

Preus, D. (2015, September 22). *The evolution of mobile application management*. https://www.linkedin.com/pulse/evolution-mobile-application-management-daniel-preus/

Quintanilla, M. (2025, March 8). The complete guide for providing laptops to employees working remotely. *Growrk*. https://growrk.com/blog/providing-laptops-to-employees#:~:text=Improved%20productivity%3A%20Employees%20can%20work,%2C%20antivirus%20software%2C%20and%20encryption.

Radboud Universiteit. (n.d.). *Information Sciences | Radboud University*. https://www.ru.nl/en/education/masters/information-sciences

Raković, L. (2020). Shadow IT – Systematic Literature Review. *Information Technology and Control*, *49*(1), 144–160. https://doi.org/10.5755/j01.itc.49.1.23801

Ramasundaram, A., Gurusamy, R., & George, A. (2022). Employees and workplace surveillance: Tensions and ways forward. *Journal of Information Technology Teaching Cases*, *14*(1), 2–6. https://doi.org/10.1177/20438869221142027

Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2021). BYOD security issues: a systematic literature review. *Information Security Journal a Global Perspective*, *31*(3), 253–273. https://doi.org/10.1080/19393555.2021.1923873

Redman, P., Girard, J., & Wallin, L. (2011). Magic Quadrant for Mobile Device Management Software. *Gartner*, G00211101. https://elrincondepachi.wordpress.com/wp-content/uploads/2012/02/gartner-mdm-magic-quadrant-2011.pdf

Renaud, K., & Van Biljon, J. (2008). Predicting technology acceptance and adoption by the elderly. *Association for Computing Machinery*, 210–219. https://doi.org/10.1145/1456659.1456684

Rondan-Cataluña, F. J., Arenas-Gaitán, J., & Ramírez-Correa, P. E. (2015). A comparison of the different versions of popular technology acceptance models. *Kybernetes*, *44*(5), 788–805. https://doi.org/10.1108/k-09-2014-0184

Rutakumwa, R., Mugisha, J. O., Bernays, S., Kabunga, E., Tumwekwase, G., Mbonye, M., & Seeley, J. (2019). Conducting in-depth interviews with and without voice recorders: a comparative analysis. *Qualitative Research*, *20*(5), 565–581. https://doi.org/10.1177/1468794119884806

Samonas, S., & Coss, D. (2014). The CIA strikes back: redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3), 21–45. https://www.jissec.org/Contents/V10/N3/V10N3-Samonas.html

Sarpong, S., & Rees, D. (2013). Assessing the effects of 'big brother' in a workplace: The case of WAST. *European Management Journal*, *32*(2), 216–222. https://doi.org/10.1016/j.emj.2013.06.008

Scarfo, A. (2012). New Security Perspectives around BYOD. *IEEE*, 446–451. https://doi.org/10.1109/bwcca.2012.79

Schall, M. A. (2019). *The relationship between remote work and job satisfaction*. https://doi.org/10.31979/etd.2x82-58pg

Siegel, R., König, C. J., & Lazar, V. (2022). The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior: A meta-analysis. *Computers in Human Behavior Reports*, *8*, 100227. https://doi.org/10.1016/j.chbr.2022.100227

Silva, P. (2012). BYOD 2.0: Moving beyond MDM. In *asprom.com*. F5 Inc. Retrieved February 28, 2025, from https://www.asprom.com/application/F5.pdf

Simon, H. A. (2019). *The Sciences of the artificial*. https://doi.org/10.7551/mitpress/12107.001.0001

Skilling, K., & Stylianides, G. J. (2019). Using vignettes in educational research: a framework for vignette construction. *International Journal of Research & Method in Education*, *43*(5), 541–556. https://doi.org/10.1080/1743727x.2019.1704243

Slonopas, A. (2024, May 3). *BYOD Security Risks and the implications for organizations*. American Public University. https://www.apu.apus.edu/area-of-study/information-technology/resources/byod-security-risks-and-the-implications-for-organizations/

Smith, D. (2020). Mobile Device Management. In *Apress eBooks* (pp. 311–338). https://doi.org/10.1007/978-1-4842-5820-0_8

SOTI. (n.d.). *Mobile Device Management (MDM) | SOTI MobiControl*. https://soti.net/solutions/mobile-device-management/

Stach, C., & Mitschang, B. (2013). Privacy Management for Mobile Platforms -- A Review of Concepts and Approaches. *Elsevier Digital Business*, 305–313. https://doi.org/10.1109/mdm.2013.45

Teixeira, J. G., Patrício, L., Huang, K., Fisk, R. P., Nóbrega, L., & Constantine, L. (2016). The MINDS method. *Journal of Service Research*, *20*(3), 240–258. https://doi.org/10.1177/1094670516680033

Toft, M. B., Schuitema, G., & Thøgersen, J. (2014). Responsible technology acceptance: Model development and application to consumer acceptance of Smart Grid technology. *Applied Energy*, *134*, 392–400. https://doi.org/10.1016/j.apenergy.2014.08.048

Toperesu, B., & Van Belle, J. (2017). Organisational Capabilities Required for Enabling Employee Mobility through Bring- Your-Own-Device Concept. *Business Systems Research Journal*, *8*(1), 17–29. https://doi.org/10.1515/bsrj-2017-0002

Tsertsidis, A., Kolkowska, E., & Hedström, K. (2019). Factors influencing seniors' acceptance of technology for ageing in place in the post-implementation stage: A literature review. *International Journal of Medical Informatics*, *129*, 324–333. https://doi.org/10.1016/j.ijmedinf.2019.06.027

Vedadi, A., Warkentin, M., Straub, D. W., & Shropshire, J. (2024). Fostering information security compliance as organizational citizenship behavior. *Information & Management*, *61*(5), 103968. https://doi.org/10.1016/j.im.2024.103968

Wallent, M. (2025, June 19). *Microsoft recognized as a Leader in the 2022 Gartner® Magic Quadrant™ for Unified Endpoint Management Tools*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2022/08/22/microsoft-recognized-as-a-leader-in-the-2022-gartner-magic-quadrant-for-unified-endpoint-management-tools/

Wani, T. A., Mendoza, A., & Gray, K. (2020). Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature. *JMIR Mhealth and Uhealth*, *8*(6), e18175. https://doi.org/10.2196/18175

Warner, C. (2023, February 7). *How to successfully implement MDM for BYOD*. Search Enterprise Desktop. https://www.techtarget.com/searchenterprisedesktop/tip/How-to-successfully-implement-MDM-for-BYOD

Webb, A. (2022, June 21). Privacy for Education Users. *JAMF*. https://www.jamf.com/blog/jamf-apple-student-data-privacy/

Weinberg, B. A. (2004). Experience and technology adoption. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.522302

Williams, M. E. (1996). *User acceptance of new information technology: theories and models*. http://hdl.handle.net/10150/105584

Wolford, M. (2025). *Is your employer watching you?: Invasive employee surveillance in the modern era*. Carolina Law Scholarship Repository. https://scholarship.law.unc.edu/ncjolt/vol26/iss4/5

Yamin, M. M., & Katt, B. (2019). Mobile device management (MDM) technologies, issues and challenges. *ICCSP '19: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 143–147. https://doi.org/10.1145/3309074.3309103

Zhang, Y. (2024). Impact of perceived privacy and security in the TAM model: The perceived trust as the mediated factors. *International Journal of Information Management Data Insights*, *4*(2), 100270. https://doi.org/10.1016/j.jjimei.2024.100270

Appendix 2 - List of Interviews

Who?	When?	Type of sampling	Type of Interview
Security Department UTwente	February 2025	Purposive Sampling	Unstructured
Security Department Utrecht University	February 2025	Purposive Sampling	Unstructured
Security Department Hanze Hogeschool	February 2025	Purposive Sampling	Unstructured
Security Department Universiteit Leiden	March 2025	Purposive Sampling	Unstructured
Security Department Windesheim Hogeschool	February 2025	Purposive Sampling	Unstructured
Security Department Hogeschool Inholland	February 2025	Purposive Sampling	Unstructured
Employee 1 Windesheim Hogeschool	April 2025	Convenience Sampling	Semistructured
Employee 2 Windesheim Hogeschool	April 2025	Convenience Sampling	Semistructured
Employee 3 Utrecht University	April 2025	Convenience Sampling	Semistructured
Employee 4 Universiteit Leiden	April 2025	Convenience Sampling	Semistructured
Employee 5 Radboud Universiteit	April 2025	Convenience Sampling	Semistructured
Employee 6 Utrecht University	April 2025	Convenience Sampling	Semistructured
Employee 7	May 2025	Convenience Sampling	Semistructured

Universiteit Leiden			
Employee 8 Universiteit Leiden	May 2025	Snowball Sampling	Semistructured

Appendix 3 – Interview questions baseline

Declare on record that the interviewee has already provided consent to participate in the interview. Ask for permission to record the interview.

1. Have you been provided a mobile telephone and/or a laptop by your institution?
    a. Yes: Go to question 2
    b. No: Go to question 6
2. Which work-related tasks do you use your device for?
3. Which personal tasks do you use your device for?
4. How would you describe your experience with the device?
    a. Have you found yourself in a position where you wanted to do something with this device but this was not possible?
        i. How did you react?
    b. Have you encountered (security) limitations?
        i. How did you react?
    c. Have you encountered technical issues or required IT support because of MDM/MAM on university-owned devices?
    d. How did you experience the communication about what you are allowed to do with this device.
    e. Do you feel your privacy is respected when using institution-managed devices? (adapt to context, if no MDM is used be hypothetical)
    f. Do you feel your privacy is respected when using institution-managed apps? (adapt to context, if no MAM is used be hypothetical)

5. What kind of communication would you like to see about MDM/MAM and related limitations?
    a. Potential follow up what ifs:
        i. Post on sharepoint
        ii. Document when receiving the device
        iii. Awareness campaign
        iv. Verbal, non-verbal, visual
        v. Detailed explanation vs general
        vi. List of approved software/applications to choose from

6. Do you use a personal device for work-related purposes?

    a. Yes: Go to question 7
    b. No: Go to question 12 (if Q1 was also answered negatively)
7. Which work-related tasks do you use your device for?
8. Which personal tasks do you use your device for?
9. How would you describe your experience with the device?
    a. Have you found yourself in a position where you wanted to do something with this device but this was not possible?
        i. How did you react?
    b. Have you encountered (security) limitations?
        i. How did you react?
    c. Have you encountered technical issues or required IT support because of MDM/MAM on your personal devices?
    d. How did you experience the communication about what you are allowed to do with this device.
    e. Do you feel your privacy is respected when using institution-managed devices? (adapt to context, if no MDM is used be hypothetical)
    f. Do you feel your privacy is respected when using institution-managed apps? (adapt to context, if no MAM is used be hypothetical)
10. What kind of communication would you like to see about MDM/MAM and related limitations?
    a. Potential follow up what ifs:
        i. Post on sharepoint
        ii. Document when receiving the device
        iii. Awareness campaign
        iv. Verbal, non-verbal, visual
        v. Detailed explanation vs general
        vi. List of approved software/applications to choose from

11. If you were given a laptop, with these settings/ if your COD laptop had these settings, what would your opinion be?

    a. MDM
        i. Prevent you from downloading certain application or software without specific approval
            1. How would you like the approval process to look like
            2. List of approved applications
        ii. Longer phone password
        iii. Maximum PIN attempts

b. MAM
    i. Blocks pairing of business Onedrive to own device
    ii. Blocks copying and saving of documents on personal device
    iii. Printing company documents from printers outside your institution
    iv. Blocks automatic forwarding of emails
        1. To other unis?
    v. Blocks pairing business email to other applications besides Outlook

12. If you were asked to bring your own device for work purposes, but you were asked to install applications that do THIS [insert later], what would your reaction be?
    a. MDM
        i. Prevent you from downloading certain application or software without specific approval
            1. How would you like the approval process to look like
            2. List of approved applications
        ii. Longer phone password
        iii. Maximum PIN attempts

    b. MAM
        i. Blocks pairing of business Onedrive to own device
        ii. Blocks copying and saving of documents on personal device
        iii. Printing company documents from printers outside your institution
        iv. Blocks automatic forwarding of emails
            1. To other unis?
        v. Blocks pairing business email to other applications besides Outlook

Appendix 4 – Consent Forms

Informed Consent

English follows Dutch

Beste deelnemer,

Binnenkort vindt je interview over Mobile Device Management (MDM) en Mobile Application Management (MAM) plaats. Het interview zal beginnen met een kort uitleg en voorbeeld van MDM en MAM. Het is niet nodig om voorkennis over MDM en MAM te hebben om deel te nemen.

Zoals besproken zal dit interview plaatsvinden op *in, lokaal.*

Ik vraag jou vriendelijk het bijgevoegde document te lezen. Het document is in het Engels. Mocht je vragen hebben, kan je gerust deze stellen door te reageren aan deze email. Dit document vraagt jouw "informed consent" (geïnformeerde toestemming) voordat je kan deelnemen aan het onderzoek. Het document legt uit hoe je (persoonlijke) data verwerkt wordt en gerelateerde informatie.

Jouw toestemming kan worden gegeven:

1) Door het invullen en tekenen van het document. Stuur dan alstublieft het ondergetekende document aan mij terug. Dit document zal worden bewaard voor maximum 10 jaar.
2) Door het reageren aan deze email vanuit jouw officieel werk-emailadres (). In dit geval voeg alstublieft de volgende zinnen toe aan je reactie:

I, the undersigned:

- **fully understand the content of the attached document "Interviews consent form_MDM-MAM"**
- **have been provided information about the research background and purposes**
- **consent to participate to the interviews for the research purposes described in that document**

- **consent to the use and processing of the information I will provide during the interviews as described in that document**
- **provide consent to the use and processing of personal data provided during the interviews as described in that document**
- **understand that I have the right to withdraw from the interview at any time without having to provide any explanation**

Full name:

Date:

Dear participant,

The date of your interview about Mobile Device Management (MDM) and Mobile Application Management (MAM) approaches. The interview will begin with an explanation and example of MDM and MAM. No prior knowledge is required to participate.

As agreed, the interview will take place *on at in, room*

I kindly ask you to read the attached document. It contains information about (personal) data processing and related matters. This document also asks for your consent to participate in the interviews. The document in in English. Should you have any question about the content of this document, you can ask them by replying to this email.

Your consent can be given:

1) By completing and signing the attached document. In this case, please send me back the signed document. This will be kept as a record for a maximum of 10 years.
2) By replying to this email from your official work email-address (). In this case, please add the following sentences to your reply.

I, the undersigned:

- **fully understand the content of the attached document "Interviews consent form_MDM-MAM"**

- **have been provided information about the research background and purposes**
- **consent to participate to the interviews for the research purposes described in that document**
- **consent to the use and processing of the information I will provide during the interviews as described in that document**
- **provide consent to the use and processing of personal data provided during the interviews as described in that document**
- **understand that I have the right to withdraw from the interview at any time without having to provide any explanation**

Full name:

Date:

Met vriendelijke groeten en tot snel,

Best regards and looking forward to meeting with you soon,

Paolo Maggioni

Paolo.maggioni@surf.nl (accessible until 07 July 2025)

Paolo.maggioni@ru.nl

+31 684300855

CONSENT FORM INTERVIEWS

Title of the research	Human-Centered Information Security: Mobile Device Management and Mobile Application Management in Higher Education
Contact details - Researcher	Paolo Maggioni

	Paolo.maggioni@ru.nl
Contact details – Radboud University Data Protection Officer, Faculty of Science	Paul Deimann privacy-fnwi@ru.nl Backup: Bjorn Bellink bjorn.bellink@ru.nl
Benefits, discomfort, and risks	Benefits: provide input for security policies that may apply to the employee him/herself No discomforts or risks
Research procedure and purposes of data processing	The role and information provided will be used to understand the interviewee's perspective on MDMs and MAMs. The interviewee will be asked for the following personal data: - Department and institution they are employed at - Age range Upon specific agreement, the interview will be recorded. Such recording will be used to transcribe the interview. This facilitates the processing of information. During the ca. 30 minutes interview a number of pre-determined questions will be asked, followed by spontaneous questions which will depend on each interview and on the answers of the interviewees.

	Participation in these interviews will help the security department of Dutch higher education institutions to account for user experience when writing MAM/MDM policies and selecting MAM/MDM tools.
Recipients of personal data	The interview recordings will only be listened to by the researcher. Pseudonymized transcripts (if any) will be made available to the university supervisor: it will be possible to opt-out of these choice at any time before June 1st 2025. Raw data and pseudonymized personal data described above will be grouped with data from all the interviews conducted and shared in a report meant for Security Departments of Dutch higher education institutions and for SURF BV. The general public might gain access to such report.
Retention period	The recordings will be deleted immediately after transcription, which will occur no later than 10 working days after the interview has taken place. All other data will be pseudonymized and stored indefinitely. The only person able to link the pseudonymized data to its natural person will be the researcher, who hereby commits to never divulge such information.
Data subject's rights Right to withdraw consent Right to withdraw data Right to lodge a complaint	The interviewee (data subject) has the right to access, rectify, erase, and restrict the use of all the data collected until June 15st 2025.

	After this date no erasure and no restriction of non-personal data will be possible. Access and rectification will always be possible. The data subject has the right to access, rectify, erase, and restrict their personal data at any time. The data subject has the right to lodge a complaint about the processing of their personal data with the Dutch Data Protection Authority: https://www.autoriteitpersoonsgegevens.nl/en

I, the undersigned:

- **fully understand the content of this document**
- **have been provided information about the research background and purposes**
- **consent to participate to the interviews for the research purposes described in this document**
- **consent to the use and processing of the information I will provide during the interviews as described in this document**
- **provide consent to the use and processing of personal data provided during the interviews as described in this document**
- **understand that I have the right to withdraw from the interview at any time without having to provide any explanation**

Full name:

Date:

Signature:

For any question, contact the researcher:

Paolo Maggioni

Radboud Universiteit

Paolo.maggioni@ru.nl

This research is conducted in collaboration with SURF, the ICT-cooperation and expertise center for Dutch education institutions.

This document has been signed by Paolo Maggioni on Friday 04 of April, 2025 at 13.21 CET.

Recording consent

At the beginning of each interview, consent of recording the interview was asked twice: before starting the recording, and after the recording was started, in order for the consent to be on record in the interview transcript.

Appendix 5 – Atlas.ti: code manager

ATLAS.ti Report

Thesis

Code groups

Report created by Paolo Maggioni on 23 May 2025

Communication errors

3 Members:

○ *lack of information*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:4 ¶ 61, Nee, nee, nee,

In Document:

4 Transcript Interview 4.docx

○ *Lack of proper communication*

Used In Documents:

2 Transcript Interview 2.docx 6 Transcript Interview 6.docx

3 Quotations:

2:5 ¶ 57, k weet niet goed Waarom dat op die manier beveiligd is dat je Alleen linkjes In de edge kan openen e…

In Document:

2 Transcript Interview 2.docx

2:7 ¶ 69, Waarom, want ik ik snap dat dat je zeg maar inlog goed moet beveiligen. Dat snap ik allemaal, Maar i…

In Document:

2 Transcript Interview 2.docx

6:6 ¶ 53, En die zei, dat wist ik dus niet. Ze hebben dus ook hele ze hebben ook trainingen rondom information…

In Document:

6 Transcript Interview 6.docx

○ *Lack of understanding*

Used In Documents:

2 Transcript Interview 2.docx 8 Transcript Interview 8.docx

4 Quotations:

2:5 ¶ 57, k weet niet goed Waarom dat op die manier beveiligd is dat je Alleen linkjes In de edge kan openen e…

In Document:

2 Transcript Interview 2.docx

2:7 ¶ 69, Waarom, want ik ik snap dat dat je zeg maar inlog goed moet beveiligen. Dat snap ik allemaal, Maar i…

In Document:

2 Transcript Interview 2.docx

8:3 ¶ 101, Most of the time they don't need to see every last document that's on the teams. For instance, we sh…

In Document:

8 Transcript Interview 8.docx

8:4 ¶ 87, But not being able to upload in like a document to an e-mail. Would be very depends. Depends on why…

In Document:

8 Transcript Interview 8.docx

Communication importance and methods

23 Members:

○ *Basic-logics usable in communication*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:12 ¶ 53, Die logica zou Iedereen moeten snappen, daar zou je op moeten kunnen bouwen in je communicatie dat.

In Document:

1 Transcript Interview 1.docx

○ *Communication*

Used In Documents:

1 Transcript Interview 1.docx 2 Transcript Interview 2.docx 3 Transcript Interview 3.docx 5 Transcript Interview 5.docx 6 Transcript Interview 6.docx 8 Transcript Interview 8.docx

20 Quotations:

1:10 ¶ 53, Een device van de Hogeschool wat wat gekocht is door de Hogeschool voor de medewerkers om daar hun w…

In Document:

1 Transcript Interview 1.docx

1:16 ¶ 58, En je hoeft het niet te blokkeren, Maar het gaat denk ik deels ook al om de bewustwording van. Dit i…

In Document:

1 Transcript Interview 1.docx

1:17 ¶ 64, us dat zou misschien dan een toevoeging zijn aan zo'n systeem. Dat zou heel goed bij passen, denk ik…

In Document:

1 Transcript Interview 1.docx

1:21 ¶ 99, et is dat is wel een een goed moment om in ieder geval het begin daarvan neer te zetten, want op het…

In Document:

1 Transcript Interview 1.docx

2:6 ¶ 61, Dus Als ik de reden zou snappen, zou ik er ook meer vrede mee hebben.

In Document:

2 Transcript Interview 2.docx

2:8 ¶ 73, Ja soms, dan zouden we laatst dat IT afdeling een soort ruim je data op campagne.

In Document:

2 Transcript Interview 2.docx

2:11 ¶ 107, Maar ik hoop bijvoorbeeld niet dat IT Mensen kunnen zien welke documenten ik of documenten kunnen op…

In Document:

2 Transcript Interview 2.docx

2:13 ¶ 123, ik zou wel dat ja dat je dat even uitgelegd krijgt. Dat is al je bent. Je haalt hem toch op. Je krij…

In Document:

2 Transcript Interview 2.docx

2:14 ¶ 143, Dan dat OK, het kan ook een een doel, waarschuwt die afdeling te zeggen. Oké, dat laptop blijft voor…

In Document:

2 Transcript Interview 2.docx

3:2 ¶ 53, huisregels. Jij krijgt nu een laptop en hoe ga je ermee om? Dat is, dat vind ik eigenlijk wel netjes…

In Document:

3 Transcript Interview 3.docx

3:3 ¶ 57, k denk gewoon aan het begin. Ja. Ja, want op een gegeven moment. Ik denk Als je Als je nog een herin…

In Document:

3 Transcript Interview 3.docx

3:4 ¶ 61, Per mail. Met een link naar de website.

In Document:

3 Transcript Interview 3.docx

3:5 ¶ 61, nieuwsbrief naar alle medewerkers dat of Misschien wordt het wel vanuit een nieuwsbrief vanuit de Un…

In Document:

3 Transcript Interview 3.docx

3:10 ¶ 205 – 207, Als je bijvoorbeeld in lees zou krijgen van één of twee applicaties die je wel mag gebruiken, maar d…

In Document:

3 Transcript Interview 3.docx

5:4 ¶ 53, Ja, ik zou daar heel graag een een hele korte, concrete, duidelijke ja. Checklist for voor willen kr…

In Document:

5 Transcript Interview 5.docx

6:5 ¶ 43, a ja zeker wel, want Het is. Ik denk ook in mijn geval, Ik weet niet of dat voor Iedereen Natuurlijk…

In Document:

6 Transcript Interview 6.docx

6:7 ¶ 57, Misschien dat je al is het maar 10 minuutjes 5 minuutjes dat je Mensen bij het opstarten van de lapt…

In Document:

6 Transcript Interview 6.docx

6:13 ¶ 165, Als je het nu zou vragen aan een aantal collega's dan en ook aan mij dan, dan zou ik het irritant vi…

In Document:

6 Transcript Interview 6.docx

6:14 ¶ 165, Waarom het belangrijk is en Waarom je het zou moeten doen, dan gebeurt het, denk ik ook zo'n beperkt…

In Document:

6 Transcript Interview 6.docx

8:18 ¶ 189, It would be nice like I think to just have a little bit of a lay of the land about like what, what's…

In Document:

8 Transcript Interview 8.docx

○ *Communication is key*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:11 ¶ 183, Ja fijn juist fijn. Ja, ja, nou nee, ik ik doe alles wat wat zeg, maar ingevoerd wordt ter beveiligi…

In Document:

4 Transcript Interview 4.docx

○ *Communication is key: we are increasing security to protect privacy and sensitive information*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:11 ¶ 183, Ja fijn juist fijn. Ja, ja, nou nee, ik ik doe alles wat wat zeg, maar ingevoerd wordt ter beveiligi…

In Document:

4 Transcript Interview 4.docx

○ *Communication via email will be read*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:14 ¶ 197, Ja behalve spammails en dat soort dingen maar maar nee, maar mails zeker van Van de Radboud uit of v…

In Document:

4 Transcript Interview 4.docx

○ *Communication: campaigns*

Used In Documents:

2 Transcript Interview 2.docx 3 Transcript Interview 3.docx

2 Quotations:

2:8 ¶ 73, Ja soms, dan zouden we laatst dat IT afdeling een soort ruim je data op campagne.

In Document:

2 Transcript Interview 2.docx

3:5 ¶ 61, nieuwsbrief naar alle medewerkers dat of Misschien wordt het wel vanuit een nieuwsbrief vanuit de Un…

In Document:

3 Transcript Interview 3.docx

○ *Communication: device is owned by the institution, it's logic security measures need to be applied*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:10 ¶ 53, Een device van de Hogeschool wat wat gekocht is door de Hogeschool voor de medewerkers om daar hun w…

In Document:

1 Transcript Interview 1.docx

○ *Communication: hey this is a company laptop*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:16 ¶ 58, En je hoeft het niet te blokkeren, Maar het gaat denk ik deels ook al om de bewustwording van. Dit i…

In Document:

1 Transcript Interview 1.docx

○ *Communication: high-level houserules at the beginning*

Used In Documents:

3 Transcript Interview 3.docx

2 Quotations:

3:2 ¶ 53, huisregels. Jij krijgt nu een laptop en hoe ga je ermee om? Dat is, dat vind ik eigenlijk wel netjes…

In Document:

3 Transcript Interview 3.docx

3:3 ¶ 57, k denk gewoon aan het begin. Ja. Ja, want op een gegeven moment. Ik denk Als je Als je nog een herin…

In Document:

3 Transcript Interview 3.docx

○ *Communication: important*

Used In Documents:

6 Transcript Interview 6.docx

2 Quotations:

6:13 ¶ 165, Als je het nu zou vragen aan een aantal collega's dan en ook aan mij dan, dan zou ik het irritant vi…

In Document:

6 Transcript Interview 6.docx

6:14 ¶ 165, Waarom het belangrijk is en Waarom je het zou moeten doen, dan gebeurt het, denk ik ook zo'n beperkt…

In Document:

6 Transcript Interview 6.docx

○ *Communication: intranet*

Used In Documents:

2 Transcript Interview 2.docx 3 Transcript Interview 3.docx

2 Quotations:

2:8 ¶ 73, Ja soms, dan zouden we laatst dat IT afdeling een soort ruim je data op campagne.

In Document:

2 Transcript Interview 2.docx

3:4 ¶ 61, Per mail. Met een link naar de website.

In Document:

3 Transcript Interview 3.docx

○ *Communication: key for user understanding and compliance*

Used In Documents:

2 Transcript Interview 2.docx

2 Quotations:

2:6 ¶ 61, Dus Als ik de reden zou snappen, zou ik er ook meer vrede mee hebben.

In Document:

2 Transcript Interview 2.docx

2:14 ¶ 143, Dan dat OK, het kan ook een een doel, waarschuwt die afdeling te zeggen. Oké, dat laptop blijft voor…

In Document:

2 Transcript Interview 2.docx

○ *Communication: mails*

Used In Documents:

2 Transcript Interview 2.docx 3 Transcript Interview 3.docx

2 Quotations:

2:8 ¶ 73, Ja soms, dan zouden we laatst dat IT afdeling een soort ruim je data op campagne.

In Document:

2 Transcript Interview 2.docx

3:4 ¶ 61, Per mail. Met een link naar de website.

In Document:

3 Transcript Interview 3.docx

○ *Communication: offer alternatives*

Used In Documents:

1 Transcript Interview 1.docx 3 Transcript Interview 3.docx 6 Transcript Interview 6.docx

3 Quotations:

1:17 ¶ 64, us dat zou misschien dan een toevoeging zijn aan zo'n systeem. Dat zou heel goed bij passen, denk ik…

In Document:

1 Transcript Interview 1.docx

3:10 ¶ 205 – 207, Als je bijvoorbeeld in lees zou krijgen van één of twee applicaties die je wel mag gebruiken, maar d…

In Document:

3 Transcript Interview 3.docx

6:5 ¶ 43, a ja zeker wel, want Het is. Ik denk ook in mijn geval, Ik weet niet of dat voor Iedereen Natuurlijk…

In Document:

6 Transcript Interview 6.docx

○ *Communication: privacy explanation, what can IT actually see*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:11 ¶ 107, Maar ik hoop bijvoorbeeld niet dat IT Mensen kunnen zien welke documenten ik of documenten kunnen op…

In Document:

2 Transcript Interview 2.docx

○ *Communication: reminders when possible*

Used In Documents:

3 Transcript Interview 3.docx

1 Quotations:

3:3 ¶ 57, k denk gewoon aan het begin. Ja. Ja, want op een gegeven moment. Ik denk Als je Als je nog een herin…

In Document:

3 Transcript Interview 3.docx

○ *Communication: short and clear communication*

Used In Documents:

5 Transcript Interview 5.docx

1 Quotations:

5:4 ¶ 53, Ja, ik zou daar heel graag een een hele korte, concrete, duidelijke ja. Checklist for voor willen kr…

In Document:

5 Transcript Interview 5.docx

○ *Communication: When users get their laptop*

Used In Documents:

1 Transcript Interview 1.docx 2 Transcript Interview 2.docx 6 Transcript Interview 6.docx

3 Quotations:

1:21 ¶ 99, et is dat is wel een een goed moment om in ieder geval het begin daarvan neer te zetten, want op het…

In Document:

1 Transcript Interview 1.docx

2:13 ¶ 123, ik zou wel dat ja dat je dat even uitgelegd krijgt. Dat is al je bent. Je haalt hem toch op. Je krij…

In Document:

2 Transcript Interview 2.docx

6:7 ¶ 57, Misschien dat je al is het maar 10 minuutjes 5 minuutjes dat je Mensen bij het opstarten van de lapt…

In Document:

6 Transcript Interview 6.docx

○ *Communication: would benefit understanding*

Used In Documents:

8 Transcript Interview 8.docx

1 Quotations:

8:18 ¶ 189, It would be nice like I think to just have a little bit of a lay of the land about like what, what's…

In Document:

8 Transcript Interview 8.docx

○ *If the goal is clear and clearly communicated, the compliance increases*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:12 ¶ 187, Dus te voorkomen dat het gehackt wordt of wat dan ook hè? Dat er een bepaalde beveiligingsstructuur…

In Document:

4 Transcript Interview 4.docx

○ *Responsibility: private use allowed, but users are not allowed to do everything*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:12 ¶ 115, Je krijgt dan een overeenkomst ofzo en dan staat iets van je mag een privégebruik, maar je mag een b…

In Document:

2 Transcript Interview 2.docx

○ *When changin jobs, there are tools that you previously used that you still would like to use*

Used In Documents:

6 Transcript Interview 6.docx

1 Quotations:

6:3 ¶ 39, Als je dan nieuw komt bij bij een werkgever en Omdat je dan voor het eerst hebt is gewoon een volled…

In Document:

6 Transcript Interview 6.docx

○ *Yearly communication*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:13 ¶ 193, Zeg maar eens per jaar lijkt me logisch

In Document:

4 Transcript Interview 4.docx

Opinion on Notifications

4 Members:

○ *Notification*

Used In Documents:

4 Transcript Interview 4.docx 8 Transcript Interview 8.docx

2 Quotations:

4:2 ¶ 23, Er zijn wel Als je bijvoorbeeld naar bepaalde websites gaat meer privé, zeg Maar dat dan, dan kan he…

In Document:

4 Transcript Interview 4.docx

8:14 ¶ 235 – 239, at least you get a message saying, hey, watch out. This is a confidential document you're exporting…

In Document:

8 Transcript Interview 8.docx

○ *Notification when user perfom action for which we have a non-shadow IT solution*

Used In Documents:

1 Transcript Interview 1.docx 8 Transcript Interview 8.docx

2 Quotations:

1:14 ¶ 58, Pop-up, of weet ik veel. Een melding zou kunnen zijn dat in dat proces eventjes.

In Document:

1 Transcript Interview 1.docx

8:1 ¶ 73, But if I did get a pop up and they say oh, here's it, I don't mind as long as you know. It. Can redi…

In Document:

8 Transcript Interview 8.docx

○ *Notification: this is a dangerous website*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:2 ¶ 23, Er zijn wel Als je bijvoorbeeld naar bepaalde websites gaat meer privé, zeg Maar dat dan, dan kan he…

In Document:

4 Transcript Interview 4.docx

○ *Notification: you are doing something with a document labelled confidential*

Used In Documents:

8 Transcript Interview 8.docx

1 Quotations:

8:14 ¶ 235 – 239, at least you get a message saying, hey, watch out. This is a confidential document you're exporting…

In Document:

8 Transcript Interview 8.docx

Opinions MAM: email forwarding

5 Members:

○ *Acceptance: no automatic forwarding*

Used In Documents:

4 Transcript Interview 4.docx 8 Transcript Interview 8.docx

3 Quotations:

4:1 ¶ 97, Nee schoot niet erg, vind ik op zich. Ik gebruik nu bijna ook eigenlijk privé altijd mijn mijn roubo…

In Document:

4 Transcript Interview 4.docx

8:10 ¶ 145, And the person outside the organization is fine. That's fair thing like because an e-mail is coming…

In Document:

8 Transcript Interview 8.docx

8:16 ¶ 177, Fair enough. I think it's automatic. Yeah. Then I understand that it it doesn't.

In Document:

8 Transcript Interview 8.docx

○ *Bloc: email forwarding, not accepted*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:17 ¶ 221, Sommige organisaties zitten gewoon dicht op elkaar en dat dat maakt soms dan maken deze regels het s…

In Document:

2 Transcript Interview 2.docx

○ *Block: MAM, limitations in forwarding to private email*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:4 ¶ 49, Of je kan het niet makkelijk doorsturen naar buiten de UU.

In Document:

2 Transcript Interview 2.docx

○ *Exceptions to block of automatic forwarding of emails, from specific people*

Used In Documents:

7 Transcript Interview 7.docx

1 Quotations:

7:15 ¶ 123, that that was my auto forwarding setup before the university blocked it and it I would have been fin…

In Document:

7 Transcript Interview 7.docx

○ *Job involves emailing people who use gmail*

Used In Documents:

6 Transcript Interview 6.docx 8 Transcript Interview 8.docx

3 Quotations:

6:11 ¶ 123, Universiteit Utrecht samenwerken in een Google document om iets van een draft te maken voor een pres…

In Document:

6 Transcript Interview 6.docx

8:6 ¶ 111, for work I do e-mail people with private e-mail addresses like other external partners like one of t…

In Document:

8 Transcript Interview 8.docx

8:8 ¶ 117, ho would only use their. Gmail ID to respond and they were far quicker with it because their work e-…

In Document:

8 Transcript Interview 8.docx

Opinions MAM: separation between private and work on a device

8 Members:

○ *2 accounts on the same laptop*

Used In Documents:

1 Transcript Interview 1.docx 2 Transcript Interview 2.docx 5 Transcript Interview 5.docx

4 Quotations:

1:3 ¶ 20, Ik heb nu in mijn browser twee profielen zitten ook een privéprofiel dat ik zo nu en dan opstart en…

In Document:

1 Transcript Interview 1.docx

2:1 ¶ 33, Ik heb een account gehad of op de laptop, maar ik sla ook documenten privé gewoon wel op, maar in ee…

In Document:

2 Transcript Interview 2.docx

2:2 ¶ 33, En ja op mijn laptop staat gewoon Outlook en teams en zo van Van de universiteit en voor privé log i…

In Document:

2 Transcript Interview 2.docx

5:1 ¶ 17, Ja, Ik heb op dit moment letterlijk een wit wolkje en een blauw wolkje. De blauwe wolkje is OneDrive…

In Document:

5 Transcript Interview 5.docx

○ *Acceptance: not being able to transfer data from business to private account*

Used In Documents:

5 Transcript Interview 5.docx

1 Quotations:

5:5 ¶ 79, Eigenlijk, eigenlijk wil ik daar naartoe. Ik. Ik merk dat ik van oudsher de neiging heb om bestanden…

In Document:

5 Transcript Interview 5.docx

○ *Acceptance: not possible to copy text from work to private account or random notebooks*

Used In Documents:

5 Transcript Interview 5.docx

1 Quotations:

5:7 ¶ 235, Ik denk dat dat weer weer een stap richting betere data beveiliging is heel praktisch gezien

In Document:

5 Transcript Interview 5.docx

○ *Acceptance: sensitive data on a separate network with extra password*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:9 ¶ 137, Die staat al vaak geblokkeerd hier, de OWC schijf en Dat is een aparte schijf.

In Document:

4 Transcript Interview 4.docx

○ *Acceptance: separation between private and work environments*

Used In Documents:

4 Transcript Interview 4.docx 6 Transcript Interview 6.docx

3 Quotations:

4:8 ¶ 133, Is prima zo dat gescheiden is ja

In Document:

4 Transcript Interview 4.docx

6:10 ¶ 105 – 107, Je telefoon bijvoorbeeld niks mag kopiëren wanneer wanneer de omgeving naar die persoonlijke omgevin…

In Document:

6 Transcript Interview 6.docx

6:15 ¶ 193, anuit mijn persoonlijke account gezien mag dat echt gescheiden zijn, ja. Ja, ja, Dat is een ja en ik…

In Document:

6 Transcript Interview 6.docx

○ *Acceptance: separation of networks*

Used In Documents:

7 Transcript Interview 7.docx

2 Quotations:

7:8 ¶ 43 – 45, Would it work for you to use this laptop in an environment that separated from the overall network o…

In Document:

7 Transcript Interview 7.docx

7:9 ¶ 49, So there are certain things at the university that I can only access if I'm connected to the the net…

In Document:

7 Transcript Interview 7.docx

○ *Block: MAM on BYOD phone, not possible to copy from the uni environment to personal environment*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:3 ¶ 41, Dit is mijn eigen mobiel, maar daar heb ik wel mijn werkmail op en daarvan mag ik mee eens kopiëren…

In Document:

2 Transcript Interview 2.docx

○ *Limited access to university data for unmanaged laptops*

Used In Documents:

7 Transcript Interview 7.docx

1 Quotations:

7:8 ¶ 43 – 45, Would it work for you to use this laptop in an environment that separated from the overall network o…

In Document:

7 Transcript Interview 7.docx

Opinions MAM: sharing documents

2 Members:

○ *Acceptance: not possible to copy text from work to private account or random notebooks*

Used In Documents:

5 Transcript Interview 5.docx

1 Quotations:

5:7 ¶ 235, Ik denk dat dat weer weer een stap richting betere data beveiliging is heel praktisch gezien

In Document:

5 Transcript Interview 5.docx

○ *Acceptance: sharing links instead of emails attachments*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:18 ¶ 221, Ik stuur het liefst gewoon documenten, een linkje naar een document op OneDrive of op sherpoint en d…

In Document:

2 Transcript Interview 2.docx

Opinions on MAM: access controls

4 Members:

○ *Acceptance: not possible to copy text from work to private account or random notebooks*

Used In Documents:

5 Transcript Interview 5.docx

1 Quotations:

5:7 ¶ 235, Ik denk dat dat weer weer een stap richting betere data beveiliging is heel praktisch gezien

In Document:

5 Transcript Interview 5.docx

○ *Acceptance: sensitive data on a separate network with extra password*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:9 ¶ 137, Die staat al vaak geblokkeerd hier, de OWC schijf en Dat is een aparte schijf.

In Document:

4 Transcript Interview 4.docx

○ *Extra code for account*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:22 ¶ 134, k denk dat dat een passendere oplossing zou zijn om de toegang tot de app, of eigenlijk tot het acco…

In Document:

1 Transcript Interview 1.docx

○ *Rejection: extra code for outlook*

Used In Documents:

8 Transcript Interview 8.docx

2 Quotations:

8:13 ¶ 225, if I had to like double double authenticate all the time, it would just drive me nuts.

In Document:

8 Transcript Interview 8.docx

8:19 ¶ 225, I'd really be annoyed. It would be really annoying because I I would be annoyed because I'm like I h…

In Document:

8 Transcript Interview 8.docx

Opinions on MAM: information labeling

7 Members:

○ *Acceptance: document classification*

Used In Documents:

2 Transcript Interview 2.docx 3 Transcript Interview 3.docx

2 Quotations:

2:19 ¶ 237, Ik zou het niet zeggen dat het voor alle documenten moet gelden, maar zeker met ja. Studentengegeven…

In Document:

2 Transcript Interview 2.docx

3:7 ¶ 138 – 145, peaker 1 Wat zijn je vrienden als er In de classificatie zou zijn? Van waar een document waar e mail…

In Document:

3 Transcript Interview 3.docx

○ *Acceptance: labeling*

Used In Documents:

4 Transcript Interview 4.docx 7 Transcript Interview 7.docx 8 Transcript Interview 8.docx

4 Quotations:

4:10 ¶ 169 – 175, En soms zeg ik van joh, Iedereen mag dit lezen, dat vind ik allemaal prima. En, want Daarom doen wij…

In Document:

4 Transcript Interview 4.docx

7:12 ¶ 89, think when I taught you guys, you guys couldn't download my slides. I don't remember if that, I don'…

In Document:

7 Transcript Interview 7.docx

7:14 ¶ 102 – 115, Speaker 1 OK. Yeah. And kind of the the the similar question, So what if for example, you were allow…

In Document:

7 Transcript Interview 7.docx

8:15 ¶ 245, actually do label most of my work. I'm a big labeler. I guess in that sense. So I'm a big. It keeps…

In Document:

8 Transcript Interview 8.docx

○ *Extra security for confidential documents*

Used In Documents:

6 Transcript Interview 6.docx

1 Quotations:

6:12 ¶ 153 – 155, Ja, Maar dat Ik denk dat het Misschien wel een beetje hetzelfde geldt als wat. Net. Voor dat een soo…

In Document:

6 Transcript Interview 6.docx

○ *I will remember to change the label*

Used In Documents:

7 Transcript Interview 7.docx

1 Quotations:

7:17 ¶ 132 – 135, Speaker 1 Are you confident that you would remember to change the label then if we actually do send…

In Document:

7 Transcript Interview 7.docx

○ *Labeling increases students privacy*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:10 ¶ 169 – 175, En soms zeg ik van joh, Iedereen mag dit lezen, dat vind ik allemaal prima. En, want Daarom doen wij…

In Document:

4 Transcript Interview 4.docx

○ *labelling can help*

Used In Documents:

4 Transcript Interview 4.docx 6 Transcript Interview 6.docx 8 Transcript Interview 8.docx

3 Quotations:

4:10 ¶ 169 – 175, En soms zeg ik van joh, Iedereen mag dit lezen, dat vind ik allemaal prima. En, want Daarom doen wij…

In Document:

4 Transcript Interview 4.docx

6:13 ¶ 165, Als je het nu zou vragen aan een aantal collega's dan en ook aan mij dan, dan zou ik het irritant vi…

In Document:

6 Transcript Interview 6.docx

8:7 ¶ 111, f it's confidential then then I would ask for an official e-mail ID and I just keep on right

In Document:

8 Transcript Interview 8.docx

○ *Rejection: labeling*

Used In Documents:

7 Transcript Interview 7.docx

1 Quotations:

7:16 ¶ 129 – 131, But and so of course all this labeling takes one effort from the user side, which is actually doing…

In Document:

7 Transcript Interview 7.docx

Opinions on MDM: access controls

7 Members:

○ *Acceptance: loger phone access code*

Used In Documents:

2 Transcript Interview 2.docx 3 Transcript Interview 3.docx 4 Transcript Interview 4.docx 6 Transcript Interview 6.docx

5 Quotations:

2:16 ¶ 183, Ja ja. Ja ja. Ja, ik zou het wel accepteren. Ik zou het een beetje bemoeiend is vinden, Maar ik zou…

In Document:

2 Transcript Interview 2.docx

3:8 ¶ 155 – 157, En je werk email. Wordt als bijvoorbeeld helemaal aanreken zou komen dat om jouw universiteit accoun…

In Document:

3 Transcript Interview 3.docx

4:6 ¶ 81, Ja. Ja ja op zich als dat nodig is zeker hier heb ik nu dubbelzinn, dus Ik heb hier naar mijn privé…

In Document:

4 Transcript Interview 4.docx

4:7 ¶ 109, Je hebt nu ook vaak hè? Bij banken en bij dingen moet ik ook continueren. Je hebt sowieso. Heb je di…

In Document:

4 Transcript Interview 4.docx

6:9 ¶ 74 – 81, Speaker 1 Een extra pincode. Speaker 2 Ja dus met je, Ik heb mijn pincode gewoon voor mijn telefoon…

In Document:

6 Transcript Interview 6.docx

○ *Acceptance: separation of networks*

Used In Documents:

7 Transcript Interview 7.docx

2 Quotations:

7:8 ¶ 43 – 45, Would it work for you to use this laptop in an environment that separated from the overall network o…

In Document:

7 Transcript Interview 7.docx

7:9 ¶ 49, So there are certain things at the university that I can only access if I'm connected to the the net…

In Document:

7 Transcript Interview 7.docx

○ *Longer code would be annoying but I would still use it*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:24 ¶ 125, a, kan maar goed, irritant is niet altijd een reden om iets niet te doen hè? Maar dat zou mijn telef…

In Document:

1 Transcript Interview 1.docx

○ *No complicated code for phone*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:22 ¶ 134, k denk dat dat een passendere oplossing zou zijn om de toegang tot de app, of eigenlijk tot het acco…

In Document:

1 Transcript Interview 1.docx

○ *Rejection: MDM on BYOD*

Used In Documents:

3 Transcript Interview 3.docx

1 Quotations:

3:9 ¶ 176 – 179, Speaker 1 Zet de vraag dus je bepaalde applicaties niet downloaden op je privételefoon. Speaker 2 Da…

In Document:

3 Transcript Interview 3.docx

○ *Rejection: phone code*

Used In Documents:

7 Transcript Interview 7.docx 8 Transcript Interview 8.docx

2 Quotations:

7:13 ¶ 101, Yeah, if you don't want to let me do that, then give me another phone. Right. So, like, if the unive…

In Document:

7 Transcript Interview 7.docx

8:12 ¶ 215 – 217, And what if what if you are? You know you're putting an account on on your personal phone. So what i…

In Document:

8 Transcript Interview 8.docx

○ *Total access to the laptop*

Used In Documents:

7 Transcript Interview 7.docx

1 Quotations:

7:2 ¶ 21, Most of the people here at Leox have self managed machines just because we need the ability to open…

In Document:

7 Transcript Interview 7.docx

Opinions on Whitelists for software and applications

6 Members:

○ *Acceptance: use only designated tools*

Used In Documents:

5 Transcript Interview 5.docx

1 Quotations:

5:3 ¶ 39, Ja ik, ik hou inderdaad wel van, Ik ben Maar dat komt Omdat ik aan de andere kant van Van het spiege…

In Document:

5 Transcript Interview 5.docx

○ *Common application*

Used In Documents:

1 Transcript Interview 1.docx 6 Transcript Interview 6.docx

2 Quotations:

1:2 ¶ 20, WhatsApp er een tijdje wel opstaan als applicatie voor voor privé communicatie

In Document:

1 Transcript Interview 1.docx

6:1 ¶ 31, Er zijn gewoon een aantal specifieke applicaties die ik dan graag gebruiken. Ze noodk, het zijn echt…

In Document:

6 Transcript Interview 6.docx

○ *Long approval for applications that could be in a whitelist*

Used In Documents:

3 Transcript Interview 3.docx

1 Quotations:

3:1 ¶ 29, Ik heb bijvoorbeeld Adobe pro wilde ik en dat daar is dan weer speciaal toestemming voor nodig van d…

In Document:

3 Transcript Interview 3.docx

○ *Whitelist*

Used In Documents:

2 Transcript Interview 2.docx 5 Transcript Interview 5.docx

2 Quotations:

2:9 ¶ 85, ooladvisor, soms mis het. We hebben een tooladvisor, dus als je dan kan je zoeken. Welke ook welke a…

In Document:

2 Transcript Interview 2.docx

5:4 ¶ 53, Ja, ik zou daar heel graag een een hele korte, concrete, duidelijke ja. Checklist for voor willen kr…

In Document:

5 Transcript Interview 5.docx

○ *Whitelist for application means many more requests*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:8 ¶ 43, whitelist van applicaties die geïnstalleerd kunnen worden of dat je daar een verzoek voor kan neerle…

In Document:

1 Transcript Interview 1.docx

○ *Whitelist: advicing tool*

Used In Documents:

2 Transcript Interview 2.docx 5 Transcript Interview 5.docx

2 Quotations:

2:9 ¶ 85, ooladvisor, soms mis het. We hebben een tooladvisor, dus als je dan kan je zoeken. Welke ook welke a…

In Document:

2 Transcript Interview 2.docx

5:4 ¶ 53, Ja, ik zou daar heel graag een een hele korte, concrete, duidelijke ja. Checklist for voor willen kr…

In Document:

5 Transcript Interview 5.docx

Privacy

4 Members:

○ *Acceptance: software that scans for malwares*

Used In Documents:

3 Transcript Interview 3.docx

1 Quotations:

3:6 ¶ 77, Zeker ik, ik werk veel voor het instituut of security in het Global Affaires. Dus ik ik Google regel…

In Document:

3 Transcript Interview 3.docx

○ *Communication: privacy explanation, what can IT actually see*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:11 ¶ 107, Maar ik hoop bijvoorbeeld niet dat IT Mensen kunnen zien welke documenten ik of documenten kunnen op…

In Document:

2 Transcript Interview 2.docx

○ *Labeling increases students privacy*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:10 ¶ 169 – 175, En soms zeg ik van joh, Iedereen mag dit lezen, dat vind ik allemaal prima. En, want Daarom doen wij…

In Document:

4 Transcript Interview 4.docx

○ *Privacy, not a big issue*

Used In Documents:

3 Transcript Interview 3.docx 4 Transcript Interview 4.docx 7 Transcript Interview 7.docx

3 Quotations:

3:14 ¶ 73, Ja, dat vind ik ja, Ik heb niks te verbergen dat vind. Wel OK. Ja ja dat Ik heb er niet zoveel probl…

In Document:

3 Transcript Interview 3.docx

4:5 ¶ 65, k vraag me wel eens af, weet je wel, in hoeverre kunnen zij zien wat ik? Wat ik doe, maar ja, Ik heb…

In Document:

4 Transcript Interview 4.docx

7:18 ¶ 57, Ohh, I'm confident they can't see what? I'm doing on my laptop. Yes. So yeah.

In Document:

7 Transcript Interview 7.docx

Prompt change with notification: offer alternatives

6 Members:

○ *Acceptance: notification prompting change or update*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:3 ¶ 27, Dat is prima ja liever wel dan niet. Ik kijk ook regelmatig, soms krijg je ook van. Zo'n security up…

In Document:

4 Transcript Interview 4.docx

○ *Communication: offer alternatives*

Used In Documents:

1 Transcript Interview 1.docx 3 Transcript Interview 3.docx 6 Transcript Interview 6.docx

3 Quotations:

1:17 ¶ 64, us dat zou misschien dan een toevoeging zijn aan zo'n systeem. Dat zou heel goed bij passen, denk ik…

In Document:

1 Transcript Interview 1.docx

3:10 ¶ 205 – 207, Als je bijvoorbeeld in lees zou krijgen van één of twee applicaties die je wel mag gebruiken, maar d…

In Document:

3 Transcript Interview 3.docx

6:5 ¶ 43, a ja zeker wel, want Het is. Ik denk ook in mijn geval, Ik weet niet of dat voor Iedereen Natuurlijk…

In Document:

6 Transcript Interview 6.docx

○ *Notification*

Used In Documents:

4 Transcript Interview 4.docx 8 Transcript Interview 8.docx

2 Quotations:

4:2 ¶ 23, Er zijn wel Als je bijvoorbeeld naar bepaalde websites gaat meer privé, zeg Maar dat dan, dan kan he…

In Document:

4 Transcript Interview 4.docx

8:14 ¶ 235 – 239, at least you get a message saying, hey, watch out. This is a confidential document you're exporting…

In Document:

8 Transcript Interview 8.docx

○ *Notification when user perfom action for which we have a non-shadow IT solution*

Used In Documents:

1 Transcript Interview 1.docx 8 Transcript Interview 8.docx

2 Quotations:

1:14 ¶ 58, Pop-up, of weet ik veel. Een melding zou kunnen zijn dat in dat proces eventjes.

In Document:

1 Transcript Interview 1.docx

8:1 ¶ 73, But if I did get a pop up and they say oh, here's it, I don't mind as long as you know. It. Can redi…

In Document:

8 Transcript Interview 8.docx

○ *Notification: this is a dangerous website*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:2 ¶ 23, Er zijn wel Als je bijvoorbeeld naar bepaalde websites gaat meer privé, zeg Maar dat dan, dan kan he…

In Document:

4 Transcript Interview 4.docx

○ *Notification: you are doing something with a document labelled confidential*

Used In Documents:

8 Transcript Interview 8.docx

1 Quotations:

8:14 ¶ 235 – 239, at least you get a message saying, hey, watch out. This is a confidential document you're exporting…

In Document:

8 Transcript Interview 8.docx

Proof: users may turn to shadow-IT if they really need something, security is too strict, and communication is not effective

22 Members:

○ *Even confidential files need to be shared*

Used In Documents:

8 Transcript Interview 8.docx

1 Quotations:

8:2 ¶ 87, because even if it's confidential, you might be because there have been many times where my colleagu…

In Document:

8 Transcript Interview 8.docx

○ *If it's too hard, users will not use it*

Used In Documents:

7 Transcript Interview 7.docx

1 Quotations:

7:13 ¶ 101, Yeah, if you don't want to let me do that, then give me another phone. Right. So, like, if the unive…

In Document:

7 Transcript Interview 7.docx

○ *If people aren't able to do something they will turn to shadow IT*

Used In Documents:

1 Transcript Interview 1.docx 2 Transcript Interview 2.docx 7 Transcript Interview 7.docx 8 Transcript Interview 8.docx

4 Quotations:

1:20 ¶ 84, ou ik zelf al gauw bijvoorbeeld mijn privé laptop pakken om zoiets te doen, weet je wel om door om d…

In Document:

1 Transcript Interview 1.docx

2:15 ¶ 145, Als ik daardoor bepaalde dingen moet gebruiken die Omdat het een UU lapt op is, dan kan ik ook niet…

In Document:

2 Transcript Interview 2.docx

7:6 ¶ 37, nd if they said. Know now what I have to use my personal machine to do work

In Document:

7 Transcript Interview 7.docx

8:17 ¶ 181, The only other time I would assume that like, oh, please, I would like emails in a different e-mail…

In Document:

8 Transcript Interview 8.docx

○ *If the goal is clear and clearly communicated, the compliance increases*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:12 ¶ 187, Dus te voorkomen dat het gehackt wordt of wat dan ook hè? Dat er een bepaalde beveiligingsstructuur…

In Document:

4 Transcript Interview 4.docx

○ *Job involves emailing people who use gmail*

Used In Documents:

6 Transcript Interview 6.docx 8 Transcript Interview 8.docx

3 Quotations:

6:11 ¶ 123, Universiteit Utrecht samenwerken in een Google document om iets van een draft te maken voor een pres…

In Document:

6 Transcript Interview 6.docx

8:6 ¶ 111, for work I do e-mail people with private e-mail addresses like other external partners like one of t…

In Document:

8 Transcript Interview 8.docx

8:8 ¶ 117, ho would only use their. Gmail ID to respond and they were far quicker with it because their work e-…

In Document:

8 Transcript Interview 8.docx

○ *lack of information*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:4 ¶ 61, Nee, nee, nee,

In Document:

4 Transcript Interview 4.docx

○ *Lack of proper communication*

Used In Documents:

2 Transcript Interview 2.docx 6 Transcript Interview 6.docx

3 Quotations:

2:5 ¶ 57, k weet niet goed Waarom dat op die manier beveiligd is dat je Alleen linkjes In de edge kan openen e…

In Document:

2 Transcript Interview 2.docx

2:7 ¶ 69, Waarom, want ik ik snap dat dat je zeg maar inlog goed moet beveiligen. Dat snap ik allemaal, Maar i…

In Document:

2 Transcript Interview 2.docx

6:6 ¶ 53, En die zei, dat wist ik dus niet. Ze hebben dus ook hele ze hebben ook trainingen rondom information…

In Document:

6 Transcript Interview 6.docx

○ *Lack of understanding*

Used In Documents:

2 Transcript Interview 2.docx 8 Transcript Interview 8.docx

4 Quotations:

2:5 ¶ 57, k weet niet goed Waarom dat op die manier beveiligd is dat je Alleen linkjes In de edge kan openen e…

In Document:

2 Transcript Interview 2.docx

2:7 ¶ 69, Waarom, want ik ik snap dat dat je zeg maar inlog goed moet beveiligen. Dat snap ik allemaal, Maar i…

In Document:

2 Transcript Interview 2.docx

8:3 ¶ 101, Most of the time they don't need to see every last document that's on the teams. For instance, we sh…

In Document:

8 Transcript Interview 8.docx

8:4 ¶ 87, But not being able to upload in like a document to an e-mail. Would be very depends. Depends on why…

In Document:

8 Transcript Interview 8.docx

○ *Limit not too high*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:6 ¶ 43, Voor mij is het eigenlijk handig als mensen een drempel ervaren die ze nu niet meer hebben, maar is…

In Document:

1 Transcript Interview 1.docx

○ *Long approval for applications that could be in a whitelist*

Used In Documents:

3 Transcript Interview 3.docx

1 Quotations:

3:1 ¶ 29, Ik heb bijvoorbeeld Adobe pro wilde ik en dat daar is dan weer speciaal toestemming voor nodig van d…

In Document:

3 Transcript Interview 3.docx

○ *Old students use gmail*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:16 ¶ 253, Nou maar ook studenten die vaak zeg maar mij mailen via hun gmail of hotmail of of live.nl of whatev…

In Document:

4 Transcript Interview 4.docx

○ *People should have local admin rights*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:9 ¶ 46 – 48, a dus dat via een bepaalde applicatie die op de laptop staat daarmee de aanvraag om een soort van lo…

In Document:

1 Transcript Interview 1.docx

○ *People sometimes need things immediately*

Used In Documents:

1 Transcript Interview 1.docx

2 Quotations:

1:18 ¶ 69, dat ga je doen op het moment dat je dat nodig hebt

In Document:

1 Transcript Interview 1.docx

1:19 ¶ 79, Nou dat dat merk je pas op dat moment en op vrijdagmiddag is er niemand te bereiken natuurlijk. Dan…

In Document:

1 Transcript Interview 1.docx

○ *Role matters*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:10 ¶ 101, Mensen die bijvoorbeeld studenten die hun data kunnen zien op op een zo ja op op zo'n document en no…

In Document:

2 Transcript Interview 2.docx

○ *Software request process is slow*

Used In Documents:

6 Transcript Interview 6.docx

1 Quotations:

6:2 ¶ 35, Ja, dat gaat naar mij, maar dan denk ik dat het voor Iedereen geldt. Gaat best traag je wilt Natuurl…

In Document:

6 Transcript Interview 6.docx

○ *Sometimes need to work offline*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:23 ¶ 113, Stel dat je In de trein zit en je. Wilt even wat? Maar Je kunt het dan niet downloaden en Je kunt di…

In Document:

1 Transcript Interview 1.docx

○ *Sometimes user need to forward email to their own email*

Used In Documents:

8 Transcript Interview 8.docx

1 Quotations:

8:9 ¶ 121, To myself, to my private e-mail, so I can work on it. Maybe I'm I'm on holiday. I'm on vacation. I j…

In Document:

8 Transcript Interview 8.docx

○ *There has to be a limit, but it needs to be high enough*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:5 ¶ 38, n er zijn altijd wel dingen die je graag wilt installeren maar als de drempel maar hoog genoeg is o…

In Document:

1 Transcript Interview 1.docx

○ *Type of job*

Used In Documents:

3 Transcript Interview 3.docx 7 Transcript Interview 7.docx 8 Transcript Interview 8.docx

3 Quotations:

3:12 ¶ 211, Wat is je functie wat heb? Nodig ja. Dat Als je het een keer nodig hebt. Je het dan aan moet vragen?

In Document:

3 Transcript Interview 3.docx

7:3 ¶ 25, I would find no restrictions acceptable. I mean, like I said right there, there's. I I basically in…

In Document:

7 Transcript Interview 7.docx

8:5 ¶ 111, my job once you know like it's not that I do some intensely confidential work that requires

In Document:

8 Transcript Interview 8.docx

○ *Type of job requires access*

Used In Documents:

7 Transcript Interview 7.docx

2 Quotations:

7:3 ¶ 25, I would find no restrictions acceptable. I mean, like I said right there, there's. I I basically in…

In Document:

7 Transcript Interview 7.docx

7:4 ¶ 33, I'm working on, you know, 10 different things at a time. If if a project, if I have to wait two week…

In Document:

7 Transcript Interview 7.docx

○ *When changin jobs, there are tools that you previously used that you still would like to use*

Used In Documents:

6 Transcript Interview 6.docx

1 Quotations:

6:3 ¶ 39, Als je dan nieuw komt bij bij een werkgever en Omdat je dan voor het eerst hebt is gewoon een volled…

In Document:

6 Transcript Interview 6.docx

○ *Work account also for private purposes*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:1 ¶ 97, Nee schoot niet erg, vind ik op zich. Ik gebruik nu bijna ook eigenlijk privé altijd mijn mijn roubo…

In Document:

4 Transcript Interview 4.docx

Request process

9 Members:

○ *Acceptance: at the start of a project think of which tools you need*

Used In Documents:

5 Transcript Interview 5.docx

1 Quotations:

5:6 ¶ 129, Ja, als dat mijn dat kan, mijn werkwijze worden. Ik bedoel, ik moet tentamens die gegeven worden. Mo…

In Document:

5 Transcript Interview 5.docx

○ *Long approval for applications that could be in a whitelist*

Used In Documents:

3 Transcript Interview 3.docx

1 Quotations:

3:1 ¶ 29, Ik heb bijvoorbeeld Adobe pro wilde ik en dat daar is dan weer speciaal toestemming voor nodig van d…

In Document:

3 Transcript Interview 3.docx

○ *People need to ask for permission for software*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:7 ¶ 43, Of het eventjes na te vragen bij mij of bij iemand anders dat is voor mij al een drempel die volgen…

In Document:

1 Transcript Interview 1.docx

○ *People should have local admin rights*

Used In Documents:

1 Transcript Interview 1.docx

1 Quotations:

1:9 ¶ 46 – 48, a dus dat via een bepaalde applicatie die op de laptop staat daarmee de aanvraag om een soort van lo…

In Document:

1 Transcript Interview 1.docx

○ *Request*

Used In Documents:

3 Transcript Interview 3.docx 6 Transcript Interview 6.docx

2 Quotations:

3:11 ¶ 209 – 211, Ja en zijn prima vinden bijvoorbeeld Als je een project moet starten om even gewoon na te denken ik…

In Document:

3 Transcript Interview 3.docx

6:4 ¶ 39, Maar ik kan voor een project ik. Dat het. Is om er over na te denken inderdaad van tevoren dat je da…

In Document:

6 Transcript Interview 6.docx

○ *Request: before starting a project*

Used In Documents:

3 Transcript Interview 3.docx 6 Transcript Interview 6.docx

2 Quotations:

3:11 ¶ 209 – 211, Ja en zijn prima vinden bijvoorbeeld Als je een project moet starten om even gewoon na te denken ik…

In Document:

3 Transcript Interview 3.docx

6:4 ¶ 39, Maar ik kan voor een project ik. Dat het. Is om er over na te denken inderdaad van tevoren dat je da…

In Document:

6 Transcript Interview 6.docx

○ *Role matters*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:10 ¶ 101, Mensen die bijvoorbeeld studenten die hun data kunnen zien op op een zo ja op op zo'n document en no…

In Document:

2 Transcript Interview 2.docx

○ *Software request process is slow*

Used In Documents:

6 Transcript Interview 6.docx

1 Quotations:

6:2 ¶ 35, Ja, dat gaat naar mij, maar dan denk ik dat het voor Iedereen geldt. Gaat best traag je wilt Natuurl…

In Document:

6 Transcript Interview 6.docx

○ *Type of job requires access*

Used In Documents:

7 Transcript Interview 7.docx

2 Quotations:

7:3 ¶ 25, I would find no restrictions acceptable. I mean, like I said right there, there's. I I basically in…

In Document:

7 Transcript Interview 7.docx

7:4 ¶ 33, I'm working on, you know, 10 different things at a time. If if a project, if I have to wait two week…

In Document:

7 Transcript Interview 7.docx

Risk Acceptance and consequences

7 Members:

○ *Consequences*

Used In Documents:

7 Transcript Interview 7.docx

1 Quotations:

7:11 ¶ 81, t's like massive data leak, then maybe like the individual employee loses. The. Kind of. I don't wan…

In Document:

7 Transcript Interview 7.docx

○ *Responsibility*

Used In Documents:

2 Transcript Interview 2.docx 7 Transcript Interview 7.docx

3 Quotations:

2:12 ¶ 115, Je krijgt dan een overeenkomst ofzo en dan staat iets van je mag een privégebruik, maar je mag een b…

In Document:

2 Transcript Interview 2.docx

7:5 ¶ 33, We do research, so if we break the machine, we can fix it. That's actually, that's one of the distin…

In Document:

7 Transcript Interview 7.docx

7:7 ¶ 41, f I install something, if I install a virus and I lose a bunch of data, I'm responsible for getting…

In Document:

7 Transcript Interview 7.docx

○ *Responsibility: private use allowed, but users are not allowed to do everything*

Used In Documents:

2 Transcript Interview 2.docx

1 Quotations:

2:12 ¶ 115, Je krijgt dan een overeenkomst ofzo en dan staat iets van je mag een privégebruik, maar je mag een b…

In Document:

2 Transcript Interview 2.docx

○ *Responsibility: the owner of unmanaged laptops has the responsibility to fix it*

Used In Documents:

7 Transcript Interview 7.docx

2 Quotations:

7:5 ¶ 33, We do research, so if we break the machine, we can fix it. That's actually, that's one of the distin…

In Document:

7 Transcript Interview 7.docx

7:7 ¶ 41, f I install something, if I install a virus and I lose a bunch of data, I'm responsible for getting…

In Document:

7 Transcript Interview 7.docx

○ *risk acceptance*

Used In Documents:

4 Transcript Interview 4.docx 7 Transcript Interview 7.docx

2 Quotations:

4:15 ¶ 204 – 207, Speaker 2 Ja. Ja. Ja ja ja. Speaker 2 Wil graag ja nee, zeker en en het lijkt me ook logisch In de h…

In Document:

4 Transcript Interview 4.docx

7:10 ¶ 73, I think that's a fair trade off, right? I I need the access in order to do my job. But yeah, it's a…

In Document:

7 Transcript Interview 7.docx

○ *Risk acceptance document needs to be concise*

Used In Documents:

8 Transcript Interview 8.docx

1 Quotations:

8:11 ¶ 205, depending on the contents of it itself, of course. Like like you mentioned. Yeah, but I'm a little.…

In Document:

8 Transcript Interview 8.docx

○ *Understanding the risks*

Used In Documents:

4 Transcript Interview 4.docx

1 Quotations:

4:15 ¶ 204 – 207, Speaker 2 Ja. Ja. Ja ja ja. Speaker 2 Wil graag ja nee, zeker en en het lijkt me ook logisch In de h…

In Document:

4 Transcript Interview 4.docx

Appendix 6 – Draft Recommendations

MDM-MAM Security Controls Recommendations

Introduction and Rationale

The recommendations in this document are based on research aiming at increasing security by designing security controls that account for user's needs. Particularly important were the interviews with users across higher education institutions (HEIs) in the Netherlands. The findings indicate the presence of "shadow IT": users frequently resort to shadow IT not out of malice but because they see their work being hindered by the security measures. In addition, research showed how communication and understanding of the reasons behind the security measures are lacking.

Hence, security solutions encountered in previous research, such as strong access control rules, device enrollment, secure authentication protocols, and strong encryption standards, need to be addressed in a human-centered manner. The policy recommendations below are a product of the balance between the technical risks and user needs. To achieve this, users' perspectives werre critical: policies designed without considering usability risk resistance and non-compliance. A human-centered approach ensures security measures are effective while respecting usability.

Recommendations

Recommendation #1 – Risk-Based, Tailored Security

Security controls should be proportional to the sensitivity of the data and the role of the user. This is a critical principle, especially in the context of higher education and academic freedom. For instance, staff may choose between corporate-owned devices (COD) managed via MDM or their own personal devices (BYOD) secured through MAM. COD provides the option of a device fully meant for work, while BYOD respects user autonomy, integrating work into familiar ecosystems. For BYOD, security measures focus on protecting the data, leaving personal use largely unaffected.

Recommendation #2 – Document Labeling: it's all about consciousness

Documents should be labeled according to sensitivity levels, such as public, internal, confidential, or restricted. This can be achieved using Microsoft Purview or similar tools. Users select a label for each document they create or download. Certain actions may require confirmation depending on sensitivity, but blocking an action altogether is not recommended, as this control can be easily circumvented. Labels act as a warning to users performing risky actions and strengthen awareness among the users. Minimal additional effort is required, and users generally perceive this as helpful rather than burdensome.

Recommendation #3 – Role-Based Local Administrative Rights

Local-access should be automatically granted to roles that genuinely require it, while other users should have restricted rights. Temporary access and exceptions should be requestable. Users should be clearly informed of access limitations, and be informed that they should submit requests timely to avoid disruption to their work.

Recommendation #4 – Role-Based Complex Passwords

For account protection, SSO and MFA remain paramount and should be implemented for all users, where possible. Extra authentication measures should be implemented based on the sensitivity of data and user role, for instance when accessing specific folders, or on the devices of high-risk users. In fact, in the context of MDM and MAM, users as HR staff, board members, directors, or sensitive research personnel require stronger authentication, while lower-risk users may use short PINs or biometrics, whereas high-risk roles may be required to employ longer PINs or multi-factor authentication. This recommendation refers to device access (MDM) and data access on the device (MAM), for instance when opening OneDrive.

Recommendation #5 – Controlled Email Forwarding

Automatic forwarding of all institutional emails to personal accounts should be disabled by default. Exceptions may be granted when risks are low and justified. Emails marked as highly confidential should never be forwarded externally. It is recommended to weight the time and effort against the increased security: is it effective to disgruntle a perhaps older standard user who might retire in a few years?

It is important to remember that users could avoid email forwarding by asking students or colleagues to email their private address directly, circumventing the control. So, the policy should provide controlled alternatives that address legitimate user needs without compromising security. As an example, a “notification-only” option allows users to receive alerts about messages from specific senders received in their work inbox without sending full content externally.

Recommendation #6 – User Communication and Engagement

Clear and timely communication is critical. For new hires, device collection provides an ideal opportunity to explain security policies, clarify expectations, and answer questions. For current employees, informal personal interactions with security officers are more effective than emails or digital campaigns. Prioritizing high-risk groups and gradually extending engagement ensures sustainability. Listening to user concerns fosters collaboration and trust, improving compliance. Practical examples of mistakes from previous incidents increase awareness and reinforce secure behaviors.

Recommendation #7 – Real-Time Risk Notifications

Users should, where possible, receive alerts when performing risky actions. For instance, banners or pop-ups can warn users attempting to upload sensitive documents to unapproved platforms. The purpose is increasing consciousness in the users that what they are doing may not be secure. Notifications should explain the risk and suggest approved secure alternatives. Priority should be given to high-impact actions, such as sharing confidential documents externally: an alert in Outlook informing the user they are sending or forwarding a sensitive document would be effective.

Recommendation #8 – Extra Authentication Measures

Additional authentication steps are required for access to sensitive applications and data repositories. Users said to accept extra security when deemed proportional. To mitigate this issue, users should be communicated about the risks they may inadvertently pose. Also, only when necessary from a risk-based perspective should institutional accounts require additional passwords or PINs for high-sensitivity

resources like OneDrive, Outlook, or restricted folders. BYOD users should receive lighter measures unless handling high-risk content.

Recommendation #9 – (Un)approved tools list

A whitelist of approved applications would provide clear guidance of what is allowed and what is not. Likewise, a list of unapproved tools, with an explanation of why certain tools or websites have been blocked would enhance awareness. A "tool picker" would support users in choosing secure alternatives for commonly used unsecure applications. Despite the local-admin block, users should be allowed to install approved applications themselves or request streamlined approval, fastening the response time and reducing frustration.

Recommendation #10 – Risk Acceptance Mechanism

Users formally acknowledge understanding of security risks and responsibilities. This can be integrated into employment contracts or acceptable use policies for COD and BYOD devices. For new hires, the process should occur during onboarding, with the new hire having access to the security policies and to the security officers to ask for clarifications. The explanation should cover the policies, common risks, and mitigation strategies, focusing on why certain security measures are implemented: the goal is enabling the users to understand the reasons behind a security control.

Appendix 7 – Ethical declaration

This thesis researches how Mobile Device Management (MDM) and Mobile Application Management (MAM) policies and solutions can be written and made in such a way that users accept and adopt these solutions and follow the policies. This aims at limiting the risk of employees resorting to unapproved IT tools (shadow IT). The RQ of this master's thesis is: "How can higher education institutions increase acceptance of MDM and MAM solutions among their employees taking both their employees' perception and security requirements into consideration?"

To answer this question, we need the end-users of the MDM/MAM solutions and policies (university and HBO employees) to understand what their needs are and ensure the limitations MDM and MAM impose are not too strict that these employees would try to dodge these limitations by using other tools. Hence, the participants are university and HBO employees, who will be reached with convenience sampling (for the first interviews) and snowball sampling. For convenience sampling, platforms such as LinkedIn and emails will be used to reach the participants.

The interview will not cause serious burdens on the participants and the interviews will last approximately 30 minutes. No manipulation will take place: the participants will be asked to narrate their experience with current limitations of MDM/MAM solutions and provide their opinion about possible future limitations by new policies and solution. The point is trying to understand what would cause too much issues or concerns to the users that they would reject the MDM/MAM policies and solution.

The only personal data gathered will be the institution the participant works at, and their role (in general, not specific: such as employee in the HR department, employee in the IT department, professor, PhD candidate, etc.). The interviews will be recorded (only if consent is provided by the interviewee) and an eventual transcript will only be accessible by the research and his supervisor.

Appendix 8 – Final Recommendations

MDM-MAM Security Controls Recommendations

Introduction and Rationale

The recommendations in this document are based on research aiming at increasing information security at higher education institutions (HEIs) in the Netherlands. This is achieved by designing security controls that account for usability needs. To establish these controls, particularly important were the eight interviews with users across institutions.

Previous research indicated the presence of "shadow IT": users frequently resort to shadow IT not out of malice but because they see their work being hindered by security measures. Hence, security solutions encountered in previous research, such as strong access control rules, device enrollment, secure authentication protocols, and strong encryption standards, need to be addressed in a human-centered manner.

This research showed how two things are deemed critical to user acceptance: communication and balance. Regarding communication, users want to understand why certain controls are implemented, and what are the risks if they are not. Regarding balance, users would like policies that are appropriate for their perceived level of risk: so, while explaining the risks, it is advised to highlight how implementing certain controls covers those risks.

In conclusion, the policy recommendations below are the product of the balance between security requirements and user needs.

Recommendations

Recommendation A – Risk-Based, Tailored Security

On top of a first basic layer of security controls applicable to all employees, stricter controls should be proportional to the sensitivity of the data and the role of the user. For instance, for users with access to large amount of personal data or to sensitive or confidential data, stricter security controls are legitimate and justifiable. Applying this principle is the context of higher education is critical, as it demonstrates that, where possible, freedom is left to the users. Furthermore, when possible, staff should be able to choose between corporate-owned devices (COD) managed via MDM or their own personal devices (BYOD) secured through MAM. COD provides the option of a device fully meant for work, while BYOD respects user autonomy, integrating work into familiar ecosystems. For BYOD, security measures should focus on protecting organizational data, leaving personal use largely unaffected.

Recommendation B – Document Labeling: it's all about consciousness

Documents should be labeled according to sensitivity levels, such as public, internal, confidential, or restricted. This can be achieved using Microsoft Purview or similar tools. Users select a sensitivity label for each document they create or download. Certain actions may require confirmation depending on sensitivity, but blocking an action altogether is not recommended, as this control can be easily circumvented. Labels act as a warning to users performing risky actions and strengthen awareness among the users. Minimal additional effort is required, and users generally perceive this as helpful rather than burdensome.

Extra information about Microsoft Purview can be found in Appendix 11.

Recommendation C – Controlled Email Forwarding

Automatic forwarding of all institutional emails to personal accounts should be disabled by default. Exceptions may be granted when risks are low and justified. Emails marked as confidential should never be forwarded externally. It is recommended to weigh the time and effort against the increased security: is it effective to frustrate a perhaps older regular user who might retire in a few years? It is important to remember that users could avoid email forwarding by asking students or colleagues to email their private address directly, circumventing the control. So, the policy should provide controlled alternatives that address legitimate user needs without compromising security. As an example, a “notification-only” option allows users to receive alerts about messages from specific senders received in their work inbox without sending full content externally.

Recommendation D – User Communication and Engagement

Clear and timely communication is critical. For new hires, device collection provides an ideal opportunity to explain security policies, clarify expectations, and answer questions. For current employees, informal personal interactions with security officers are more effective than emails or digital campaigns. Prioritizing high-risk groups and gradually extending engagement ensures sustainability. Listening to user concerns fosters collaboration and trust, improving compliance. Practical examples of mistakes from previous incidents increase awareness and reinforce secure behaviors.

Recommendation E – Real-Time Risk Notifications

Users should, where possible, receive alerts when performing risky actions. For instance, banners or pop-ups can warn users attempting to upload sensitive documents to unapproved platforms. The purpose is increasing consciousness in the users that what they are doing may not be secure. Notifications should explain the risk and suggest approved secure alternatives. Priority should be given to high-impact actions, such as sharing confidential documents externally: an alert in Outlook informing the user they are sending or forwarding a sensitive document would be effective.

Recommendation F – Extra Authentication and Access Controls

For account protection, SSO and MFA remain paramount and should be implemented for all users, where possible. Extra authentication measures, on top of the baseline applicable to all users, should be implemented based on the sensitivity of the data and the role of the user, for instance when accessing specific folders, or on the devices of high-risk users. In fact, in the context of MDM and MAM, users such as HR staff, board members, directors, or sensitive research personnel require stronger authentication, while lower-risk users may use short PINs or biometrics, whereas high-risk roles may be required to employ longer PINs or multi-factor authentication. This recommendation refers to device access (MDM) and data access on the device (MAM), for instance when opening OneDrive.

Recommendation G – (Un)approved tools list

A whitelist of approved applications would provide clear guidance of what is allowed and what is not. Likewise, a list of unapproved tools, with an explanation of why certain tools or websites have been blocked would enhance awareness. A “tool picker” would support users in choosing secure alternatives for commonly used unsecure applications. Despite the local-admin block, users should be allowed to install approved applications themselves or request streamlined approval, fastening the response time and reducing frustration.

These recommendations have been shared with SURF and its members, including the rationale behind them (Appendix 8). The policy proposal contain recommendations: it is responsibility of the HEIs to identify the recommendations to implement first, but it is suggested to grab the “low-hanging fruits”, as they are called in the consultancy world. It refers to those low-effort actions that deliver some improvements compared to the current situation. In this case this consist of recommendations B and D.

Appendix 9 – Table 8 (Interview goals and related questions)

Interview Goals:	Interview Questions:
Understand user experience with and opinions about MDM and/or MAM for CODs	1 to 5
Understand user experience with and opinions about MDM and/or MAM for BYODs	6 to 10
Understand interviewees' perception and opinion about potential use of MDM/MAM with hypothetical scenarios for interviewees who do not have a COD nor a BYOD	11, 12
Understand which use interviewees make of MDM and/or MAM for CODs	2, 3
Understand which use interviewees make of MDM and/or MAM for BYODs	6, 7
Understand user experience with MDM/MAM (benefits and limitations)	4a, 4b, 4c, 9a, 9b, 9c
Understand how the interviewee experienced communication (if any) about their possibilities and limitations with COD	4d

Understand how the interviewee experienced communication (if any) about their possibilities and limitations with BYOD	9d
Understand eventual privacy concerns COD-MDM	4e
Understand eventual privacy concerns COD-MAM	4f
Understand eventual privacy concerns BYOD-MDM	9e
Understand eventual privacy concerns BYOD-MAM	9f
Test potential MDM/MAM limitations on COD/BYOD	11, 12
Understand which communication methods would be best suited to the users (interviewees)	5, 10

Appendix 10 – Translation of users' quotes

1) "I don't know well why that is secured in that way: that you can only open links in Edge and that you cannot copy and paste them outside of the Outlook application. I don't know why it is secured like this. And thus I would like to be able to do it"
   "Ik weet niet goed Waarom dat op die manier beveiligd is dat je Alleen linkjes In de edge kan openen en dat je Alleen dat je niks mag kopiëren en buiten de Outlook app mag plakken. Ik weet niet Waarom dat zo beveiligd is. En Daarom zou ik dat wel graag gewoon willen kunnen."
2) "So if I could understand the reason, I be more at peace with it"
   "Dus Als ik de reden zou snappen, zou ik er ook meer vrede mee hebben".
3) "that is a good moment [when people receive their device] to set a first step in that [communication]"
   "dat is wel een een goed moment [when people receive their device] om in ieder geval het begin daarvan [communication] neer te zetten".
4) "Yes, I would like to receive a really short, concrete, clear checklist"
   "Ja, ik zou daar heel graag een een hele korte, concrete, duidelijke ja. Checklist for voor willen krijgen"
5) "it's also about making people aware of this"
   "het gaat denk ik deels ook al om de bewustwording van dit"
6) "Pop-ups or something similar, a notification would possibly help a bit at that point"
   "Pop-up, of weet ik veel. Een melding zou kunnen zijn dat in dat proces eventjes zou helpen"
7) "On the website a whitelist of the applications that can get installed or requested"

"Op de website een whitelist van applicaties die geïnstalleerd kunnen worden of dat je daar een verzoek voor kan neerleggen"

8) "…then I would quickly take my personal laptop and do it, you know, to be able to go on with the work"
   "…dan zou ik zelf al gauw bijvoorbeeld mijn privé laptop pakken om zoiets te doen, weet je wel om door te kunnen"
9) "Yes and it would be ok for example if you needed to think about that when starting a project"
   "Ja ik zou het prima vinden bijvoorbeeld Als je een project moet starten om even gewoon na te denken"
10) "Yes, I currently have a white and a blue cloud. The blue is the OneDrive of the university, the white one is my personal OneDrive".
    "Ja, Ik heb op dit moment letterlijk een wit wolkje en een blauw wolkje. De blauwe wolkje is OneDrive van de universiteit, de witte prive"
11) "Yes, I would accept it [extra code for work-apps], I would find it a bit intrusive, but I would accept it".
    "Ja, ik zou het wel accepteren. Ik zou het een beetje bemoeiend vinden, maar ik zou het wel accepteren"
12) "That happens often, also with banks application I have to continuously do it [insert a code]"
    "Je hebt nu ook vaak hè? Bij banken en bij dingen moet ik het ook continueren doen"

Appendix 11 – Microsoft Purview & Sensitivity Labels

Microsoft Purview: Data Security and Governance | Microsoft Security

Learn about sensitivity labels | Microsoft Learn