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 – Know the sensitivity of your data

Documents, emails, data, and even systems should be labeled according to sensitivity levels, such as public, internal, confidential, or restricted. For documents and emails, there are tools that enable users to select a sensitivity label for each document or email they create and download. Mainly, 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. Moreover, this also allows the implementation of specific security controls based on the sensitivity: for instance, certain actions (such as forwarding an email to an external party) may require confirmation

depending on sensitivity, but blocking an action altogether is not recommended, as this can often be easily circumvented.

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.