Acceptable Use Agreement for Mobile Application Management (MAM)

Introduction

This Acceptable Use Agreement outlines the guidelines and responsibilities for staff members of Dakota State University who choose to use their personal devices to access University resources and agree to enroll their devices in the university's Mobile Application Management (MAM) solution. This agreement is designed to ensure the security, confidentiality, and integrity of university data and the mobile applications used to access these resources while supporting a productive and safe working environment for all staff.

Scope

This agreement applies to all staff members who wish to use their personal devices to access University resources and choose to connect them to the University's MAM solution.

Device Enrollment and Compliance

MAM Enrollment: All staff who wish to access any DSU resource are required to enroll their personal devices in the university's MAM solution before accessing any University systems. MAM enrollment allows the university to manage and secure University application of personal devices, ensuring compliance with security policies.

Compliance Checks: Periodic compliance checks will be conducted to ensure that devices remain compliant with university security standards. Non-compliant devices may be restricted from accessing university resources until they meet the necessary security requirements.

Non-compliant devices: For any devices that have been found to be out of compliance set forth by ITS/DDS security standards, enrolled users agree to allow ITS/DDS compliance staff to wipe/remove all University related data and/or apps to mitigate any compromise or device theft.

Data Security

Application Management: Access to DSU resources on personal devices will require the installation of Microsoft Company portal.

Application Security: These applications will be containerized and isolated from any personal data or other applications installed on the device.

Security Posturing: Staff devices enrolled in MAM shall have the latest security patches for their systems before accessing any DSU resources.

Network Usage

Secure Wi-Fi Connections: When connecting to any non-University Wi-Fi networks, staff members should prioritize secure networks and avoid using public, unsecured Wi-Fi whenever possible.

Avoid Public Computers: Staff should refrain from using public computers or internet cafes to access university resources, as these may pose security risks.

Approved Devices: Staff shall only have access to DSU resources using those devices which have been added to the University's MAM solution.

Reporting Security Incidents
Staff are required to report any lost or stolen devices immediately to DSU's Digital Data Services. This helps to mitigate potential data breaches and ensures a swift response to protect university information.

DSU Digital Data Services Phone: 605-256-5675

DSU Digital Data Services Support Ticket: support.dsu.edu

Personal Use Restrictions
Staff members are reminded that personal use of university devices should adhere to the same standards as professional use. Inappropriate or unauthorized use may result in loss of access to these applications.

Agreement Violations
Any violations of this agreement may result in the removal of device access to university resources, and further disciplinary actions may be taken in accordance with university policies.

Review and Updates
This agreement will be reviewed periodically and updated as necessary. Staff members will be notified of any changes to the agreement.

By agreeing to this, DSU staff members acknowledge their responsibility to adhere to these guidelines and understand the importance of safeguarding university data and resources during international travel.