UNIVERSITY of DENVER	**UNIVERSITY OF DENVER** **POLICY MANUAL** **MOBILE DEVICE USE POLICY**

Responsible Department: Information Security Office **Recommended By:** VC Information Technology **Approved By:** Chancellor, University of Denver	**Policy Number** IT 2.30.066	**Effective Date** 10/27/2021

I. INTRODUCTION

Mobile computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using them.

II. POLICY OVERVIEW

A. The purpose of this policy is to establish rules for the use of mobile devices and their connection to University networks. These rules are necessary to preserve the confidentiality, integrity, and availability of University data and systems.

B. This policy applies to all University faculty, students, and staff that utilize portable (mobile) computing devices and access University Information Resources. All mobile devices, whether owned by the University or its faculty, students, or staff that have access to university Information Resources are governed by this Mobile Device Use Policy.

III. PROCESS OVERVIEW

A. Only IT Department-approved mobile computing devices may be used to access the University's networks and Information Resources for business purposes.

B. All University-owned mobile computing devices must be protected with a password required at the time the device is

powered on. The password must meet the requirements of the University's **Password Policy**.

C. Sensitive data shall not be stored on mobile computing devices. However, in the event that there is no alternative to local storage, all sensitive data must be encrypted using approved encryption techniques per the **University E-mail Encryption Policy**.

D. Data must not be transmitted via wireless to or from a Mobile Device unless approved wireless transmission protocols along with approved encryption techniques are utilized. *See* the **Wireless Access Policy** for more information.

E. Non-University owned mobile computer devices that require network connectivity must conform to the University of Denver's IT standards and its user(s) must comply with the University's **Acceptable Use Policy**.

F. Unattended mobile computing devices must be physically secured. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

G. Laptops and other mobile computing devices that access the University's network infrastructure shall have active and up-to-date anti-malware protection.

H. Annual security education and awareness training shall be provided to University staff that use mobile devices. Such training shall include:

- Minimum necessary. Staff shall only have access to the minimum amount of data necessary to perform their job duties.
- Lost devices. Staff must immediately report any lost or stolen devices.
- Unauthorized access. Any unauthorized access to the mobile device or company data must be immediately reported.
- Rooting devices. Mobile devices must not be "rooted" (device access restrictions removed to allow low-level function access. Often referred to as "Android Rooting" or iPhone "Jailbreaking") or have unauthorized software/firmware installed.
- Content. Staff shall not load illegal content or pirated software onto a mobile device.

- Patch management. Mobile devices and applications must be kept up to date. Patches should be installed within 30 days of release.
- Anti-malware. Mobile devices must have active and up-to-date anti-malware protection software.
- Encryption. Encryption shall be used to protect sensitive information.
- Work habits. Staff shall use the University's corporate e-mail system when sending or receiving University data.
- Backups. Staff are responsible for ensuring all important files stored on the mobile device are backed up on a regular basis.
- Management software. Mobile device management software will be used to enforce common security standards and configurations.

I. The Chief Information Security Officer (CISO) shall ensure:

- Training. Annual security training is provided to users of mobile devices. Periodic security reminders may be used to reinforce mobile device security procedures.

- Mobile device management. An evaluation is performed to determine the appropriate Mobile Device Management software to be used to reduce costs and business risks related to mobile devices. Features of Mobile Device Management software include the ability to inventory devices, monitor devices (e.g., application installations), issue alerts (e.g., disabled passwords, out of date operating systems, rooted devices), and issue reports (e.g., installed applications, carriers). The CISO shall ensure Mobile Device Management software enforces security features such as encryption, password, and key lock on mobile devices. The CISO shall perform a review to determine if Mobile Device Management software should include the ability to distribute applications, data, and configuration settings

- Security. The CISO shall remain up to date on industry standard security best practices for mobile devices. Resources can include NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise (**NIST Special Publication 800-124**).

- Exemptions. A risk assessment and risk analysis shall be performed for any requests for exemptions from this Policy.

J. The IT Department shall implement procedures and measures to strictly limit access to sensitive data from mobile computing devices which are generally higher risk than non-portable devices (e.g., desktop computers).

V. DEFINITIONS

None

Revision **Effective Date**	**Purpose**