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 13.10.011	**Effective Date** 4/4/2023

I. INTRODUCTION

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.

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

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

III. PROCESS OVERVIEW

A. Personally-owned Mobile Devices with access to University Data must conform to this Policy, accept the University's terms of use including privacy expectations and device management requirements, and comply with the University's **Acceptable Use Policy**.

B. Mobile devices used to access the University’s networks and store or access University Data must meet the following minimum security requirements. Mobile devices must:

1. be encrypted.
2. be protected with a power on password or passcode. Biometric authentication (e.g. facial recognition, fingerprint scanning, etc.) can be used instead of a power on password or passcode.
3. have the activity timeout activated.
4. have the automatic device wipe after set number of login attempts activated.
5. not be modified in a way that bypasses security controls and privacy requirements. E.g. device jailbreaking or rooting.

C. Device-owners must notify the University’s Help Center in the event a Mobile Device, which stores or accesses University Data, has been lost or stolen. The University reserves the right:

1. To suspend University Data synchronization
2. To initiate data wipe procedures to delete University Data.

D. Unattended Mobile Devices, that store or access University Data, 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.

E. Annual security education and awareness training shall be provided to University faculty and staff that use Mobile Devices.

F. Laptops and other computing devices that access the University’s network infrastructure must have active and up-to-date anti-malware protection.

G. Subject to the approval of the Senior Vice Chancellor for Legal Affairs and General Counsel, in certain circumstances, including to comply with legal obligations where litigation is threatened or pending, the University may require employees with University Data stored on University-owned or personal devices to preserve such data and/or make the device available to the University to facilitate collection of such data. *See also* University Policy LEGL 1.10.060 – *Litigation Hold*.

H. The Chief Information Security Officer (CISO) is responsible for assessing security risks and implementing appropriate security controls on Mobile Devices.

I. Travelers on University-sponsored travel to destinations with heightened cybersecurity risk must use a loaner Mobile Device(s) from IT. *See* the policies and procedures on Mobile Devices and High-Risk Travel available on the IT website for requirements and guidance about the transport and use of electronic devices when traveling to high cybersecurity risk destinations and the University program for loaner devices while traveling on University business.

V. DEFINITIONS

A. "Information Resources" means all devices, services, networks and other resources and technology related to the transaction of University business, regardless of form or location, that are owned, provided, or administered by or through the University, or used to electronically store, process, or transmit information.

B. "Mobile Device" means a communication device that is portable and designed to be carried by a person to carry out business communication activities. Mobile Devices items include but are not limited to cell phones, smart phones, iPhones, iPads, Droid, hands-free devices and laptops (Note: For purposes of this Policy, the definition of Mobile Device does include laptops, in contrast to the definition used in University Policy FINA 2.30.020 – *University-issued Mobile Device(s)*.

C. "University Data" means all data owned or licensed by the University.

Revision Effective Date	**Purpose**
4/4/2023	*Update to align policy with practice and update policy number*