	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

B. Mobile devices used to access the University 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

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.