Operational Area:	Information and Technology
Responsible Executive:	Chief Information Officer
Responsible Office:	Information Technology Services
Effective:	January 1, 2022

Device and Infrastructure Security

Information and Technology

Contents

I. Introduction

A. **Authority:** Colorado Revised Statutes (C.R.S.) § 23-54-102, *et seq.* (2022) authorizes the Trustees of Metropolitan State University of Denver ("MSU Denver" or "University") to establish rules and regulations to govern and to operate the University and its programs. The MSU Denver Trustees retain authority to approve, to administer, and to interpret policies pertaining to University governance. The MSU Denver Trustees authorize the MSU Denver President to approve, to administer, and to interpret policies pertaining to University operations.

B. **Purpose:** The purpose of this policy is to ensure that all devices used to process, transmit, or store data associated with Metropolitan State University of Denver computing systems are appropriately secured.

C. **Scope:** This policy applies to all individuals, including students, faculty, staff, and contractors provided access to University data and information technology systems. Contractors and otherwise affiliated individuals must agree to abide by the information security policies before accessing University systems and data. Role-based policies and procedures that apply to specific groups of users will be provided when applicable, in accordance with functional requirements and data classification.

Device and Infrastructure Security

Information and Technology

II. Roles and Responsibilities

A. **Responsible Executive:** Chief Information Officer

B. **Responsible Administrator:** Chief Information Security Officer

C. **Responsible Office:** Information Technology Services

D. **Policy Contact:** IT Services, www.msudenver.edu/technology, 303-352-7548

III. Policy Statement

A. **Institutionally Issued Devices**

1. Devices purchased with University funds are the property of the University, not the individuals to whom they were assigned. These devices must be returned to IT Services upon lease-end, when no longer supported, or when the assignee ends their employment with the University.
2. Devices issued by MSU Denver will be configured with certain security configurations and security applications. These devices may include disk encryption, virus protection, built-in firewalls, and other features. These security applications and settings must not be altered by end users without authorization from IT Services.
3. Software installations and updates must be performed using approved IT Services processes. Any software acquisitions including free software must be approved by IT Services.

B. **Mobile Devices.** Mobile devices, including but not limited to, smart phones, mobile readers, laptops, and portable storage devices may be used to connect to MSU Denver computing systems. These devices must be appropriately secured and must never be used to store confidential information such as Social Security Numbers (SSN) or credit card numbers.

C. **Personally Owned Devices.** Personally owned devices may be used to connect to MSU Denver computing systems. These devices must be appropriately secured and must never be used to store University confidential information, such as Social Security Numbers (SSN) or credit card numbers.

D. **Network Devices and Services**

1. Networking devices attached to MSU Denver networks are to be installed and maintained by MSU Denver IT Services Networking administrators or those authorized by IT Services. Unauthorized installation or use of networking devices such as wireless access points, network switches or routers, or other devices can interfere with MSU Denver Networking systems, and is therefore prohibited. Unauthorized devices found to be connected to MSU Denver networks may be disabled, disconnected, and/or confiscated if they are found to be inappropriately installed.
2. Any technical systems or services which will require connections to MSU Denver computing and networking infrastructure must be reviewed and approved by IT Services prior to purchase or implementation.

E. **Procedures.** Adherence to MSU Denver information-security policies is mandatory and may be based on state or federal statute, contract language, or information-security standards. These policies are not intended to unreasonably interfere with system utilization. Individuals should contact the IT Service Desk to report security risks, violations of policy, or to make requests for exceptions or amendments to the policies. The Chief Information Security Officer (CISO) and other IT Services staff will respond to all reported security issues.

F. **Sanctions.** Violations of these policies may result in fitting administrative action up to and including revocation of system privileges, employee termination, or student expulsion.

IV. Related Information

A. MSU Denver Global Email to Employees Policy
B. MSU Denver Global Email to Students Policy
C. MSU Denver Acceptable Use of Computing Systems Policy
D. MSU Denver ACTC Wireless Network Standard
E. MSU Denver Information and Instructional Technology Policy Subcommittee

V. History

A. **Effective:** January 1, 2022
B. **Enacted:** July 1, 2017
C. **Review Schedule:** This policy will be reviewed every three years or as deemed necessary by University leadership.

VI. Approval

Janine Davidson, Ph.D.
President, Metropolitan State University of Denver

N/A

Chair, Board of Trustees, Metropolitan State University of Denver