Published on *University of Colorado* (https://www.cu.edu)

Secure Computing Standard for CU System Administration Computers [1]

Background

Please refer to the System Administration of Colorado’s Administrative Policy Statement (APS) 6005 [2] IT Security Program and the System-wide Baseline Security Standards [3], which apply to all individuals who access or control the University of Colorado's information technology resources.

Purpose

This standard identifies the minimum requirements for all CU System Administration-owned computers (“System computers”) to ensure the integrity and security of System Administration data and the shared information technology environment, including networks, services and systems.

All System computers used by faculty, staff, students, or other authorized individuals must meet this Standard, regardless of manufacturer, function of the system, or location. These actions are necessary to ensure resource availability, reinforce System Administration's security and compliance posture, and protect the confidentiality of data assets.

Standard

The following IT capabilities must be met to ensure consistent application of protections and adherence to the System Administration Information Technology Policy [4], provide visibility into campus threats, and support incident response. At all times university computers must:

1. Run current, supported software. Using out-of-date operating systems or software that is not being actively updated and considered *end-of-life* is prohibited.

2. Be enrolled in Microsoft Endpoint Configuration Manager (Windows computers) or Jamf (Mac computers).

3. Be encrypted with whole disk encryption (Bitlocker for Windows, FileVault for macOS).

4. Run Microsoft Defender for real-time scanning to prevent, detect, and remove malware or potential vulnerabilities.

5. Gather and send hardware and software information to the central inventory for vulnerability tracking, network identification, and audit preparedness.

6. Use UIS-supported and UIS-approved enterprise cloud storage solutions (Microsoft OneDrive) to back up and protect data from loss.

7. Have the System Administration approved VPN client installed to ensure timely application updates and patches.

More information about the UIS-supported and UIS-approved applications associated with the computer requirements listed above can be found on the UIS Service Desk website.

Exceptions

Systems Administration employees and authorized individuals who are unable to meet all components of the standard must apply to UIS for a computer exception. If a compelling business reason exists, exceptions to the requirements outlined in this standard may be granted by the CU System Information Security officer in consultation with the Chief Information Officer (CIO). Inquiries regarding exceptions should be made to the CIO.

University computers subject to specific data protections (e.g., federal regulations, data use agreements) that exceed the requirements identified within this Standard must meet whichever controls are more stringent.

University computers not capable of meeting the requirements identified in this Standard must be identified and their users must work with UIS and Information Security to determine the appropriate compensating security controls for such computers. Should a computer be identified as a high risk to the System Administration network, it must be removed.

Administration and Enforcement

Computers that do not meet the campus-certified computer standards may pose a risk to Systems Administration and its data. Per the Acceptable Use Policy [4], the Chief Information Officer or Information Security Officer may suspend a computer’s and/or an end-user's access to the campus network or any campus computing resources when it reasonably appears necessary to preserve the integrity, security, or functionality of campus computing resources.

Definitions

Authorized Individuals: This includes those in roles such as:

- Person of Interest (POI): an individual affiliated with System Administration but not paid as an employee who is granted access for official university needs.

- Sponsored Affiliate: an individual affiliated with System Administration who is granted access for official university needs when an HR appointment, including POI, is not a possibility.

End of life: A designation by the vendor when a product is unable to be supported and should be replaced. This generally occurs when the operating system or application is no longer supported, and the hardware cannot support a new operating system.

University data: Official information of the institution, including but not limited to university work products, results, materials, records, or other information developed or produced with university goods, funds or services. University information encompasses all information created by System Administration, including information classified as private or restricted. Examples include university website content, schedules of courses, requests for proposals, policies and guidelines, personnel records, electronic communications, student data, and patient data.

Systems Administration-owned computer: Any computer that was purchased with System Administration funds used by faculty, staff, students, Persons of Interest (POIs) and sponsored affiliates to access information technology resources, including laptops, desktops, tablets or mobile phones. This does not include printers, removable storage, or Internet of Things (IoT) devices and sensors.

Related Policies

Administrative Policy Statement, "IT Security Program Section 1, IT Resource User Responsibilities”
https://www.cu.edu/policies/aps-it.html [5]

Administrative Policy Statement, for IT Users, "Providing and Using Information Technology"
https://www.cu.edu/policies/aps-it.html [6]

Administrative Policy Statement, "Political Participation by Members of the University Community”
http://www.cusys.edu/policies/Personnel/politicalpart.html [7]

Administrative Policy Statement, “Use of Electronic Mail”
https://www.cu.edu/ope/aps/6002 [8]

Published Date

June 16, 2023

Groups audience:
UIS Service Desk

Source URL:https://www.cu.edu/service-desk/about-us/secure-computing-standard-cu-system-administration-computers

Links
[1] https://www.cu.edu/service-desk/about-us/secure-computing-standard-cu-system-administration-computers [2] https://www.cu.edu/ope/aps/6005 [3] https://www.cu.edu/security/system-wide-baseline-security-standards [4] https://www.cu.edu/docs/system-administration-information-technology-policy-use-it-resources [5] https://www.cu.edu/policies/aps-it.html%C2%A0 [6] https://www.cu.edu/policies/aps-it.html [7] http://www.cusys.edu/policies/Personnel/politicalpart.html [8] https://www.cu.edu/ope/aps/6002