-

Computer Standardization Policy

Policy ID:	500
Version:	2.0
Policy Owner:	Chief Information Officer (CIO)
Policy Approver:	President, University of Oklahoma

PURPOSE

The purpose of the OU Computer Standardization Policy is to support and enhance the missions and administrative functions of the University of Oklahoma. The objective of the OU Computer Standardization Policy is to achieve and maintain computing capabilities that provide a high level of productivity for OU workforce members in a secure and cost-effective manner. Standardizing computer equipment at OU:

- Provides employees with guidance in planning for future needs.
- Allows the University to negotiate the best possible pricing on select models.
- Makes the computer procurement process more efficient.
- Helps maintain technology compatibility across the organization.
- Brings a systematic approach to the acquisition and disposal of computer equipment, and
- Standardizes equipment to minimize maintenance and support and to simplify regulatory compliance.

SCOPE

Effective January 1, 2019, this policy applies to all University of Oklahoma employees, as well as all temporary workers and those given access to IT systems and services, at all access locations including on-site and remote/off-site locations. (Note: Computers purchased prior to January 1, 2019, may continue to be used until the end of their lifecycle, but must still comply with the relevant control statements regarding configuration, lifecycle, warranty, and disposal, below.)

DEFINITIONS

Computers, in the context of this policy, are defined as all computer variations (desktop, laptop, notebook, etc.) owned by the University of Oklahoma that run a complete desktop operating system and are used for performance of job functions and/or business/instructional purposes. Other computing devices, such as servers and hand-held devices, are not considered computers for the purpose of this policy.

Externally derived research funds, in the context of this policy, refer to University accounts categorized as SPNSR, SP490, or NONSP (e.g., FAR/SRI distribution) funds within the PeopleSoft financial system.

Internally derived research funds, in the context of this policy, refer to all other funds intended for research activities, including internally funded research grants, center, and startup funds.

University funds, in the context of this policy, refer to all University accounts and funding sources within the PeopleSoft financial system that are NOT defined above as ***internally*** or ***externally derived research funds***.

POLICY

Standardized Computers

University computers must be purchased from OU's published Computer Standards List (https://ou.edu/ouit/computer_standardization/specs), which includes standard vendor models, hardware configurations, recommended lifecycles, and use cases. Pre-negotiated pricing can be viewed on OU Marketplace. Exceptions must follow the Standard Computer Equipment Exceptions process outlined below.

One Computer Per Employee

This policy allows ***University funds*** to be used to purchase one (1) desktop computer or one (1) laptop with docking station and external monitor, as necessary, per employee. Users will be eligible to replace this computer at the end of the lifecycle documented on the Computer Standards List or if the computer malfunctions and cannot be repaired or replaced through a warranty claim.

Additional **standard** computers may be purchased for a single employee using ***externally derived research funds***. Requests to use ***internally derived research funds*** to purchase additional computers for a single employee must follow Non-Standard Computer Equipment and Inventory process below, as these funds often share accounts with other funding sources.

Non-Standard Computer Equipment and Inventory

Users or Departments requesting computer equipment that deviates from this policy must complete the Non-Standard Computer Equipment and Inventory form linked from the Computer Standards List, providing at a minimum: mission-specific (academic, research, administration, etc.) justification, provision of the requested computer equipment, and available price.

- OU IT will automatically approve requests using ***externally derived research funds***.
- Requests using ***internally derived research funds*** will be approved once the funding source can be confirmed, as these funds often share accounts with other funding sources.
- All Non-Standard Computer Exceptions requested using ***University funds*** require approval by designated authorities defined for each campus process.

This process enables OU IT to maintain a asset inventory for risk mitigation, security, support, and compliance purposes and also facilitates future planning of standard offerings.

Procurement/Acquisition

Per Purchasing guidelines (http://www.ou.edu/purchasing/pcard/pcard/pcard_guide_no.html), computer equipment must not be purchased utilizing a University procurement card (Pcard) and individual personal purchases of computer equipment are not reimbursable as a personal expense.

Equipment Lifecycle

OU IT recommends that departments purchase, operate, and retire computer equipment within lifecycle limits documented on the Computer Standards List.

Departments may choose to extend the life of a computer past these recommended limits or down-cycle devices to use as a secondary computer for the original employee or for research laboratories, field applications, student employee equipment, etc. until the technology can no longer meet support, cybersecurity, or policy requirements, at which time the computer will be returned to OU IT for disposal as outlined below. The department and computer user are accountable for ensuring that down-cycled systems are sanitized to to comply with all University policies and to protect data and systems from unauthorized access.

Equipment Warranty

All computer equipment must be purchased with warranty and/or support options suitable for the device and intended business use so that the University reduces premature replacement costs.

System Disposal

All University-owned computer equipment must be returned to OU Information Technology at end-of-life using the appropriate campus-based retirement process to ensure proper disposal. OU IT will ensure that hard drives, data backup tapes, and any other storage devices are destroyed or wiped in compliance with Department of Defense (DoD) standards, either internally or through an approved third-party.

Policy Compliance

Any computer used for OU-related business is subject to all University and related-campus governing policies.

ENFORCEMENT AND COMPLIANCE

Failure to comply with this policy or other applicable laws, policies, and regulations may result in the limitation, suspension, or revocation of user privileges and may further subject the user to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, and applicable laws. This policy is approved by the University of Oklahoma President. This Policy is enforced by the OU Chief Information Officer. Internal Audit, or other departments, may periodically assess compliance with this policy and may report violations to the Board of Regents.

ASSOCIATED POLICIES, STANDARDS & DOCUMENTS

- OU Cybersecurity Policy
- OU IT Acceptable Use Policy

REFERENCES

- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI) Data Security Standards

- Gramm-Leach-Bliley Act (GLBA)
- Family Education Rights and Protection Act (FERPA)
- National Institute of Standards and Technology Special Publication 800-171, Controlled Unclassified Information
- National Institute of Standards and Technology Special Publication 800-37, Risk Management Framework
- National Institute of Standards and Technology Cybersecurity Framework

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
10/04/2018	1.0	Chris Jones, Jeralyn Woodall, Sharon Nichols, CISA, CRISC, CGEIT	Initial Draft
11/8/2018	1.02	Jeff McCanlies, Chris Jones, Dana, Saliba, Ron Nealis, Bryan Schuster, Chris Kobza, Nicholas Key, Jeralyn Woodall, Chance Grubb, Miranda Sowell	Cross-campus comments & needs added/removed
11/15/2018	1.03	Jeff McCanlies, Chris Jones, Dana, Saliba, Ron Nealis, Bryan Schuster, Chris Kobza, Nicholas Key	Updates based on campus leadership comments and additional feedback
11/15/2018	1.04	Jeff McCanlies, Chris Jones, Dana, Saliba, Ron Nealis, Bryan Schuster, Chris Kobza, Nicholas Key	Final draft updates
11/26/2018	1.04.1	Jeff McCanlies, Chris Jones, Dana, Saliba, Ron Nealis, Bryan Schuster, Chris Kobza, Nicholas Key	Added effective date, marked INTERIM
12/20/2018	1.04.2	Jeff McCanlies, Chris Jones, Dana, Saliba, Ron Nealis, Bryan Schuster, Chris Kobza, Nicholas Key	Added effective date, removed INTERIM, added clarification on peripherals
1/9/2019	1.04.3	Chris Jones, Chris Kobza, Dana Saliba, Nicholas Key	Updated language based on feedback from OUHSC ISRB
1/14/2019	1.04.4	Chris Jones, Chris Kobza, Dana Saliba, Nicholas Key	Integrated feedback from Legal Counsel
01/21/2021	2.0	Nicholas Key, CIO David Horton, Provost Jill Irvine	Integrated feedback from Provost-led faculty committee

Table 2 Approval History

Version	Approval Date	Approved by:
1.0	01/01/2019	University President
2.0	03/09/2021	Security Governance Advisory Council (SGAC) Information Security Review Board (ISRB)
2.0	03/23/2021	University President

Table 3 Review History

Version	Review Date	Reviewed by:
1.04.4	2nd Qtr 2020	Provost-led faculty committee