Draft Document.
10/30/26

Administrative Regulation — Information Technology Resources, Information Security and Privacy

I. Scope

This *Administrative Regulation* outlines the rules governing the use of technology resources, information security and privacy of resources provided by or through the University of Kentucky, including external resources facilitated or enabled by the University. This regulation applies to all individuals interacting with the University's technology resources, including students, faculty, staff, contractors, visitors and authorized third parties, regardless of where resources are accessed or located.

The President, through the Executive Vice President for Finance and Administration (EVPFA), delegates authority to the Enterprise Chief Information Officer (Enterprise CIO) to establish requirements for the access, appropriate use of University technology resources, security and other technology resource matters and to establish related policies to fulfill the requirements of this *Administrative Regulation*. The Enterprise CIO shall oversee and administer all technology resources used for University business or connected to University technology resources. This *Administrative Regulation* governs all University colleges, departments and affiliated corporations.

For additional information and policies, see Information Technology Services. For export control policies, see Security, Export, Compliance and University Research Engagement.

A. Definitions

1. "University technology resources" shall include all software, data, accounts, devices, licenses and networks owned, managed or facilitated by the University, including the use and access of University networks or data by personal devices.

2. "Cloud-based services" shall mean those data-control and sharing services in which data is typically distributed across multiple off-site servers, infrastructure or both. Typically, this service is by subscription with a third-party provider. University data stored within cloud-based services are still the property of the University.

II. University Technology Resources

A. Oversight of University Technology Resources

Information Technology Services (ITS) administers the procurement, management and terms of use for the voice system, University technology resources and networking infrastructure, including cloud infrastructure.

DRAFT

The Enterprise CIO establishes ITS processes for the selection and approval of all related procurements of hardware, software and cloud-based services. ITS will coordinate procurement activity with Procurement Services and will follow *Administrative Regulation — Contracting Authority, Procurement and Disposal of University Property and Other Delegated Authority*.

The Enterprise CIO is responsible for administering the University's technology resources, access to those resources and authorizing any computing systems used for University activity or connected to University technology resources.

The Enterprise CIO may create policies to evaluate the potential impact of new and emerging technologies on University operations including, but not limited to, artificial intelligence and ensure appropriate and responsible use and protection of University technology resources.

B. Access to University Technology Resources

University technology resources exist to support the work and mission of the University, and as such, its access is limited to those fulfilling that purpose. No student, faculty, staff, University retiree, contractor or their party has a legal right to access University technology resources. The Enterprise CIO will establish policies identifying authorized users, terms of use, issuance of accounts, methods of access, duration of access and access by other computing systems and artificial intelligence.

C. Limitations of Access and Use

As a publicly provided asset, access and use of technology resources has limitations and prohibitions. In addition to the parameters established in this *Administrative Regulation*, the Enterprise CIO may administer policies to include others. Authorized users must follow established policies for responsible and ethical use of technology resources. Failure to adhere to policies may result in termination of access to technology resources and/or disciplinary action under *Administrative Regulation — Employee Code*.

1. Prohibitions on Use of Technology Resources

University technology may only be used for authorized business. Users may not use University technology resources for political activity of any types, soliciting contributions, promoting a commercial product, operating a personal or private business, posting to non-University social media or engaging in substantial personal communications. Though discouraged, *de minimis* use of technology resources for personal matters by employees is permissible, but supervisors or the Enterprise CIO may set usage and storage limits. Failure to adhere to these prohibitions may result in termination of access to technology resources and/or disciplinary action as set out in *Administrative Regulation — Employee Code*.

DRAFT

2. No Expectation of Privacy

Authorized users do not have an expectation of privacy for the data and content of the University-owned computer and software assigned to them. The University may access the content or copy the content of such a computer at any time for any reason. The University may also demand the return of the University-owned computer and software at any time for any reason. Failure to cooperate with the University's directives concerning access or equipment may result in termination of access to technology resources and/or disciplinary action as set out in *Administrative Regulation — Employee Code*.

III. Cybersecurity and Data Security

A. Data Classification and Disclosure

The Enterprise CIO is authorized to categorize the types and sensitivity of data and establish compartmentalized access and usage rights.
Training and reporting requirements may be assigned based on level of access authority.

B. Incident Response

All users with access to University technology resources must report suspected security incidents to ITS. ITS is responsible for monitoring security incidents centrally and initiating responses under the promulgated Cybersecurity Incident Response Plan. Failure to report suspected security incidents requirements may result in termination of access to technology resources and/or disciplinary action as set out in *Administrative Regulation — Employee Code*.

C. Research and Export Control

The Enterprise CIO and Vice President for Research shall jointly administer the University's compliance with applicable export control laws and regulations, including requirements governing access to, use, disclosure, transfer or export of controlled technology, technical data, software, equipment and research information. The Enterprise CIO shall have primary responsibility for information technology security, access controls and protection of controlled technology and data within University technology resources. The Vice President for Research shall have primary, but not exclusive, responsibility for export control compliance associated with research activities, including the sharing or transfer of research information and materials, interactions with foreign persons and entities and applicable regulatory and reporting requirements.

DRAFT

Violation of applicable export control laws and regulations, including requirements governing access to, use, disclosure, transfer or export of controlled technology, technical data, software, equipment and research information may result in termination of access to technology resources and/or disciplinary action as set out in *Administrative Regulation — Employee Code*.

D. Enforcement

University technology resources are shared assets affecting the learning and work of the University. The Enterprise CIO is authorized to monitor and investigate improper use of resources, including data. Users are required to fully cooperate with any investigation. Failure to cooperate may result in termination of access to technology resources and/or disciplinary action as set out in *Administrative Regulation — Employee Code*.

The Enterprise CIO may also limit or regulate usage if a user's actions are deemed to negatively affect the learning or work of other University members.

The Enterprise CIO shall determine which actions undermine the security of the systems and data, and violations may result in termination of access to technology resources and/or disciplinary action as set out in *Administrative Regulation — Employee Code*.

DRAFT