Proposed Substitute

Administrative Regulation — Information Technology Resources, Information Security and Privacy

Draft of November 18, 2026

I. Scope and Principles

This Administrative Regulation governs the use, security and privacy of technology resources that the University owns, leases or operates. It applies to students, faculty, staff, contractors, visitors and authorized third parties who use those resources.

For the avoidance of doubt, this regulation does not govern services, platforms or forums that others operate, such as the discussion lists of scholarly and professional societies, publishers' and conference websites, and social media services, including when a user reaches them from a University account, device or network, or has access to them because of the user's University position or the University's membership in the organization that operates them. It does not govern the content of personally owned devices or accounts.

The President, through the Executive Vice President for Finance and Administration, delegates to the Enterprise Chief Information Officer (Enterprise CIO) authority to set technical, security, procurement and operational requirements for University technology resources, consistent with this regulation. That authority does not include restricting the content of communications, the personal use permitted by Section II.C.2 or the privacy protected by Section II.C.3. Any such restriction may be adopted only as Section V provides. Every decision under this regulation that limits a user's access, use or privacy, or that examines, copies or retains a user's files, is made in writing, names the provision on which it rests and states its reasons, and a copy is given to the user, except as Section II.C.4 permits notice to be delayed.

Academic freedom and free expression. The University does not wish to be the arbiter of the content of electronic communications. The First Amendment, Sections 1 and 8 of the Kentucky Constitution and the principles of academic freedom apply in full to the use of University technology resources. Like other citizens, faculty members, staff and students are free to engage in political activities, including through University technology resources. A student who lives in University housing may use the University network there for personal communications of every kind, including political activity, subject only to Section II.C.1 and the security requirements of Section III.D.1. The University does not restrict the content of a resident's communications more than this regulation restricts the content of any other user's communications. The University does not restrict communications over its technology resources because of their content or viewpoint, except as Section II.C.1 provides. For example, teaching, research, scholarship, and extramural and citizen speech through University technology resources may address any subject, including politics, religion and international affairs, and no provision of this regulation may be applied to restrict their subject matter or viewpoint. A communication does not become the University's speech, or speech made pursuant to a user's official duties, because it is made with a University account, device or network, and no disclaimer is required for it. This regulation is read consistently with the University's governing and administrative regulations on academic freedom and freedom of speech, and where they give users greater protection, they control.

A. Definitions

1. "University technology resources" means software, data, accounts, devices, licenses and networks that the University owns, leases or operates. A personally owned device or account is not a University technology resource, even when it connects to a University network. While connected, it is subject only to the network-security requirements of Section III.
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. A user's personal files stored in a University cloud account are not University data for purposes of this regulation. This regulation does not give the University ownership of any intellectual property. A faculty member's scholarly and creative works, including books, articles and course materials, and a user's personal files do not become University property or University data because they are created with, stored in or sent through University technology resources.
3. "Personal files" means files and communications that a user creates, receives or keeps for personal, family, extramural or citizen purposes, as distinguished from records of University business. A faculty member's scholarly and teaching materials in progress receive the same protection as personal files. A file is not a record of University business merely because it is stored on a University technology resource.
4. "University distribution lists" means email lists that the University generates from its records to reach all students, all employees, or all members of a University-wide category such as all faculty or all staff. Lists of a college's or department's faculty, faculty listservs, subscription lists, and discussion groups that members may join or leave are not University distribution lists.
5. "Official University accounts" means websites and social media or email accounts that speak for the University or one of its units, such as a college's social media account. A user's individual University email account is not an official University account.
6. "Technology Rights Review Committee" means the committee established by Section IV.

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.

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 the security and protection of University technology resources.

Procurement and approval processes under this section are limited to security, legal, accessibility, data-protection and contractual requirements. They must be published and must provide decisions within a stated time. They may not be used to restrict the subject matter, methods or tools of teaching or research, including the use of artificial intelligence in teaching and research.

B. Access to University Technology Resources

University technology resources support teaching, research, scholarship, service, patient care and the work of the University, and they are also open to the expression, communication among colleagues and incidental personal use that this regulation protects. Faculty, staff and students receive the access that their teaching, research, study, service and work require, and that access may be limited or withdrawn only as Sections II.C and III.D provide. The Enterprise CIO will establish policies on accounts, authentication, and the methods and duration of access, consistent with this regulation.

C. Use, Privacy and Access

1. **Prohibited uses.** Users may not use University technology resources to:
   (a) violate federal, state or local law;
   (b) advocate for or against a public question on the ballot, to the extent KRS 48.025 prohibits;
   (c) use University distribution lists or official University accounts to support or oppose a candidate for public office, or solicit contributions for a candidate, party or political committee;
   (d) operate a business or promote a commercial product or service for private gain, except as another regulation permits, including consulting and other professional work approved under the University's rules on consulting and overload employment, and licensing, commercialization and start-up activity conducted under the University's intellectual property regulations. Sharing research results, software and scholarly works with industry collaborators or the public is not the promotion of a commercial product;
   (e) send commercial electronic mail in bulk, or post to a University distribution list without the posting permission the list provides (the University assigns posting permission by office or role, publishes who holds it, and never grants or withholds it because of a message's content or viewpoint);

(f) forge or falsify the sender, header or routing information of a message, or impersonate another person with intent to deceive;

(g) use another's credentials, gain access without authorization, circumvent security measures, introduce malicious software, or intentionally disrupt or degrade the technical operation of University systems, as by a denial-of-service attack; or

(h) infringe a copyright or software license.

No other prohibition applies to the content of communications. Expression protected by the First Amendment, Sections 1 and 8 of the Kentucky Constitution or academic freedom does not violate item 1, and an allegation that a communication constitutes harassment is not a ground for access under Section II.C.4 unless the communication is alleged to be directed at a particular person and to be so severe, pervasive and objectively offensive that it denies equal access to education or employment. Teaching, research and scholarship about candidates, parties and ballot questions, and the dissemination of their results, are not barred by items 2 and 3. Users may, among other things, communicate on any subject, including politics, religion and international affairs; post to personal social media and to outside websites, forums, listservs and discussion groups; take part in the forums of scholarly and professional societies; and circulate their own writings to colleagues, from University accounts, devices and networks.

2. **Personal use.** Incidental personal use is an accepted and appropriate benefit of being associated with the University's technology environment, and it benefits the University by allowing users to avoid needless inconvenience. It is permitted so long as it does not interfere with the operation of University technology resources, interfere with the user's duties, or impose a noticeable incremental cost on the University. A supervisor may limit a particular use only in writing, stating which of those conditions the use does not meet, and the user may seek review under Section III.D.4. Personal use may not be limited as a sanction, during an investigation, or because of the content or viewpoint of the user's communications. Direct costs of personal use, such as printing supplies, are borne by the user.

3. **Privacy.** The University respects the privacy of electronic files and communications in the same way that it respects the privacy of paper correspondence and telephone conversations. The protections of this regulation for communications, including Sections II.C.4 and III.D.1, apply equally to telephone calls, voicemail and text messages carried by the University voice system or a University network. Users have a reasonable expectation of privacy in their personal files, including personal files on University devices and in University accounts. The University does not examine or disclose the content of a user's files or communications without the user's consent, except as Section II.C.4 provides. The University claims no ownership of or property interest in a user's personal files. Personal files are not records of University business, and they are not public records under KRS 61.870(2) unless the University prepares, owns, uses, possesses or retains them as a public agency; even then, their disclosure would be a clearly unwarranted invasion of personal privacy under KRS 61.878(1)(a). If the University receives a request under the Kentucky Open Records Act that it believes reaches a user's file, it will notify the user before responding, will not disclose a personal file, and will assert every applicable exemption, including KRS 61.878(1)(a).

4. **Access without consent.**

(a) *Grounds.* The University may examine the content of a user's files or communications without consent only when a statute, warrant, subpoena or court order specifically requires access to the particular files; when there is substantiated reason, meaning reliable evidence as distinguished from rumor, gossip or other unreliable evidence, to believe that the user has violated law or Section II.C.1 and access is necessary to investigate it; when failure to act might result in significant bodily harm, significant property loss or damage, or a compromise of the security of University systems; when the user is unavailable because of death, incapacity or separation and access is needed to continue University business; or when the University must search a University account for public records, as KRS 61.870(2) defines them, to respond to a request under the Kentucky Open Records Act, a litigation hold or an obligation to produce documents in litigation. A search for public records is limited to records responsive to the request, hold or obligation; the University first gives the user notice and a chance to identify personal files; and personal files are excluded. Access may never be used to investigate or sanction a communication that Section II.C.1 permits.

(b) *Authorization.* Access must be authorized in advance and in writing by two officials. For faculty, they are the Provost and the dean of the faculty member's college; for staff, the Executive Vice President for Finance and Administration and the head of the employing unit; for students, the Vice President for Student Success and the Dean of Students. This authority may not be delegated. An official who is a complainant, witness, investigator, decision-maker, adviser or counsel to the University, or party to litigation in a matter involving the user, or who has publicly characterized the user's expression or taken part in the decision to investigate it, may not authorize access or appoint an alternate. The Technology Rights Review Committee names the alternate and decides any dispute over disqualification. The authorization must state the ground, the facts that support it, the files to be examined, and why a less intrusive means will not serve, and must weigh the need for access against academic freedom and personal privacy.

(c) *Emergencies.* In the emergencies described in item 1, the University may act at once, taking the least action necessary, and must obtain written authorization within two business days.

(d) *Scope.* Access is limited to the least perusal of contents and the least action necessary. Metadata is examined before content where it will serve. Review is limited to the dates and subjects stated in the authorization. Personal files are excluded unless the authorization specifically finds that a particular personal file is necessary. Information obtained may be used only for the purpose authorized. Copies are limited to the authorized records. They are duplicates of records kept elsewhere and are destroyed when the authorized purpose ends, unless a litigation hold or law requires that they be kept, and the user is told in writing what was copied, who reviewed it and when it was destroyed.

(e) *Notice.* The University will notify the user before access, in time for the user to seek protection, unless a court order forbids notice or delay would create an

imminent risk to human safety or University property, in which case notice will be given as soon as the risk passes. The notice will include the authorization and its reasons. Before releasing information in response to legal process, the University will notify the user.

(f) *Records and oversight.* Each authorization is recorded. A de-identified annual report of all access without consent is given to the Faculty Senate and published.

5. **University-owned devices.** The University may require the return of a University-owned device only at separation, for scheduled replacement, repair or upgrade, or when access to its contents is authorized under Section II.C.4 and a copy of the authorized records will not serve. Before return, the user may copy and remove personal files. When a device is needed under Section II.C.4, the user may first copy all personal files, and personal files are then excluded from review; any dispute over whether a file is personal is resolved under Section III.D.4 before the file is examined. The University will make a record of anything copied or removed and give the user a copy. It will image only the authorized records and return the original device to the user within ten business days, unless the user consents or a court orders otherwise. A replacement device does not substitute for return. A user who asserts privacy in good faith, or asks that a dispute be resolved before access, does not thereby fail to cooperate.
6. **Personally owned devices and accounts.** The University does not search a personally owned device or account. A record on a personally owned device or account is a public record only if KRS 61.870 makes it one. When a request under the Kentucky Open Records Act, a litigation hold or legal process reaches such a record, the University asks the user to search for and provide responsive records, and it does not otherwise access the device or account except with the user's consent or under a court order.
7. **Records retention.** Public records kept on University technology resources are retained and disposed of as KRS Chapter 171 and the State University Model Records Retention Schedule require. Personal files are not subject to the schedule, and the University keeps no copy of them except as Section II.C.4 permits.

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.

Research and contract-controlled data. Data that the University or a user holds under a law, a sponsored award, a non-disclosure agreement, a cooperative research and development agreement, a data use agreement, or a requirement for controlled unclassified or export-controlled information is handled as that law or agreement requires. Classification under this section may not lower the protection that law, contract or another University regulation gives such data. Access is limited to the persons the law or agreement authorizes and to the least access their work requires. No one may copy, image, monitor or examine such data, including under Section II.C.4 or Section III.D, without the written authorization of the principal investigator or

other responsible custodian, unless a law, a court order or the agreement itself requires otherwise, and then only by persons the law or agreement permits to see the data and only to the extent it requires. Any copy is a duplicate of data kept elsewhere and is destroyed when the authorized purpose ends, unless a litigation hold or law requires that it be kept, and the custodian is told in writing what was copied, who saw it and when it was destroyed. If the University believes such data is at risk, it works with the custodian and the sponsor to protect it.

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 may result in termination of access to technology resources and/or disciplinary action as set out in Section III.D.4.

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.

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 Section III.D.4.

Export control compliance under this section does not extend to information that arises during or results from fundamental research, or to information that is published or in the public domain, which federal law excludes from export controls. 15 C.F.R. §§ 734.3(b)(3), 734.7, 734.8; 22 C.F.R. § 120.34. The University will not monitor or restrict users' communications with foreign colleagues about such research or information.

D. Monitoring and Enforcement

1. *Systems monitoring.* ITS may monitor University technology resources for security and system performance using automated tools and aggregate or non-content data. ITS staff may not seek out the content of communications, or transactional information about particular users, when it is not germane to system operations, and may not search content for violations of law or policy except under Section II.C.4. No University unit that sends communications to students, faculty or staff may collect or receive information showing whether, when or where a particular recipient opened a communication or followed a link

in the communication, whether through tracking images, tracking links or similar means. Such units may use counts that do not identify individual recipients. No information about whether, when or where a person read a University communication may be used in any personnel, disciplinary or investigative matter. Monitoring beyond this paragraph is itself a violation of this regulation. The University will not require a user to install monitoring, management, remote-access or content-inspection software on a personally owned device, or to give the University access to the contents of a personally owned device or account, as a condition of connecting to a University network or using University technology resources. Network-security requirements for personally owned devices are limited to authentication, current security updates and protection against malicious software that does not give the University access to content. Where the security of particular data or systems requires device controls, the University will supply a University-owned device for that work at no cost to the user.

2. *Investigations.* An investigation of an alleged violation of Section II.C.1 proceeds under Section II.C.4. A user who has notice of an investigation must preserve relevant data. No user is required to waive privacy in personal files, any privilege, or any constitutional right. Investigations proceed in compliance with the laws protecting the privacy of the records and data involved.

3. *Security holds.* The Enterprise CIO may suspend an account's or device's access only to stop a specific, ongoing threat to the security or functioning of University systems, for no longer than necessary and for no more than 72 hours; any extension requires a written decision describing the threat, is limited to seven days, and may be renewed only by the Technology Rights Review Committee. The user will be notified as soon as practicable. A hold may not be imposed because of the content of a communication.

4. *Limits on access and review.*

   (a) *Discipline.* Limiting a user's access to University technology resources as discipline is a severe sanction. It may be imposed only through the hearing procedures that the University uses for its most serious sanctions, such as termination of employment or expulsion, against members of the user's constituency (faculty, staff or students). It may not take effect until that hearing has ended in a decision imposing it.

   (b) *The user's choice of Committee review.* A user charged under paragraph (a) may choose to have the charge decided by the Technology Rights Review Committee instead. The user makes this choice in writing before the hearing begins. If the user makes this choice, the Committee decides whether the user violated this regulation and whether the limit is warranted, and the limit may not take effect unless the Committee imposes it. This choice covers only the limit on access. Any other sanction sought for the same conduct stays subject to the procedures that apply to that sanction.

   (c) *Protected conduct.* Conduct that this regulation permits, including expression protected under Section I, is not a ground for discipline. No user may be disciplined for conduct that this regulation permitted when it occurred.

(d) *Limits not imposed as discipline.* A limit on access imposed for a reason other than discipline requires written notice to the user. The notice must name the provision of this regulation on which the limit rests, and the user must have a chance to respond. If the user asks the Committee to review the limit before it takes effect, the limit does not take effect until the Committee decides. This paragraph does not apply to a security hold, which is governed by Section III.D.3.

(e) *Review of other decisions.* A user may ask the Committee to review any limit on personal use, security hold, device demand or access decision that affects the user.

(f) *Timing.* The Committee decides a request under paragraph (d) or (e) within ten business days after receiving it.

IV. Technology Rights Review Committee

The Technology Rights Review Committee decides the matters that this regulation assigns to it.

Membership. The Committee consists of eleven members: five faculty members chosen by the Faculty Senate, three staff members chosen by the Staff Senate, and three students chosen by the Student Government Association. No employee of Information Technology Services, the Office of Legal Counsel or the Office of Equal Opportunity, and no administrator with authority over technology resources, investigations or discipline, may serve. Faculty and staff members serve staggered three-year terms, and student members serve one-year terms. The Committee elects its chair from among its faculty members. No member may serve at the same time on the University's information technology advisory council.

Panels. A matter concerning a particular user is heard by a panel of three members drawn from the user's own constituency—faculty for faculty, staff for staff and students for students—named by the chair. Other matters are decided by the full Committee. A member who would be disqualified under Section II.C.4 may not take part, and the chair names a replacement from the same constituency.

Decisions. The Committee decides by majority vote, in writing, with reasons. Its decision is final.

Support and reporting. The University provides the Committee with staff support. Each year the Committee reports to the three senates and the University's information technology advisory council the number of access authorizations, security holds, device demands and reviews, and their outcomes, without identifying any user. The Committee may recommend changes to this regulation and to implementing policies to the Enterprise CIO, the advisory council and the three senates.

V. Implementing Policies

Policies, standards and procedures under this regulation are limited to technical, security, procurement and operational matters, and are published. A rule that would restrict the content of communications, personal use or privacy beyond this regulation, or add a prohibition, may be adopted only as an administrative regulation, through the University's procedure for adopting administrative regulations, after the draft has been posted for campus comment for at least thirty

days, after the Faculty Senate, the Staff Senate and the Student Government Association have each had at least thirty days to give their advice, and never on an interim basis. Every other policy, standard or procedure under this regulation is adopted only after the University's information technology advisory council has reviewed it and the Faculty Senate, the Staff Senate and the Student Government Association have each had at least thirty days to give their advice, except that a change needed to meet an immediate and serious threat to the security of University systems may take effect at once if the Enterprise CIO states the threat in writing. Such a change is temporary. It must be withdrawn once the risk is mitigated, and it lapses after thirty days unless, within that time, the advisory council has reviewed it and the three senates have had the opportunity to give their advice. The faculty members of the advisory council are nominated by the Faculty Senate, its staff members by the Staff Senate and its student members by the Student Government Association.

VI. Effective Date and Transition

This regulation replaces Administrative Regulation 10:1 and applies to conduct after its effective date. It does not repeal the University's regulations on the security of data and of information technology resources, which remain in force to the extent consistent with this regulation; where they give users or their data greater protection, they control. No provision of this regulation, and no change it makes, may be applied to conduct before that date, or in a pending matter, to a user's detriment. No charge, finding or sanction may rest on any use of University technology resources that this regulation permits, whenever the use occurred. Adoption of this regulation does not ratify or validate any action, directive or investigation taken under AR 10:1 or any predecessor rule. Any limit on a user's personal use, and any retention of a user's device, imposed before the effective date that this regulation would not permit ends on that date.