THE
UNIVERSITY
OF RHODE ISLAND

Community Comments Previously Submitted Regarding an Approved Administrative Policy

Policy on IT Data, Systems, and Services (07.105.1)

The University of Rhode Island's *Policy on IT Data, Systems, and Services* (07.105.1) was approved with an effective date of August 21, 2026. Prior to approval, A multi-phase stakeholder review was conducted from February 17th through April 7th, 2026, and the draft policy was made available for community comments from April 16 through April 30, 2026. Below are the comments submitted, together with responses that may be provided in whole or in part by the policy owner, the Administrative Policy Committee (APC), and/or policy development staff.

Substantive edits were made in response to these community comments and additional OGC review, and a supplemental stakeholder review with 44 invited participants was conducted from June 4th through June 23rd, 2026. Feedback received during the supplemental review period was then reviewed and discussed in collaboration with several respondents, resulting in further edits. As a result of this extended participatory process, some edits referenced here in response to community comment may not match language in the final draft as approved.

Prior community comments and corresponding responses relating to approved administrative policies are posted for 30 days following approval on the University's Administrative Policy Development web page (https://web.uri.edu/policies/administrative-development/). Following this posting period, submitted comments remain available upon request by contacting policies-group@uri.edu.

Comment #	Respondent's Capacity	Community Comment	Response
1	Staff	With regard to applicability: "This policy applies to all individuals who are granted access to interact with University IT Resources, including, but not limited to all faculty, staff, students, and University Affiliates." While implied, it should be more clearly specified that, "[...] including, but not limited to [...]", governs guests, visitors, parents or other users of generally public resources, if intended. The word "guest" only appears under section III. A. on Endpoint Protection; the word "visitor" does not appear. Examples of generally public resources: guest WiFi, Library terminals, public kiosks, Campus Recreation, etc... Additional clarity should be included if this draft applies to non-formal affiliates of the University. This might include individuals employed by organizations to which the University has had long-standing service agreements, but are not registered individually as University Affiliates. Examples: Kingston Fire Department, The Ryan Center, Inner Space Center, RI Nuclear Sciences Center. Only URI FAE is mentioned under the definition of University Affiliate, to include	We consider "All individuals who are granted access to interact with University IT Resources" to be sufficiently inclusive.

		all employees. Again, the observation made above implicitly includes them, but a mention of organizations to which the University provides a service would be preferable.	
2	Faculty	No concerns.	Thank you for your feedback.
3	Staff	This feedback is submitted from the Office of Strategic Procurement, Contracts Management perspective. COHERENCE 1. Governing authorities: The policy's governing list omits the Contracts Policy (Policy on Approval and Execution of Contracts) and the URI Board of Trustees Procurement Regulations – both directly relevant. The Contracts Policy is cited in §I.E.5 as governing EULAs, and the Procurement Regulations govern IT procurement and contain accessibility requirements at §13.22(A)(10). 2. "Contract Owners" (§II.B.1): "Contract Owner" is a defined term in the Contracts Policy. If this policy intends to invoke that role, the term should be capitalized with a cross-reference to that policy's §3.8. As written, it risks implying obligations are limited to data ownership rights. 3. Insurance: The Procurement Regulations and GC Addendum A establish insurance requirements for IT contracts. A cross-reference to Addendum A and the ERM review process would ensure readers know these requirements apply. COMPLETENESS 4. System inventories (§II.A): The policy requires Administrators to maintain inventories but sets no standards for how they are kept or whether they must be available to ITS upon request. The policy should establish minimum documentation requirements, confirm inventories are available to ITS upon request, and work toward a centralized inventory as the longer-term goal. 5. Connecting procurement and compliance review: The Procedures accompanying the Contracts Policy already identify ITS as a required reviewer for IT contracts and point to its.uri.edu/services/it-contract-review. Acknowledging this would help users understand how these processes connect. It is also worth asking whether the policy should address who evaluates whether a proposed system is the right fit (distinct from security and contract review) as that question has no defined owner. 6. "Approved Services List" (§I.E.5): The policy references an Approved Services List but does not explain what it is or how a	1. The *Board of Trustees Procurement Regulations* and the *Policy on Approval and Execution of Contracts and Other Binding Documents* have been added to the table. 2. Contract Owner is not a defined term in this policy, so we would not capitalize it here. As the content here narrowly addresses University ownership of data, a cross-reference to content on contract approval is not deemed necessary. We are assessing whether to add a reference to the insurance requirements. In any event, items 3-6 will be addressed in procedures accompanying this policy. 7. A separate Policy on Accessibility is currently in development. 8. Generative AI contracts must follow the same review requirements as other contracts. 9.We will consult with general counsel, and if advised to do so we'll insert concise compliance content as appropriate. 10. ITS will make URI Data Classification Schema and Guidelines - 20240424.docx a public web page. It is currently discoverable.

		service gets on it. A service on our existing registry has completed a security and accessibility documentation review (it has not been approved for use). Departmental, supervisory, and contract approvals are still required. Describing the list as "approved" risks implying listed services are cleared for any purpose, which is not the case. 7. Accessibility – two separate obligations: A vendor's VPAT covers the product. It does not cover URI's responsibility to ensure that content faculty and staff create and publish through that system is itself accessible. The policy's references in §§IV and V do not distinguish between these two things. Product accessibility review is required during IT contract review due to Procurement Regulations §13.22(A)(10); content accessibility is better addressed through the Office of External Relations and Communications, in coordination with ADA Title II requirements. 8. Generative AI: The policy's prohibition on unapproved services would cover generative AI tools but does not say so explicitly. Contracts involving AI-enabled services also carry elevated risk – data use rights, training data, IP ownership, and liability terms are all evolving. Any contract involving AI capabilities should require IT Contract Manager review, even where it would otherwise qualify for self-review under the Contracts Policy. Is a dedicated AI policy forthcoming? 9. Federally prohibited vendors: The NDAA §889 prohibition on certain telecommunications and video surveillance equipment applies broadly to IT hardware and services but is not referenced. Requiring confirmation of §889 compliance before procuring IT equipment would be a useful addition. CLARITY 10. Data Classification Schema: Referenced as operative but does not appear to be publicly available, with no defined process for when classification is required. Guidance on when it is expected (for example, at the point of IT procurement) and where it is documented would help.	
4	Faculty	I am commenting on this both as a faculty member (in Mathematics) and also current chair of my department's Technology Committee. My biggest issue is with part D. of Section I. on Responsible and Acceptable Use. At the bottom of page 6, it states `Individual user storage locations are not appropriate systems of record for such materials, even when those locations are provided by the University. This includes, but is not limited to, folders or files stored in an individual User's University-provided Google Drive, OneDrive, Box,	As a result of this and other submitted comments, Section I.D. was substantially modified for clarity to read: *University Records and operationally essential documents must be stored in University-approved, centrally managed repositories that are institutionally owned and governed by a department, role, or shared University*

		email account, or similar service that is tied to a single person rather than a department, role, or shared function.' I would suggest that this needs modification, particularly not allowing the use of `an individual User's University-provided Google Drive' or `email account'. This would make it very difficult to exchange relevant information either between computers (e.g. for accessing material from a computer at one's home) or with others directly connected with one's activities as a faculty member such as department colleagues or a grader for a course. The paragraph above this does mention `University-approved, shared, or centrally managed repositories designated for that purpose', but it is not specified what these are, and it is difficult to imagine even what they might be in practice. The above also seems to be at variance with point 7. of E. on Confidentiality and Security of Data where it says `If University Data is created or stored on a User's personal computer or other device, or in databases that are not part of the University's IT Resources....'. which appears to acknowledge that we can use our own devices to store university data. If this is indeed allowed, then how is one supposed to transfer these data from a university computer to one's own machine? The sentiment expressed in the sentence at the start of page 7`If it lives in one person's account, it is not an acceptable system of record, even if the service is University-provided.' is rather general and sweeping. While I understand the need for redundancy and access in case of emergency, in practice, this could be very inconvenient to implement, for example with files (such as LaTEX source code) relating to exams which are not the exams themselves and would not be posted on Brightspace. A further objection concerns part E. of Section 1. where in the second paragraph it states `Users are prohibited from using any unapproved third-party application, platform, service, or tool (no matter how obtained) to create, store, transmit, process, or handle Confidential and/or Restricted data.'. The question is just what is approved and what is not - are emails alright, are paper exams legitimate, is even Brightspace an acceptable place to store and exchange confidential university data? In point 4. of part E. of Section 1. it states `All computers connecting to the University's network must run security software prescribed by the Chief Information Security Officer (CISO) to properly secure University IT resources.' Again, this seems superficially reasonable, but what software is this in practice? Overall, to summarize this document and what needs to be changed, I would go with what one of my colleagues said which was that a lot	*function, not in a location tied to a single individual user account. This includes, but is not limited to, materials such as:* *1. Administrative and operational documents (e.g., procedures, reports, planning materials).* *2. Financial records and supporting documentation (e.g., budgets, invoices, procurement records).* *3. Student, employee, or research-related records subject to institutional oversight.* *4. Compliance, legal, or audit-related materials.* *5. Communications or documentation that support official decisions or University business activities.* *6. Any records subject to retention requirements under University policy or applicable law.* *Locations tied to a single user account are not acceptable systems of record for University materials, even when the account is University-provided and even when folders or files are shared with others. This includes, for example, content stored in "My Drive," OneDrive, Box, or email accounts associated with an individual user.* *Shared access does not equal institutional custody. If materials reside in an individual's account, their availability, integrity, and continuity remain dependent on that account and may become inaccessible or deleted due to role changes, account deactivation, or separation from the University.* *To meet this requirement, materials must be stored in repositories that are assigned to and governed by a department, program, or shared University function, and not to an individual user account. Examples include Microsoft Teams or SharePoint sites with organizational ownership, Google Shared Drives (not "My Drive"), or other University-designated systems of record.* To the first paragraph of Section I.E., we inserted for additional clarity: *University-provided and University-managed services (e.g., University email, learning management systems, and other institutionally supported platforms) are considered approved for use in accordance*

		of things which appeared reasonable and which we all do were apparently being prohibited while no information was being given of what alternatives would be provided. As a concrete suggestion, I would say that not allowing one's university Google Drive to be used to exchange information is not reasonable. Of course there should be restrictions, such as for the most sensitive data for the university or those connected with it, but not for routine files relating to running a course. IT security guidelines should enhance the university's mission, not impede it, and an important part of this is allowing faculty to pursue their normal activities of teaching, research, and service without oversight or interference.	*with their intended purpose and applicable data-handling requirements.* Regarding section I.E.4, we can address that in procedures.
5	Faculty	I have numerous concerns. D. Storage of University Records and Operational Documents: specifically the language that even the URI-provided Google Drive may not be used to store documents suggests that (though it's never stated) we should be storing all documents on a shared drive. This seems odd and punitive. For instance, if I'm drafting a letter providing a concern or complaint about a colleague, or writing an annual review, I do not want incomplete, unrevised *drafts* of those to be visible to other faculty who might be subject to the review. Secondly, what about things that can't be done in Google Drive? I and many colleagues use LaTeX to write manuscripts, letters, and update our CVs. Some use Overleaf, some prefer to work remotely in a text editor and (depending on the document) share it via Github. We simply *cannot* do our jobs if we're expected to do everything in GDrive. Thirdly, what about things like benchmarking or actively developing software (including testing)? I can't write, compile, test, and benchmark my research software using GDrive. It's just not possible. Also I may often need to do this on my laptop, as well as departmental or Unity compute servers. This entire policy is written like it expects all faculty to do everything in Office or Google Docs. We don't. We can't. 3. Data Storage and Encryption: Confidential University Data must be stored on centrally managed or contracted IT Resources, not on local hard drives or portable devices, unless prohibited by law or binding agreement. This is unworkable, because I often need the speed of my local machine (and its very fast SSD drive) to quickly iterate on software and computational experiments. Again, I write software.	As a result of this and other submitted comments, section I.D. and section I.E. were modified for clarity as detailed in the response to submission #4 above. Section I.E.3 was modified to read: *Confidential University Data must be stored on centrally managed or contracted IT Resources as the authoritative system of record. Unless prohibited by law or binding agreement, such data may be accessed and temporarily stored on endpoint devices solely for active use, provided that the device meets University-defined security requirements and that the data is not maintained solely on the device but remains stored in an approved institutional repository.* The following paragraph was inserted into section II.F. to address this concern: *Systems that implement privilege elevation mechanisms (e.g., sudo) on individual endpoint devices may satisfy this requirement without separate privileged accounts, provided that such systems are used by a single user, do not store or process Restricted data, do not provide administrative access to sensitive University systems or infrastructure, and maintain logging and attribution for actions taken with elevated privileges.* The following paragraph was inserted into section II.G.1 to address this concern: *Systems that cannot implement University-required anti-virus, security, or monitoring software because those controls would materially interfere with legitimate research or instructional requirements must have a*

		F. Privileged access to Systems must be restricted to the smallest practical number of individuals In my research (and my teaching) I routinely need command-line admin access (sudo). Not occasionally. Not temporarily. The "admin by request" feature doesn't even work for this. This needs to be re-thought. Privileged accounts must not be used for non-privileged activities. This is also unworkable. I need routine privilege escalation to run performance profiling tools on Linux and macOS -- on code I'm developing as a user. G. Administrators must 1. Install Approved Software: Ensure all Systems have the necessary University-approved anti-virus, security, and monitoring software installed. This is problematic on some research systems. Some antivirus tools are highly invasive and consume significant resources, leading to inaccurate and inconsistent benchmarking. I can't do my research on a system that isn't "quiet".	*documented exception approved in accordance with the Exceptions section of this policy, must operate within an approved restricted network environment or secure enclave, must not store or process Confidential or Restricted data, and may store or process Internal data only when justified in the documented exception.*
6	Graduate Student & Instructor of Record	This policy seems to suggest that personally owned devices are subject to university provided "monitoring software" and / or remote wiping? Does this mean URI can remotely wipe personal phones? (section III.D) If the above is an accurate summary of the proposed policy, will the University be required to provide alternative devices for system access to all employees (including graduate students who are instructors of record)? This policy should make clear that the University is required to offer University owned devices to all persons impacted by this policy (including students and graduate instructors). Can the limitations of forwarding university emails please be clarified? Section IV suggests that forwarding any university emails is prohibited. I would urge the committee to extend the period of consideration for this policy and postpone adoption until the Fall semester. This draft policy was released late in the semester and many instructors and graduate students have not had time to adequately review the implications of these proposed changes.	Section III.D. states: *Personal devices used for University business must allow the User to remotely wipe all data in the event the device is lost, stolen, or compromised.* For clarification, this requires that the device used for University business has the capability to be remotely wiped by the user under the circumstances listed, and does not authorize the University to wipe a user's personal (non-University-owned) devices. Prior to the community comment period, dozens of stakeholders were invited to review the policy draft, including the GSA Executive Council.