Boulder Faculty Assembly

UNIVERSITY OF COLORADO **BOULDER**

Faculty Working Group on IT Security Standards

Benjamin Brown
Jed Brown (co-chair)
Ellen Burnes
Amber Kelsie
Robert MacCurdy
Christopher Osborn
Valerie Otero
Markus J. Pflaum (co-chair)

September 15, 2025

Preliminary Report on Secure Computing Standards and Academic Freedom

Executive Summary

The BFA Faculty Working Group on IT Security Standards (IT-FWG) was formed in Spring 2025 and tasked with understanding the IT standards and their potential unforeseen impacts, addressing faculty concerns, and providing feedback to CU Boulder leadership. The focus of this work has been the Secure Computing Standard for Computers (SCSC), which was published in 2022 and has a target for mandatory compliance of October 2025. The IT-FWG finds that the SCSC was created with insufficient faculty involvement and fails to meet the needs of CU Boulder's diverse research and educational activities. The requirements are overly prescriptive and the exemption process is inadequate, ill-defined, and represents an undue burden. Moreover, the requirements have severe privacy implications that infringe First Amendment rights and academic freedom, which Regent Law requires the University administration to protect. The IT-FWG calls for the SCSC to be revised with specific attention to research and educational needs and to protecting privacy and academic freedom from a range of threats, both internal and external. The revised policy should be designed to be responsive to a broad range of foreseen and unforeseen use cases as a matter of comprehensive strategy rather than a proliferation of exceptions. The IT-FWG calls for faculty representation in the decision-making process and for education so that faculty can better understand the internal and collective implications of security choices and so that OIT can better understand academic freedom and the diverse needs of the research and educational mission.

Boulder Faculty Assembly (BFA)
Norlin Library E138 - UCB 184
Boulder, CO 80309

303-492-6271
https://www.colorado.edu/bfa

1 Introduction

The IT Security Challenge We Face: The CU Boulder campus is confronted with an array of information security threats that have increased in pace and severity over time. Campus leadership tasked the Office of Information Technology (OIT) to address these threats, and one of the strategies was a set of proposed standards that were published in the Secure Computing Standard for Computers (SCSC) policy. The SCSC was published in July 2022, the deadline for installation of Defender for Endpoint on all university-owned computers and for all campus servers was June 2024. The target date for all campus university-owned computers to be compliant with the SCSC is October 2025. Exception criteria, while promised to be delivered by OIT, have still not been defined. The publication and subsequent initial implementation of the SCSC prompted questions from faculty across campus, and in response the BFA Executive Committee formed the Faculty Working Group on IT Security Standards (IT-FWG) in Spring 2025. The IT-FWG is tasked with understanding the IT standards and their potential unforeseen impacts, addressing faculty concerns, and providing feedback to CU Boulder leadership. The present standard for secure computing [Vic22] has been determined by the Office of the Vice Chancellor for IT in 2022 and is stated below:

> The following IT capabilities must be met to ensure consistent application of protections and adherence to the CU baseline security standards, provide visibility into campus threats, and support incident response. At all times university computers must:
>
> 1. Run current, supported software. The use of out-of-date operating systems or software that is not being actively updated and is 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.
> 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 central inventory for vulnerability tracking, network identification, and audit preparedness.
> 6. Use OIT supported and approved enterprise cloud storage solutions to back up and protect University data from loss.
> 7. Have the campus public safety emergency notification client installed to ensure timely awareness of campus incidents.

Exemptions from the standard require a “compelling business reason” and approval by the “Provost and Chief Operating Officer in consultation with the VC/CIO”.

1.1 Implications

For each of the requirements above, we highlight implications of relevance to this report. See section 7 for further details.

1. This is a best practice (a standard professional procedure that should serve as a default). A commonly-needed exception is for vendor-provided lab computers running proprietary software, such as to operate microscopes. In some cases, vendors no longer exist, or upgrading the computer would require replacing other physical devices. Reproducing experiments may require running unsupported software. Open source software tools, which are commonly used in research activities across campus, rely on software that provides no warranty, including active maintenance.

2. Endpoint Management Software (EMS) is a serious invasion of privacy and increases the scope of trusted service infrastructure, which are often targeted by attackers [Man25].

3. This is a best practice, especially for devices that do not have high physical security, such as laptops. However, it can be a severe performance impact for video editing and data-intensive computing, especially with parallel file systems.

4. Endpoint Detection and Response (EDR) software is privileged software (like a kernel module) that records full URLs as well as metadata about processes and files. Note that full URLs may encode search queries and tracking information, identifying not just scholarly literature that a researcher accesses, but also the intellectual process by which those materials were found. These records are automatically transmitted to third-party servers with privacy policies that permit disclosing for various purposes including government requests. This represents persistent surveillance that will be a recurring subject of this report. EDR is frequently evaded by advanced threat actors and EDR admin consoles are targets for exploits [Man25].

5. Some units and research groups operate hundreds of computers, sometimes with configurations that change continually, for educational and research purposes, and thus scalable policies that avoid burdensome overhead are necessary.

6. This currently requires Microsoft OneDrive, which has performance, security, privacy, and accessibility/language support issues for some purposes. The mandate also implies an unfounded assumption that all data on a device is University data, to which the University should maintain access and assert control.

7. This alert software has interrupted presentations and crashed machines, even while on travel. This is inappropriate and reflects poorly on the researcher and institution, as well as being a potential security vulnerability.

The SCSC articulates a narrow view of computer use on campus that frequently conflicts with the university mission, yet the exception process is unreasonably onerous and does not define criteria.

2 Academic freedom with security

The foundational mission of the University, as articulated in Regent Law Article 1.B is: "The University of Colorado is a public research university with multiple campuses serving Colorado, the nation, and the world through leadership in high-quality education and professional training, public service, advancing research and knowledge, and state-of-the-art health care". Stated succinctly, the mission is to generate and disseminate knowledge. All other activities at the university are secondary or subordinate to this primary reason for existing. All policy choices that might impede this mission must be carefully considered across campus so that all stakeholders can provide input, and mitigation strategies can be established in order to not violate the Article 1, part C provisions of policy precedence. It is also critical to observe that the mission of the University of Colorado differentiates it from those of other institutions, such as for-profit organizations.

Academic freedom is a bedrock principle of the University of Colorado, and one that administration and regents are required to defend, both by Regent Law and via CU's endorsement of the 1940 Statement of Principles on Academic Freedom and Tenure [Ame40] together with more than 280 national scholarly and educational associations. Moreover, Regent Policy 5.B.1 Associated Rights states the following with respect to academic freedom:

> (A) All faculty members, within the scope of their faculty responsibilities, must have freedom to study, learn, and conduct scholarship and creative work within their discipline, and to communicate the results of these pursuits to others, bound only by the control and authority of the rational methods by which knowledge is established in the field. The best method for advancing the state of knowledge is engaging with the broadest range of theories, methodologies, data, and conflicting opinions.
>
> (B) Faculty members shall not be subjected to direct or indirect pressures in an attempt to influence their work in a manner that would conflict with professional standards of the field. The Board of Regents and administration shall not impose such pressures or influence and shall resist such pressures or interference when exerted from inside or outside the university.

Faculty understand that security is necessary to protect academic freedom. Faculty also recognize that privacy is necessary to protect academic freedom. Indeed, privacy is recognized by federal

courts as essential to First Amendment protections[1] and the Colorado Supreme Court has ruled that Colorado's Constitution provides more expansive protection for privacy in consumption of media[2]. This is also enshrined in

- the Universal Declaration of Human Rights affirming the right "to seek, receive and impart information and ideas through any media and regardless of frontiers" [Nat48],
- the Library Bill of Rights "All people …possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information." [Ame19],
- and international norms and precedent [SC10].

Commitment to these principles is demonstrated by Colorado law specifically exempting library records from CORA requests (24-72-204 C.R.S.).

The SCSC creates many records analogous to library records in revealing intellectual processes, but far more invasive and searchable system-wide. The EDR systems log full URLs (which not only identify documents, but may include search terms), metadata about processes running on the computer, and metadata about files stored on the computer, and has the capability to upload files deemed suspicious to the cloud for analysis without faculty notification or consent. While such records might be determined to be exempt from CORA requests (but see [PK25]), faculty cannot have confidence that they would never be disclosed in response to law enforcement requests, court orders, congressional subpoenas, etc. Moreover, the data are stored on servers of service providers like Microsoft and Crowdstrike and their partners, which have terms of service permitting them to provide data in response to such requests, without providing notice or appeal by the University much less faculty who may have an interest.

The SCSC and EDR systems also create records that may infringe labor rights of campus workers. In 2022 the NLRB issued a memo addressing digital surveillance [Nat22], noting precedents including that employers obtaining photos of public union activity such as picketing infringes labor rights due to chilling effects, and requiring similar care in the digital realm. Although this report focuses primarily on those roles that are afforded protections of academic freedom, the NLRB memo's concerns apply to all campus workers. Moreover, Colorado's PROPWA examples [Col24] discuss criteria for an employer to have cause for surveilling workers, suggesting that routine electronic surveillance of all workers may not be acceptable under Colorado law.

By retaining URLs, EDR grants the employer (CU) metadata revealing when an employee reads particular scientific, legal, political or cultural information, participates in union communication channels, or engages in sensitive research or teaching. Chilling effects would not be alleviated by assertions that data would not be accessed for such purposes.

Academic freedom must protect activities that challenge powerful entities, including the government and companies CU contracts with for IT services. While defending against a landmark anti-trust lawsuit in 1998, Microsoft attempted to subpoena source material for a book that two professors were writing about Netscape and the browser war. In United States v. Microsoft (Harvard University and Massachusetts Institute of Technology), 162 F.3d 708 (1st Cir. 1998), the First Circuit upheld the district court quashing the subpoena: "Just as a journalist, stripped of sources, would write fewer, less incisive articles, an academician, stripped of sources, would be able to provide fewer, less cogent analyses. …[A]llowing Microsoft to obtain the notes, tapes, and transcripts it covets would hamstring not only the [professors'] future research efforts but also those of other similarly situated scholars." [Eub02] Under the SCSC, researchers would by default be required to store those files (via OneDrive) and metadata (via EDR) on Microsoft's servers, protected only by an unauditable promise constraining Microsoft's actions. While the Provost and COO might conclude such research represents a "compelling business reason" for granting an exception, a system that requires a permission slip to conduct scholarship that challenges power is not a system of academic freedom.

[1] "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation –and their ideas from suppression –at the hand of an intolerant society." — McIntyre v. Ohio Elections Commission, 514 U.S. 334, 357 (1995)

[2] "Search warrants… demanding information about the reading history of customers, intrude upon the First Amendment rights of customers and bookstores because compelled disclosure of book-buying records threatens to destroy the anonymity upon which many customers depend." — Tattered Cover v. City of Thornton, 44 P.3d 1044 (Colo. 2002)

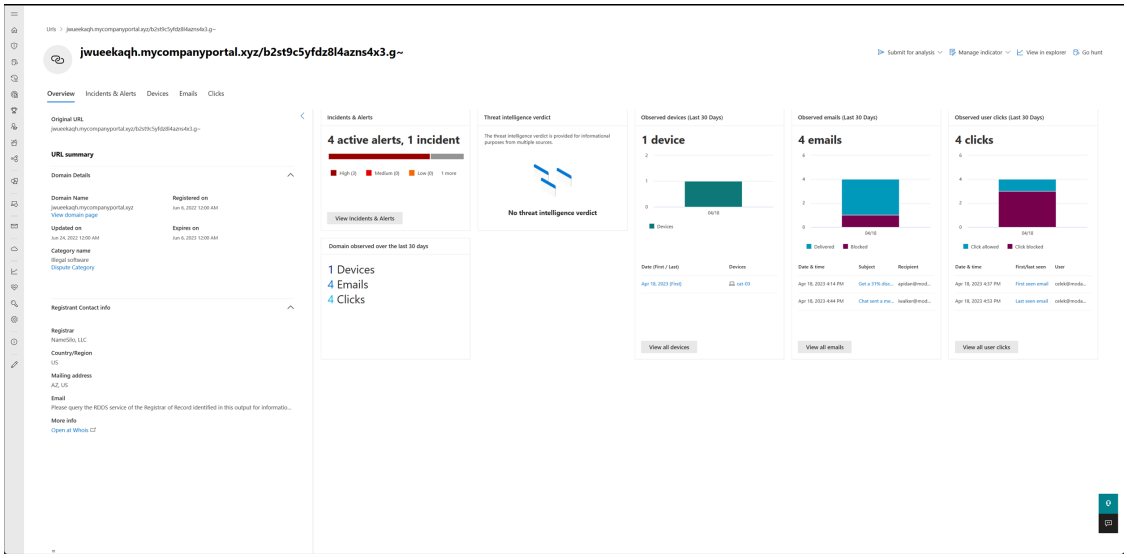

Figure 1: Screenshot from Microsoft Defender for Endpoint: Investigate domains and URLs. A URL identifies specific pages and may include search terms and tracking information. The device timeline feature would show, for example, when a researcher is editing a file alongside reading an article, which saved articles they may be opening while reading, and the queries used to find articles. Site-wide temporal analysis can also implicate colleagues: when one researcher mentions an article to colleagues in a hallway conversation and those colleagues visit the article, administrators or state actors would have circumstantial evidence of the timing, people present, and subject matter of an otherwise-private conversation.

Colorado law requires that OIT "shall implement and maintain reasonable security procedures and practices" (24-73-102, C.R.S.) and that any third-party services be "reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction." Pervasive digital surveillance via EDR and capability for warrantless access via EMS are not required by law, and indeed the detail and quantity of data raise significant concerns about freedom of speech, academic freedom, and Fourth Amendment Rights; see Carpenter v United States (2018) and Riley v California (2014) on warrant requirements. In the conduct of a search, the Colorado Supreme Court ruled in Tattered Cover, Inc. v. City of Thornton, 44 P. 3d 1044 (2002) that a "balancing test" was needed and that "a compelling governmental need for the specific …records" must be established. The need for specificity was emphasized in Comprehensive Drug Testing v. MLB, 13959 (9th Cir. 2010), holding that "[t]he government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents." EDR records stored on third-party servers constitute "large private databases", for which government searches "have the potential to expose exceedingly sensitive information about countless individuals not implicated in any criminal activity, who might not even know that the information about them has been seized and thus can do nothing to protect their privacy".

The Cybersecurity and Infrastructure Security Agency (CISA) Joint Cyber Defense Collaborative (JCDC) represents an additional mechanism of warrantless disclosure. Microsoft and Crowdstrike are founding members of the JCDC, engaging in "rapid bilateral and multilateral threat information sharing." Such sharing is a heightened privacy concern in 2025 after an executive order promoting unrestricted inter-agency data sharing [PST25] that would enable harassment and targeting of members of the CU community. Issues of privacy, including surveillance implications of the JCDC, were of extreme concern to the University of California Academic Senate, which has been engaged in a formal dialog with administrators about EDR mandates for well over a year, and on June 12, 2025 passed a resolution [Uni25a] calling for a delay due to these concerns. An associated open letter [Uni25b] was signed by over 1500 faculty across the UC system. The gravity of such surveillance is especially acute at UCLA, which is currently dealing with over $500M in federal ransom demand over vague allegations of activities that are likely protected by the First Amendment, and at UC Berkeley, which recently gave the federal government a list of 160 faculty, staff, and students without vetting or notification of the

allegations much less due process [Asi25].

Nothing is more important to faculty careers than reputation. Accordingly, attacks on academic freedom have often come in the form of conspiracy theories, innuendo, and online harassment directed at faculty. During the 37-year reign of the House Unamerican Activities Committee (HUAC), congressional subpoenas and testimony was used to smear faculty, creating lists and accusations without charges. The HUAC would have been impotent without media complicity and university administrators anticipatory obedience, condemning and firing faculty who were named by the HUAC, and refusing to hire or promote them [DiR25]. In recent years, the US House has wielded congressional subpoenas to target researchers of disinformation, channeling grievances from fringe conspiracy theorists, inciting digital harassment and threat of physical violence [DiR24]. Groups like Campus Reform, Professor Watchlist, and Canary Mission are part of a network of domestic and foreign actors who, via apparent ideological alignment with congressional committee chairs and the executive branch, threaten to invoke state power to suppress faculty and student speech and inquiry, and to coerce administrators. CU Boulder faculty have declined high-impact scholarly activities, such as testifying at the United Nations [Ho25], because state power, especially in border crossing, is being used to harass people named in such lists.

The President of the United States has made clear his desire that entire university departments and programs be dismantled or transformed, and has used financial weapons of dubious legality to extract concessions from administrators at Columbia and Harvard against the will of faculty, as well as threats. Donors and members of the Board of Regents represent a persistent threat to academic freedom [Uni25c; NL23]. NSF grant cuts to CU Boulder are the third-highest of all universities in the country [Lak25] and it would be naive to believe that upper administration is immune to these methods of coercion. It is thus essential that university policies minimize leverage that external or internal groups could apply to infringe academic freedom, including preventing collection and retention of records that are not required by law or direct business functions.

3 On the relationship of faculty with university

The relationship between faculty and their university is unlike that between employees and employers in other private- and public-sector settings. Universities have limited or no rights to many of the products created by faculty (Regent Policy 5.K). Moreover, external service is a required part of the professional duties and rights of faculty, and the conduct of that service is entirely based on agreements between faculty and external entities (professional societies, external research institutions, domestic and international funding agencies, hospitals, law clinic clients, etc.), to which the university is not a party. A faculty member's professional reputation (and licensing when applicable) hinges on their upholding privacy standards, even under government scrutiny such as administrative and court orders and congressional subpoena.

Unlike employees in other sectors, faculty are granted broad autonomy in faculty affairs, including determining research agendas and curricular decisions. The necessity of defending academic freedom extends beyond protection of individual liberties. Indeed, the Supreme Court has upheld "the dependence of a free society on free universities. This means the exclusion of governmental intervention in the intellectual life of a university. It matters little whether such intervention occurs avowedly or through action that inevitably tends to check the ardor and fearlessness of scholars, qualities at once so fragile and so indispensable for fruitful academic labor." — Sweezy v. New Hampshire, 354 U.S. 234, 262 (1957) (J. Frankfurter, concurring). In Keyishian v. Board of Regents, 385 U.S. 589 (1967), the Court further held "Our Nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely to the teachers concerned."

Regent Policy 5.A.1(b) requires that "the development of new policies or policy changes with respect to matters that directly affect the faculty shall be adopted only after consultation with appropriate faculty governance bodies". We note that SCSC impacts faculty teaching, research, and service in many fundamental ways, and yet there are zero faculty representatives on the OIT Cabinet. SCSC has also negatively impacted CU's reputation and that of faculty members, driving some to purchase computers out of pocket to escape OIT's unacceptable mandates. Computing and purchasing policies are important to applicants, drawing questions from faculty candidates and prospective PhD students, and have been cited when our offers are declined.

4 Different stakeholders have different IT needs

The faculty and staff across campus who are part of our knowledge-driven enterprise have extremely diverse research practices and teaching methodologies, and therefore their information technology needs are equally diverse. This makes the one-size-fits-all approach of mandating SCSC compliance for all computers incompatible with many research and teaching efforts. Faculty discretion over computer hardware and software environments affects the methods and scope of research and teaching, and thus is necessary for academic freedom [Ame40]. The IT needs of faculty range from the most basic office computing infrastructure such as web access, word processing, and data tabulation to creating large scale distributed hardware and software systems, operation of bespoke lab equipment, automation and robotics, and cybersecurity research. It cannot be overstated how critical to the University mission enabling and accelerating these research activities is, because in Colorado statute, the University of Colorado is *defined* as the "comprehensive graduate research university…". Any choices that impair research activities must made with the active engagement of faculty and must ensure that observation and mitigation strategies are in place.

In this section we will highlight some of the identified challenges that we anticipate will be created by the proposed SCSC. It is important to note that these are simply the challenges that we have identified in our relatively small sampling; other unanticipated impacts seem likely to arise if the SCSC is implemented, as-written. The fundamental incompatibility that we want to highlight is that large-scale corporate Information Technology systems like those sold by Microsoft were designed around and marketed to a type of institution that is not representative of the needs of our University. While we appreciate the complexity of implementing an IT strategy across such a heterogeneous set of users and needs, the current path proposed creates institution-level impacts that necessitate a revaluation of the strategy. Our primary finding is that additional reflection and fact finding must be done to assess the impacts of attempting to apply a set of tools to our campus that were designed for an entirely different user need base. This working group wants to acknowledge and emphasize that the key challenge in providing a unified IT Security policy for the University is the inherent heterogeneity of the University, as defined by its mission. The University is complex, and a proper IT security stance must acknowledge and adapt to this complexity.

In the following we provide a list of problems in regard to academic freedom rights faculty are facing with the new OIT mandated secure computing requirements. In particular, this list outlines the severe obstructions faculty face by these measures in their field specific research and teaching. Note that this is not a complete, but a first exemplary list. Note also that this part of the report is more technical than others because of the nature and the diversity of the technical problems arising from SCSC in different units.

Cinema studies

(a) *Problems with encrypted drives and video editing*. The full disk encryption requirement is not a feasible solution for any research and teaching in regard to Cinema Studies. The time to request/decrypt/play and request/decrypt/write are slow enough that under load with the CPU working to encode/decode the CODEC for video and to process effects (dissolves, color, repositions, etc.) the video stutters and drops sync. This is not a major issue for simple consumer-targeted system like Adobe Premiere, which will slow down the playback to adjust for performance. For any commercial/professional designed application that is working with broadcast sync or genlock, however, this is (literally) a show stopper. Professional video editing systems use inode mapping to manage the file read/writes to a drive (and utilize their own on-disk directory to keep track of the files) skipping the operating system queue for file management. This allows the video editing system to switch from file to file much more quickly than having to depend on the OS of the computer, which can often get bogged down (or make write errors) by other requests. When the disk is fully-encrypted, it means the application software has to stop and send in a request for a decryption with every read/write further slowing down the access under a time critical process (playback of uninterrupted video or cache files).

(b) *3rd party Cloud Services*. Few filmmakers trust cloud solutions and most prefer local hardware options. This is for a couple of reasons. Cloud solutions are slow and require a constant network

connection that slows down the network access for all of the machines in that network. Moreover, all external cloud-based solutions put intellectual property at risk for theft.

(c) *Cinema Studies media servers*. Since 3rd party cloud services are not a serviceable option, Cinema Studies maintains its own network service to allow network based editing and distributed rendering. These servers have special needs. Media delivery network services rely on a fast playback system to manage read and write requests with a latency of less than 4ms for up to 20 people simultaneously. Cinema Studies uses a dedicated server to serve both NAS and SAN LUN's for its labs. This server is carefully balanced to prioritize speed which is necessary for uninterrupted media I/O. This specialty tuning is necessary to do video and audio editing work that distinguishes Cinema Studies, yet it is beyond the scope of OIT's general computing support capability. Cinema Studies has additional servers that allow for multi-user collaboration and distributed rendering that requires understanding of specialty applications. OIT's SCSC policies will interfere with student and faculty work and classes.

Mechanical engineering and robotics The robotics faculty and many other experimentalists in engineering have a large number of network-connected instruments/experimental setups with "computers" that must be connected to our network. These are devices that may not have graphical capabilities at all (so the typical user-oriented network registration is not an option), will be frequently moved/added/removed, or which serve a specific research purpose (are not general-purpose office PCs), yet they may be closely related to "office PCs" in terms of constituent parts and appearance. Every robot, 3D printer, mechanical testing instrument, microscope, etc., uses one of these compute devices, with OS flavors ranging from none to Windows XP to Windows 11 to Ubuntu. There are a very large number of these, and we are adding/removing/moving these frequently. Some facts about these devices: They are operated by highly skilled users. They run very lean, with only the software on them that we intend. We frequently rebuild them, swapping out NIC (and MAC). They are low-cost and come/go frequently as projects require. They are associated with a specific type of data and are very unlikely to deviate from that type. Speed and agility are essential and central to their use. We also point out that this concern applies to many of the engineering lab courses as well, which use many flavors of computation, including physical and virtual machines, that need to be network-connected and rebuilt every semester by a new cohort of students.

The IT-FWG hopes that all these use-cases are what was envisioned by the "This does not include printers, removable storage, or Internet of Things (IoT) devices and sensors" text, but this needs to be clarified in writing because the current text is inadequate and will lead to misunderstandings in implementation and procurement approvals. If these devices are not excluded, the current policy likely creates an untenable research environment. From a cursory read, it looks like the risk acceptance form would need to be filled out for every unique network-connected device in engineering research and teaching labs[3]. There are literally thousands of these in the engineering center and more importantly they are frequently changing (adding/removing/modifying) as part of their core use-case. It is important to note that the need to use these devices as has been described is driven by current grants and contracts that the university has signed, as well as by our core teaching mission.

Foreign languages Faculty doing research in or teaching of foreign cultures or languages face the significant problem that the OIT mandated cloud solution Microsoft OneDrive does not allow certain characters in file names. Besides non-allowable characters like colon or inequality symbols in file and folder names, Microsoft OneDrive modifies and corrupts names containing Asian characters. For example, Chinese characters in the folder path or file name get replaced with question marks, making the files unrecognizable. When these issues were reported to OIT, they provided no redress other than that researchers should manually change all filenames to avoid characters that OneDrive corrupts. Some faculty report that forced implementation of OneDrive destroyed some of their research files with foreign characters in their filenames. One of the main arguments for SCSC is that it should prevent ransom attacks from making research files inaccessible, yet the SCSC-mandated cloud storage solution has done exactly that for faculty in certain research fields.

[3] https://oit.colorado.edu/webform/it-security-risk-acceptance-form-secure-computing-standard-computers

Law Law scholars are dependent on their data being secure and not accessible by external parties, in particular when they provide service to law school clinics or have ”of counsel” relationships with law firms or external clients. Having their confidential legal data stored on a university owned computer with mandatory EDR and OneDrive cloud storage is not a tenable situation for law professors because it might violate certain attorney-client privileges and create dangerous liabilities. The effect of SCSC on law professors has often been to compel them to use only private laptops for their scholarly and legal work.

Bioinformatics, climate research, and computational research such as quantum physics, quantum chemistry, and multiscale fluid and structural mechanics Common to these research areas is that they are very demanding in regard to computational power and therefore mostly use Linux servers or even clusters of Linux servers for high-performance computing. Besides this, to be at the national or international forefront in research in such fields, computational competitiveness is a key requirement. The requirement by OIT that all Linux servers have CrowdStrike Falcon software installed is particularly threatening to privacy and confidentiality, since the CrowdStrike Falcon software requires kernel access within the Unix operating system and thus allows for surveillance of essentially everything happening on the server. It is the IT-FWG's opinion that CrowdStrike's intrusion detection software actually constitutes a significant intrusion into researcher's academic freedom and privacy rights, potentially even bringing them into violations of contractual confidentiality agreements with federal or other external grant institutions. In addition to this, the CrowdStrike Falcon software slows down certain workloads. This is absolutely detrimental to scientific high-performance computing where computational power and speed is key to being competitive within the national and international research communities.

Mathematics and STEM Education The Mathematics Department and the School of Education run and/or create open source software for webgrading or online STEM education on Linux servers. The corresponding academic work is partially research and partially teaching, and falls fully within faculty's academic freedom rights. As explained with more technical and legal details in Section 5, outsourcing of Linux server management threatens research and teaching activities on Linux servers in mathematics and education and thus constitutes a significant intrusion into the academic freedom rights of faculty in these units.

Computer Science The Computer Science department maintains a range of computing hardware, including racked servers that provide local environments similar to commercial clouds. Networking and security labs may configure large numbers of computers to understand bottlenecks or to explore the anatomy of cybersecurity attacks and mitigation. Some activities require BIOS and hypervisor-level access while others need bespoke user environments. Some researchers develop open source software that large external communities rely on, using local servers for continuous integration and collaborative development, including with partners that are not affiliated with CU. The scope of data on such machines is narrow and specific to the research group. This requires a unique security policy and involves jobs that create new processes and open/close ports at a high rate; CrowdStrike Falcon has been observed slowing down workloads of this type by as much as a factor of 2.

Academic freedom is also infringed by OIT decisions that limit availability. For example, in response to a suspected security incident, OIT confiscated servers for an investigation, but then took more than a year to return the servers to operation. In doing so, OIT facilitated a denial of service attack on CU-led research that the attacker disfavored. OIT should instead actively work to ensure that such research can continue without endangering other functions at CU, and collaborate with researchers to minimize the harm from security incidents that may not be preventable (e.g., state actors and other advanced persistent threats may have access to zero-day exploits and coercive measures).

5 Linux server management

Linux servers form the backbone of many major research efforts at CU Boulder. These servers exist in a variety of labs throughout campus, with the vast majority (more than 1900) supported by institute

IT staff rather than OIT. These servers support major NASA, NSF and DOE funded research and are often principal points of contact between campus and national-level supercomputers, where CU faculty members and their groups are major (and sometimes nation-leading) resource users.

Critical attributes of these servers and their administration are: security, responsiveness, and flexibility. Much of the research conducted using Linux servers requires specialized software stacks that require frequent updating and often require modern Linux operating systems that OIT does not support. For example, many open-source projects are fully developed within the large Debian ecosystem (e.g., Debian, Ubuntu, `Pop!_OS`). In such ecosystems, these software packages are easily installed and maintained. In contrast, OIT supports only Red Hat Linux (RHEL), which is at this point a narrow community and woefully behind in software accessibility. This has particular impacts for faculty-developed toolkits that utilize modern interpretative languages (e.g., Julia, Python, etc.) where RHEL-supported versions can lag far behind the current state of the art.

Maintaining and operating toolchains for research at the cutting edge requires on-demand IT support, and for these reasons many of us directly pay for institute IT support out of grants. A critical component of this is sustained working relationships with a deep understanding of the needs of research scientists and the possibilities of the Internet of Things. As one example, the Laboratory for Computational Dynamics (Duane Physics) has a multi-decadal working relationship with the JILA IT adminstrators, who participate in grant writing opportunities, supercomputing allocation requests, and in decision making sessions about the structure of the computational lab and the research needs of the teams working there. Response times are same-day and often same-hour, which is critical while coordinating with large federal computing campaigns and internationally distributed teams.

Interactions with federal supercomputing facilities raise substantial questions about widespread deployment of EDR and similarly intrusive security measures on Linux servers such as the CrowdStrike Falcon software. While most federal supercomputing facilities practice zero-trust with regard to users connections (e.g., NASA), mandated federal IT security training highlights the importance of users ensuring that their computers are not loaded with keyloggers or similar software. Some of the proposed security solutions (e.g., CrowdStrike Falcon) can embed these prohibited tools. The presence of these tools could jeopardize national and international research collaborations, and could bring faculty using Linux servers in their research or teaching into legal limbo. We note that even DOE Leadership Class Facilities, including machines worth over $500M and those that process Controlled Unclassified Information (CUI), do not require or encourage installation of software (including EDR) on endpoints.

A significant problem in this space is the outsourcing of Linux server management from OIT to a company in Canada, Crafty Penguins. In the past, about 60 Linux servers on campus were managed by OIT. As mentioned before, the majority of the roughly 2000 Linux servers on campus have not been managed by OIT but are maintained by the institutes, by grant supported personnel or departmental IT staff hired specifically for such Linux administration purposes. OIT decided to cease Linux server management supposedly for financial reasons and because, as several faculty have heard at open forums, the administration labeled Linux servers as ”dangerous” and therefore CU should get rid of them. The IT-FWG regards such a statement as unqualified, in particular in view of the fact that certain types of research such as on bioinformatics, big data, climate modeling, nuclear reaction modeling, high-performance scientific computing, large language models in AI, or quantum chemical computations are almost solely performed on Linux servers or even clusters of Linux servers. Restricting availability of and access to Linux servers is a significant intrusion into faculty's academic freedom rights and endangers the competitiveness of many research groups in Engineering, the Natural Sciences and the School of Education.

Faculty were not consulted about the plans to outsource Linux server management; rather a Denver consulting company was tasked with checking whether outsourcing Linux server management is feasible and allowable. The OIT directors informed faculty members after a meeting with the BFA Executive Committee that the consulting company and their lawyers gave the OK to outsource Linux management to out of the country. No faculty members were consulted in reaching this decision, which has had substantial impacts on academic affairs. Rather, the only faculty member who had a seat on the OIT Cabinet has since been removed from that influential oversight committee. Moreover, several departments on campus heard only accidentally about OIT's plan to cease Linux server management through emails sent to IT technicians or by word-of-mouth.

Two units severely affected by the outsourcing of Linux server management are the Department

of Mathematics and the School of Education. Originally, the Linux server of the Department of Mathematics was managed by OIT, contained research data of faculty and most importantly confidential student data from an open source webgrading software. After the Department of Mathematics was informed only accidentally in Spring 2024 that OIT will cease to maintain the departmental Linux server, the Department of Mathematics felt forced into outsourcing, and there was no time to find alternative solutions. So in the end faculty worked over the summer with the departmental IT technician to remove all student databases and other sensitive student data from the server. The open source webgrading software developed by mathematics faculty from all over the world for mathematics faculty cannot be used anymore by FERPA restrictions as long as the server is externally managed.

The School of Education is in a similar difficult situation because they created software, called *LA Campus*, which is hosted on a Linux server at CU Boulder, and is currently licensed to 20+ universities nationwide, with intent to increase the number of contracts in upcoming years. Licensing fees range from 8K to 40K annually. By outsourcing server management, the license agreement could be voided. Security negotiations with other universities included a Higher Education Community Vendor Assessment Toolkit (HCVAT). When Linux servers were supported by OIT, the School of Education was able to report security standards and practices posted by OIT–which have proven to be trusted by other universities. But now, with the outsourcing of Linux management, the HCVAT would have to point to Crafty Penguins, which not only is not at CU Boulder, but in another country! Hence the School of Education will negotiate fewer, if any new contracts for *LA Campus* in the future, and some existing contracts will be voided. Temporarily, a short-term solution has been worked out with the gracious support of an institute, but the health of the researcher's work on *LA Campus* depends on a long-term in-house solution. For the Mathematics Department no long-term solution has been found yet either.

Let us cite the CIO Gerd Chrzanowski from the Schwarz group, the largest European retailer, which faces 350,000 hacker attacks per day from Russian hackers: "There are data which should not lie on servers in another country". Unfortunately, CU is doing exactly that. We allow IT technicians from another country to fully control quite a number of our campus servers which house important and confidential data of our faculty and students. This causes a severe security hole because CU does not have any influence on IT security at Crafty Penguins, the labor laws in Canada, and whether or not Crafty Penguins does appropriate background checks of its IT personnel. OIT claims that CU faculty is protected by the contractual agreements with Crafty Penguins and other external software companies. But that appears to be a risky approach because

1. CU does not have the means to enforce adherence to the contractual obligations of external companies, let alone if they reside in a foreign country,

2. outsourcing Linux server management opens security holes instead of closing them,

3. CU can not react appropriately in the case of a significant hack on university servers when server management has been outsourced (who will pull the plug?),

4. it might open up legal ramifications against the University of Colorado or loss of insurance protection because the vulnerabilities by outsourcing Linux server management have been foreseeable, and finally because

5. it creates significant dependencies on outside expertise and knowledge while at the same time CU loses the necessary internal expertise.

Outsourcing Linux server management is a significant intrusion into faculty's academic freedom rights including the freedom of research. Certain software like online open source grading software or student educational software can not be run on servers managed externally due to, e.g. FERPA protections. A server managed from another country cannot be used for export-controlled research, but by outsourcing such activities, CU loses the internal expertise to meet the diverse needs of export-controlled research at CU.

The IT-FWG believes that outsourcing Linux server management increases the technical and legal threat surface, and that the associated hollowing out of local expertise represents a persistent strategic vulnerability.

6 Microsoft monoculture

The IT-FWG finds that over-reliance on Microsoft products unduly constrains research and teaching, and limits the range of OIT expertise to address threats across the diversity of platforms necessary for research and curricular objectives. The IT-FWG finds the lack of attention to Linux/BSD/Unix operating systems in the SCSC policy document surprising and inappropriate. The document is incomplete as well as too narrow, focusing on prescriptive, platform/vendor-specific directives rather than desired outcomes, and lacking provisions for different use-cases with suggested strategy for achieving these desired outcomes when subject to unanticipated constraints.

The IT-FWG understands the very real security concerns, and the complications that the patchwork of state and federal laws create regarding the various types of data that we receive, store, generate and disseminate across campus. The IT-FWG wants to point out that these issues are complicated, and unfortunately so are the solutions. The current solution that requires that everyone uses Microsoft-managed services in a locked-down way does not address the core needs of our campus; it actually impairs them.

Overall, OIT should not presume to know the best specific IT solutions for the tasks that researchers on campus perform; our collective research activities are simply too diverse for one-size-fits-all solutions, and faculty are uniquely equipped to evaluate IT requirements for their research and teaching activities. A flexible pragmatic approach that balances the important and real concerns about security against the diverse and dynamic needs across campus should be the organizing principle.

Regarding the delivery of services via bundles by Microsoft, there is an actual risk that becoming reliant on a single vendor introduces a vulnerability to regulatory breakup as well as a weaker negotiating position. For example, in light of a Michigan Microsoft anti-trust case, law scholars wrote in [KSC05]:

> …that intervention against bundling should never be considered unless all three of the following conditions are met:
>
> (a) the firm in question has monopoly power (i.e. at least a dominant position), in one market which is affected by bundling;
>
> (b) the bundled goods are complements; and
>
> (c) there is significant (and costly to overcome) asymmetry in the product lines of the dominant firm and its rivals.

All three of these conditions are clearly met by the Microsoft 365 suite. Relying solely on these products as a unified bundle is a risk to the University. It is also well-understood that bundling does not, over the long term, lead to savings to customers. Consumers buy more when bundling is used [DK13]:

> Sales of hardware and software components decrease in the absence of bundling.

Indeed, bundling is more profitable for the vendors of these products than selling individual products and therefore more expensive for consumers, meaning in our case the University [GMR18]. Finally, the reliance on a single vendor exposes the University to cyberattacks by hackers exploiting loopholes in widely-deployed software products. The recent cyberattack [Pea25] on Microsoft SharePoint servers and the failure of Microsoft to provide appropriate security patches in time is just one example of that.

Last but not least, the IT-FWG wants to point out that the sole discretion on the choice of hardware and software necessary to fulfill research and teaching at the University of Colorado lies within the faculty. It is not within the purview of OIT to impose on faculty certain office, cloud storage or telecommunication products. The dominant reliance on Microsoft products is not adequate within an academic environment and creates additional and unnecessary vulnerabilities.

7 Summary of issues with OIT's Secure Computing Standard

1. The definition of ”computer” in the SCSC policy needs additional clarification. As-is, it is open to interpretation regarding various types of lab/research and teaching compute platforms including embedded computers that are network connected.

2. The specific plan for "Chief Information Officer or Information Security Officer may suspend a computer's and/or an end-user's access to the campus network" leads us to conclude that the plan is for an "allowlist policy", though this is not explicitly mentioned. The implementation (e.g. MAC allowlist) of this capability will create major impediments for how researchers use the network. A "allowlist policy", which requires action and registration for a computer to join the network is an unacceptable burden for users of an academic network, which by definition must support a heterogeneous compute infrastructure.

3. This SCSC policy, as it becomes understood and enforced, is going to generate a large number of exception requests for the acquisition and use of computers. This is going to be a problem for all concerned, given the fact that the exceptions that it anticipates are actually the rule in an academic research environment, and given the requirement that these exceptions be approved by the Provost and Chief Operating Officer. This will prevent research that is federally contracted from occurring as proposed, and provides a pretext to infringe the freedom to conduct research that university leadership may find to be politically risky.

4. The mandatory use of EMS in the form of Microsoft Endpoint Configuration Manager (Windows computers) or Jamf (Apple Mac computers) creates critical issues for faculty and researchers. It gives the technical capability for OIT to monitor all data and control all access on a user's computer. This is unacceptable from an academic freedom standpoint. It is also unacceptable given the heterogeneity of work that faculty do (external society service, 1/6th time, etc.), the global reach of this work, and the global extent of where this work is performed (for example, our computers need to work everywhere, regardless of a data connection). In addition to the academic freedom concerns there are significant technical problems connected with Microsoft Endpoint Manager (via ConfigMgr/Intune). The following scenarios just provide a few examples:

   - restart of a PC in a managed configuration requiring an update,
   - computer use when the network connection is unstable,
   - pushed update during a talk or lecture,
   - withdrawal of OS administrator rights via e.g., an OIT-induced template change while the faculty member needs to address an issue with the PC or install a piece of software requiring full privileges.

   Such operations can destabilize a PC, can be extremely slow, and have led to crashes and interruptions of faculty giving talks or teaching. For all of these reasons faculty are reluctant to have EMS installed on their computers and in general do not consent to blanket OIT access to CU PCs used by faculty. Endpoint management might be convenient when campus workers need technical support from OIT, but it should never be used without affirmative consent from the workers. For most faculty and researchers, it is a vulnerability and privacy threat for the capability to be enabled.

5. Microsoft Defender for Endpoint constitutes invasive surveillance stored on third-party servers. Faculty have no control over this, and no means of even knowing who maintains these data and for how long. This is a clear violation of academic freedom, especially given the present information and political context in which universities are subjected to unprecedented coercive measures.

6. The requirement to use OneDrive by Microsoft as the only OIT supported and approved enterprise cloud storage solutions is not acceptable. OneDrive has very poor sync performance, and exposes faculty to academic freedom concerns and risk of data loss. Many researchers feel that Microsoft products for cloud storage are inferior to other tools like Dropbox. For example, the incremental sync features of Dropbox are faster, use fewer PC resources, provide better quality of service across shared networks, and use less bandwidth. The Dropbox file sharing capabilities are easier to use cross-platform, and provide more control over user access and access duration. Dropbox has better file-change tracking capabilities and recovery options. Further problems with OneDrive arise when researchers attempt to collaborate on an article with external researchers not having a `colorado.edu` account. Microsoft's cloud collaboration software SharePoint is not only an inferior tool for collaboration to e.g., Dropbox, it has inadequate support for Linux and

even causes access and syncing problems when all collaborating researchers use Windows. Moreover, OneDrive corrupts certain special characters and many foreign language characters, whereas Dropbox is fully UTF-8 compatible and allows for use of special and foreign characters in filenames. Finally, it is a vulnerability that OneDrive (and Dropbox) lack zero-knowledge encrypted backups, which requires that encryption keys never leave the user's device and the backup provider has no knowledge of file content or metadata. A researcher cannot affirmatively protect sources while storing those files on a platform owned by an entity that wishes to identify those sources.

7. The SCSC largely ignores Linux/BSD/Unix systems, resulting in labor-intensive processes for purchasing and compliance.

8. The SCSC states that computers must: "Run current, supported software. The use of out-of-date operating systems or software that is not being actively updated and is considered end of life is prohibited." Even though in many cases this is a very reasonable requirement, it can cause a problem in a large number of common research scenarios in which using software that "is not being actively updated" is common practice, and is legitimate. Examples include established disk utility tools, printer drivers, software development tools, a vast array of open source software (packages and source code), etc., or any software development effort that is complete (including software that we write in our labs). The quoted text reveals how little contact the authors of the SCSC document have had with the diversity of academic research environments. Addressing this gap solely via exceptions is infeasible and places an undue and disparate burden on such research programs.

9. The encryption requirement appears to be reasonable in many cases (especially for mobile devices) but turns out to be detrimental for I/O intensive computing tasks such as video editing or high-performance scientific computing; see the paragraphs on **Cinema Studies** and **Bioinformatics, climate research, and computational research in quantum physics and quantum chemistry** in Section 4.

10. The exception procedure requiring COO and Provost approval is inadequate for the frequency and scale of exceptions necessary. Moreover, the requirement to demonstrate a "compelling business reason" is an infringement of academic freedom. The criteria for granting exceptions have not been adequately specified.

8 Cybersecurity at peer universities

We have investigated the security computing standards at peer universities. We found several models that could work, however, we discovered that some peer universities are implementing policies similar to the SCSC. Nevertheless, the SCSC at CU Boulder appears to be by far the most restrictive secure computing standard among peer institutions, and it was implemented with the least faculty involvement. For example, at no university in our sample has Linux server management been outsourced, and EDR for Linux servers (e.g., CrowdStrike Falcon) has been mostly only recommended instead of being required as it is at CU. It became apparent to the IT-FWG that the fact that secure computing mandates infringe academic freedom has not been considered by administrators. CU Boulder has an opportunity to be a leader in careful consideration of "when cybersecurity meets academic freedom."

In the following, we give some (still incomplete) information about secure computing standards at a sample of peer institutions. The IT-FWG notes that while the practices of other institutions can help provide ideas for IT implementation choices on our campus, the specific practices of other institutions are not relevant from a decision-making perspective. Under no circumstances is the following explanation sufficient or convincing: "institution X is doing Y, and therefore our choices to follow that practice are justified." We note that language similar to this has been written by OIT and shared verbally with the IT-FWG. The charter, objectives, values, and requirements of CU Boulder are unique to our campus, and decision-making must reflect this.

Cornell University Cornell IT defines two areas of security:

- Staff working with personal or financial data that requires strong security protocols
- Academic research and pedagogy that may require a more nuanced security model that is based on recommendations and opt-in protocols that professors and faculty can decide how they want their computers or data to be handled.

Cornell students are not required to adhere to any policy but are instead offered a list of options they are encouraged to consider.

University of Texas at Austin The UT Austin Technology Resources (TRecs) provide colleges, schools, and departmental units routine installation, maintenance, and monitoring of their servers. Through its Liberal Arts Instructional Technology Services (LAITS), the Liberal Arts College of UT Austin offers a la carte management of Windows and Linux servers as well as of Linux workstations for its units and faculty.

University of California On February 26, 2024, the University of California President Drake issued a mandate to implement EDR system-wide by May 28, 2025 (as at CU, this target deadline was not met). This prompted a series of open letters [Uni25b] and UC Academic Council resolutions opposing the mandate on the basis of unacceptable surveillance implications and calling for "a transparent and inclusive evaluation process involving faculty representation to ensure the safeguarding of privacy, academic freedom, and research integrity" [Uni25a]. The current UC President Milliken's term started August 1, 2025 and we are not aware of his having addressed this issue yet. We note that outside of this EDR mandate, UC campuses generally have more support for internal services and at least some faculty representation on IT committees. For example, UCLA offers, through its UCLA IT Services, standard and extended support for the management of their Linux servers. In this case the essential Linux server management is also done by reliable IT personnel on campus.

University of Washington UW does not mandate EDR, EMS, or specific backup solutions. Units have IT staff that collaborate with faculty to implement cybersecurity best practices in a way that is responsive to research and educational needs, and coordinate with campus IT to understand persistent threats. Faculty governance and administration agree that privacy is necessary for academic freedom and seek to minimize collection and retention of records that are not essential to the university's mission.

Massachusetts Institute of Technology Dropbox for Business is licensed for use by MIT faculty and students. Even though the precise reason for that choice is not stated on the MIT webpage, it is probable that Dropbox appeared to be a better fit for academic, scientific and technological purposes than other cloud solutions. Email and file-storage services on the MIT campus are handled in a distributed way, with units exercising control over specific vendor choices; some units provide these services internally, without an external vendor.

9 Recommendations

9.1 Restoring trust

It is critical to acknowledge from the outset that Information Technology security is an extremely complex and fast-moving field with numerous competing approaches and philosophies. There is not a single "correct" established answer to IT security, despite reductive assertions from various parties. A robust dialog built on mutual trust is necessary to arrive at mutually-acceptable strategies that protect individuals and the diversity of research and teaching activities while mitigating evolving cybersecurity threats.

The IT-FWG has identified a loss of mutual trust over the past several years, largely stemming from a lapse of robust dialog. This loss of trust runs both ways, with OIT projecting a belief that faculty are naive and out of touch with present cybersecurity threats while faculty complain that OIT is unaware and uninterested in understanding the nature of their work or collaborating with them in

decision-making processes. Recognizing asymmetries in power due to job roles and relations with campus leadership, the IT-FWG recommends initiating a restorative dialog between OIT leadership and faculty with the assistance of an *external facilitator* to build mutual trust as a first step in a restorative process.

9.2 Operational recommendations

9.2.1 Cybersecurity preserving academic freedom

First and foremost, all OIT decisions about hardware and software mandates should be made with academic freedom as a first-class principle, with meaningful, substantive, and comprehensive faculty participation in the drafting process. The IT-FWG therefore recommends that OIT partner with faculty experts to conduct a comprehensive review of policies, starting with SCSC, to understand their implications for privacy and academic freedom, and to propose revisions.

9.2.2 Adherence to privacy and data protection standards

It is recommended that the University adheres voluntarily to certain privacy and data protection standards beyond those legally required in Colorado. For example, OIT could provide IT products compliant with the General Data Protection Regulation (GDPR) and privacy policies of the European University Association, which provides privacy protections that generally align with that of academic freedom. OIT should establish a policy that no metadata be recorded or stored without an immediate business function, and that any metadata extent and retention be minimized. Under no circumstances should full URLs accessed by an endpoint be communicated by OIT-sponsored software beyond that endpoint without direct human oversight. OIT should provide clear policy statements on how data and metadata are stored and the length of time it is accessible.

9.2.3 Data classification

The present data classification table[4] where data are classified within in the three categories *Highly Confidential Information*, *Confidential Information*, and *Public Information* needs to be updated, potentially even revised. In particular the data classification should contain the point *Student's Academic Work* which presently it does not. The IT-FWG recommends to list *Student's Academic Work* under the category *Confidential Information*. The policy should also address data to which CU has no rights, such as that associated with external professional service, law clinics, materials to which faculty own copyright, etc.

9.2.4 Backup and cloud services

OIT should support a zero-knowledge encrypted backup system and researchers should be able to opt into that system at their sole discretion.

9.2.5 Implementation of a disclosure model instead of exceptions model

The model for IT security at CU Boulder should be an opt-in model instead of the current opt-out model, with "profiles" for common scenarios. For many faculty members maintaining labs, servers, and faculty laptops, the number of things to work around to eliminate the "standard" installation approach eats up incredible amounts of time and interferes with faculty teaching and research.

System administrators for departments have a front-line position interfacing directly with our students and our fellow colleagues, and often are pressed into making sure everything works together. If a class is using a Filmlight plugin for grading, for example, it is important that the IT resource person for the department can make sure faculty teaching in that lab have the matching version for their own computers to be able to set up their lesson plans. Unit system administrators often have the clearest picture of what is needed and what needs to be disabled or removed for a functioning system. Forcing everyone to comply with a pre-set install regimen makes the work of System administrators vastly

[4] https://www.cu.edu/data-governance/resources-support/data-classification

more complex and adds the additional layer of bureaucracy to request a waiver or exemption for each system.

The IT-FWG recommends to support and trust the departmental system administrators, and let them together with the departmental faculty IT representative or computer chair make the judgment calls on what level of security or restrictions are necessary for their departments. It is recommended to let these departmental teams of computer chair plus system administrator choose how restrictive the computers need to be and opt in to the resources OIT can provide to help them.

In order to achieve that level of trust, OIT can and should require departmental and unit system administrators and possibly even faculty computer chairs to go through training or certification to assess that they understand the risks and the technology available (see also Recommendation 9.2.15). After successful training the computer chair plus system administrator team can then make an appropriate assessment on how to deploy security within their unit. OIT should be a service for the units, not a policy-making group that dictates to the units.

9.2.6 Establishment of IT user roles

The CU Boulder campus hosts a very diverse set of IT users and needs, with almost no common overlap among all users. There are however various best practices and known mistakes to avoid. Different use-cases require different IT security approaches. One potential way of addressing the heterogeneity on campus is to identify different user groups and attempt to classify their Information Technology needs, competencies, and risks to the university. Appropriate IT recommendations and requirements can then be applied to these roles. Note that in the list that follows we are referring to roles and not individuals specifically because in many cases the same individual fulfills more than one role and therefore any policy proposed should acknowledge this fact and accommodate a heterogeneous workstyle. Let us also mention that the list of roles we recommend should be regarded as a first step which should be fine-tuned and possibly extended during a revision of the SCSC.

- **Office Work 1** One set of roles could be characterized as office work in which users utilize a variety of University provided tools including database, word processing, and other office productivity tools that require a trained user to manipulate the tools but that user is not engaging in the generation of new knowledge through writing or coding. This type of role may include student support, financial and contract support staff, and also encompasses some faculty administrative roles. These roles require access to sensitive data including financial and protected data, and therefore place this type of role in a higher-risk profile.

- **Office Work 2** Another common set of roles across campus is characterized as office work accessing University data, manipulating it, and making decisions. These types of activities include reviewing applications from students and job seekers, processing applications prior to review, affecting hires once a decision to hire or offer a student position have been made. This role is performed by faculty and staff often in an asynchronous mode with periods of activity during the year followed by lulls during which time the individuals perform other roles. The types of data involved in these roles include transcripts, resumes, personal contact information, and other forms of personally identified information but do not need to include personal financial data or banking or social security information. These roles could be considered to have a medium risk profile.

- **Instructor 1** Another role involves creating and delivering course content to students. This includes both live in-person, live remote, and asynchronous remote delivery strategies. It is important to acknowledge that according to Regent Law Article 5, in most cases the creators own this course content, not the University. As such the university must not take steps via information technology management and delivery mechanisms that could potentially deprive these owners of access to their data. As owners of these data, these individuals have a vested interest in protecting it and the university should provide resources and tools that enable them to do so. These data are commonly made available on public websites and forums and therefore the risk profile of such data is not primarily about public disclosure but rather about depriving the owner of access to it.

- **Instructor 2** This role also involves teaching, but with a significant lab component that relies on IT infrastructure. This will involve procuring IT hardware (computers, embedded computers), and

deploying operating systems on these computers. In some cases this is done by course support staff and in others it is done by students. This task set includes many of the tasks described in “Researcher – Data Analyst” and “Researcher – Embedded Systems Dev”. The risk to the University is similarly low, with no data that is protected or private used.

- **Researcher** Another role, which is common among research staff, research faculty, and tenure track faculty involves the creation of new knowledge through research and discovery, and disseminating that knowledge to the broader community. Individuals own the copyright to their writings and commonly transfer an instance of this copyright when they publish their papers to the publisher. In tandem with copyright issues, the University via the structure of the Bayh-Dole act, owns the right to intellectual property generated using University resources including laboratory facilities and IT infrastructure. In the overwhelming majority of cases the data generated, transferred, and maintained in the course of these activities is low or medium risk with little to no protected categories. If the intellectual property generated were disclosed prior to the submission of a patent application or a publication, it would disadvantage the researcher and the University, but little evidence suggests that the financial magnitude of this risk in terms of present expected value is significant [Pea24]. It is important to note that the explicit stated expectation for University research is that it will be published and will not be kept private as a trade secret or other private mechanism. For this reason public disclosure of research findings or research data is not likely to be a significant systemic risk to the university. It is certainly the case that depriving the researcher and the University access to research data and research findings is a risk and therefore resources and guidelines must be provided to mitigate this risk. The Researcher category consists of several distinct subcategories with varying IT needs and capabilities.

- **Researcher - Data Analyst** One role subcategory includes researchers who perform their research by accessing public or private data sets, and knowledge in the larger research community, performing analyses using existing data manipulation tools, and documenting and publishing their findings. This use case does not involve a significant component of novel tool generation and these users can perform the bulk of their work using readily available hardware and commercially available software tools. However, this role may require specific data safeguards such as encryption, access control, dedicated offline storage, and anonymization. The specific implementations of these general practices will vary depending on the data type, source, ownership structure, and/or license constraints.

- **Researcher - Software Developer** Another subcategory involves research enabled by commodity hardware including lab tools and computer infrastructure but requires a significant customization or creation of software tools in the course of this research. These users will leverage their own coding expertise in various software generation platforms including web-based, ai-enabled, and conventional user-centric coding practices. These users will also leverage a significant component of open-source or otherwise pre-existing code to accelerate and enhance their work. It is essential to acknowledge that in most copyright and use agreements, the original code authors offer no warranty or guarantee of use, suitability or reliability etc. in the code that they post online. It is up to the user to determine the suitability and safety of the code they are using. These third-party code bases may or may not be actively maintained, yet they serve as an essential enabler of research progress. Accessing these external code bases requires a network connection to the public internet from the machine being used for development. The data used and generated in the course of this research in this context is primarily low risk of disclosure meaning the data types contain no personal identifying data or Financial/Social Security data.

- **Researcher – Embedded Systems Developer** Another subcategory contains many or all of the software features and needs addressed in the subcategory “Researcher – Software Developer” above but also incorporate modifications and development of hardware. This may include custom experimental apparatus and typically includes custom computer systems which encompass an array of computer types ranging from individual desktop computers that have been specifically customized with hardware to enable a particular feature set, to server systems that have been similarly customized for the task, to embedded computer systems that run minimal operating systems and incorporate networking technology for various features. These types of computer systems are ubiquitous across campus and represent a significant oversight in the SCSC. It is

common practice in this use category to download and run virtual machines, Docker images, etc. that create virtual computing instances and to do so rapidly and frequently during the course of a research project. It is similarly commonplace to purchase, develop on, and deploy small embedded computers that include various operating systems spanning Windows, Mac, and Linux/Unix. The ubiquity of these systems, and their centrality to research, makes addressing them via an exceptions policy a critical mistake with the current conception of the SCSC.

- **Student** It appears to be reasonable to have one or several student roles which should be made more precise when such a role based secure computing classification for users will be established.

9.2.7 Campus-funded in-house Linux server management

The IT-FWG recommends that a campus *UnixOps* group should be established, consisting of Linux experts tasked to provide fundamental Linux server management to units needing such support, and which provides general cybersecurity services for Linux-based computers together with education and advice on Linux and cybersecurity for all on campus who use such operating systems. Let us mention that CU had such a *UnixOps* group within OIT already until about 15 years ago and that it was quite successful and highly regarded by faculty.

9.2.8 Use of open-source and host-based intrusion detection systems

The IT-FWG recommends the University to use open source and host-based intrusion detection systems for Linux servers instead of externally managed software for intrusion detection. The main reason for this recommendation is to avoid transfer of sensitive data/metadata to external servers as the current EDR solutions do. Examples of such privacy-respecting products include CrowdSec, OSSEC, and AIDE. Another useful software product in this spirit is dorkbot, which finds high-risk vulnerabilities (like e.g. SQL injections) in web applications based on publicly available data, and which is free for universities. Overall, the IT-FWG recommends that less intrusive response software is used for cybersecurity purposes on any computer, whether it runs Windows, MacOS, or Linux.

9.2.9 Heightened scrutiny for bundling

As discussed in section 6, software bundling is a strategic liability for customers (i.e., the University), ultimately leading to higher costs and increased lock-in. The IT-FWG recommends that procurement decisions consider this long-term risk and always conduct a comparison to leading non-bundled alternatives before settling on bundled options.

9.2.10 Transparency

The IT-FWG recommends transparency of discussions and decisions on IT matters as a fundamental principle. The process of proposing, negotiating, and procuring IT Solutions must be open and subject to review. We are a state institution subject to the Colorado Open Records Act and moreover, we owe transparency to our constituents including faculty, staff, students, alumni, and the people of the state of Colorado. IT vendor contracts must articulate critical items such as data privacy, and when, how, and by whom data privacy can be violated. Note that third-party services have been identified as a leading security threat for universities [Kos25], and thus merit high scrutiny. The contract terms must be publicly available. A vendor that refuses these terms is not suitable for the University of Colorado. Similarly, in order to ensure good stewardship of our public University dollars, the contracts and justifications for campus-scale IT service procurement, including costs and durations, must be publicly available. There must be a transparent process for proposed changes and soliciting feedback from users for substantial IT changes. We observe that recent changes such as migrating our email provider and cloud storage solutions, and removing phones from staff and faculty offices, were done with de minimis comment and no evidence that the comments returned were incorporated into the decision-making process. The same lack of transparency led to the current set of issues with the SCSC that must be corrected. These campus-wide operational choices, and the process by which we

arrived at them call into question the operational strategy of OIT leadership, which has not solicited feedback from broad campus groups and has actively resisted the questions from this Working Group.

9.2.11 Data collection, retention, and records requests

The IT-FWG recommends that data collection and retention policies for each software product be documented and shared. The University should develop a strategy to minimize exposure to open records-based harassment, including IT policies, and review its procedures for handling such requests in accordance with AAUP recommendations [PK25]. This process should be clearly documented for faculty and other campus workers and students to review, and should maximize their agency to recognize exemptions and to consider independent counsel to challenge requests.

9.2.12 Faculty representation on OIT governance board

Lack of faculty representation on IT governance boards, in particular the OIT Cabinet, is the main reason the SCSC was so mismatched with the university mission and unacceptable to faculty. After complaints about the lack of faculty involvement in critical IT matters by a member of the BFA Executive Committee, the OIT director included the BFA Chair as a permanent member of the Executive IT Governance Board. Even though that is a positive development, it is not a sufficient one because the major decisions are discussed and made within the OIT Cabinet where there is still no faculty representative. Not only has that been critized by CU's faculty, it even has been noticed from the outside. The former Trusted CI[5] director Jim Basney expressed in April 2024 in a video conference with a BFA member that faculty representation on IT governance boards of US universities is standard, that CU is lacking that, and that CU Boulder should have a faculty representative on the OIT Cabinet. The IT-FWG recommends that BFA-nominated research-active faculty representatives from a range of departments and institutes have permanent seats on the OIT Cabinet. Moreover, it is recommended that these faculty representatives are involved in all major decision making, especially those that implicate academic freedom. Parallel to this, it is recommended to the BFA to make the IT-FWG or the IT-faculty advisory committee a permanent one and establish it as a standing BFA committee specifically tasked with advising on the matter of academic freedom in regard to cybersecurity measures on campus from a faculty point of view.

9.2.13 Public comment process

Faculty have often been caught off-guard with policy mandates that have unintended consequences on their research and/or teaching activities. While faculty representation on the OIT Cabinet will increase transparency, we feel that a public comment period is necessary to ensure stakeholder voices be heard. The IT-FWG recommends that OIT collaborate with BFA to design a public comment process for significant OIT policy changes. The process shall serve a function similar to that of public comment in federal regulations, with the comments shared with BFA and jointly reviewed by the OIT Cabinet.

9.2.14 OIT career paths and organization structure

OIT does not provide sufficient career progression for technical staff, causing experienced technical staff to either transition into management or leave the university. The Boulder campus has transitioned, without public discussion, from providing a large variety of IT services internally to becoming extremely reliant on external vendors. This has led to a management-heavy organization with hollowed-out technical expertise and a substantially diminished staff morale—a state of affairs that is evident to faculty on our campus. The IT-FWG recommends deliberate restructuring of OIT strategy and institutional values to provide career progression for senior technical staff, to foster safe internal dissent, and to adopt a more collaborative posture toward faculty and other colleagues. The IT-FWG also recommends shifting resources to college-level IT leaders who report to the colleges, similar to those employed by some institutes and similar to the model at the University of Washington. Their role would be to work directly with faculty to understand nuanced research and teaching needs, to design solutions that balance security with the research and teaching mission, and to coordinate with OIT to

[5] Trusted CI, The NSF Cybersecurity Center of Excellence

understand implications and evolving threats. Our recommendation for a distribution of IT expertise across campus units is part of an overarching recommendation that communication between OIT and the people it supports must be improved. OIT has a current and unsustainable culture problem. It is unresponsive to its customers and mandating unworkable policies, seemingly without realizing this fact in spite of good-faith attempts by faculty to redirect course. As this report has laid out, there is no one-size-fits-all IT solution and therefore addressing campus IT needs will only occur as part of a sustained and ongoing dialog between OIT staff and campus users. This shift should occur as part of an organizational reimagining of OIT, accompanied by a modification to the OIT charter that preserves the principles addressed in this document.

9.2.15 Education and dialog

While faculty and system administrators who seek ”exceptions” or need to make ”opt-in” decisions should undergo training and/or assessment on standards, OIT decision makers should undergo training on academic freedom and how deeply it influences faculty members' ability to do their job. The IT-FWG endorses the Trusted CI recommendations regarding operation of a central IT security unit; see [CI21a, Section 6.1 Building a Relationship with Centralized IT] & [CI21b, Must 7: Cybersecurity Lead]. Such a central IT security unit should not only provide support in the case of an intrusion but provide education to various groups, in particular to system administrators and faculty in matters of cybersecurity and ways to improve it.

Jed Brown
Associate Professor, Department of Computer Science

Markus J. Pflaum
Professor, Department of Mathematics

References

[Ame19] American Library Association. *Library Bill of Rights*. 1939–2019. URL: https://www.ala.org/advocacy/intfreedom/librarybill.

[Ame40] Association of American Colleges. *1940 Statement of Principles on Academic Freedom and Tenure with 1970 Interpretive Comments*. 1940. URL: https://www.aaup.org/sites/default/files/1940%5C%20Statement.pdf.

[Asi25] Nanette Asimov. *UC Berkeley gives Trump administration 160 names in antisemitism probe*. 2025. URL: https://www.sfchronicle.com/bayarea/article/uc-berkeley-gives-160-names-antisemitism-probe-21043760.php.

[CI21a] Trusted CI. *Research at Risk: Ransomware Attack on Physics and Astronomy Case Study*. 2021. URL: https://scholarworks.iu.edu/iuswrrest/api/core/bitstreams/bbd1024b-c96c-425d-a310-d9bc7f384ec3/content.

[CI21b] Trusted CI. *The Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators*. 2021. URL: https://www.trustedci.org/framework/implementation.

[Col24] Colorado Department of Labor and Employment. *Interpretive Notice & Formal Opinion ("INFO") #15C: Speech and Organizing Rights for Government Employees under the Protections for Public Workers Act ("PROPWA")*. 2024. URL: https://cdle.colorado.gov/sites/cdle/files/INFO%20%2315C%20PROPWA%20accessible.pdf.

[DiR24] Renée DiResta. *Invisible Rulers: The People Who Turn Lies Into Reality*. PublicAffairs, 2024. ISBN: 978-1-5417-0339-1.

[DiR25] Renée DiResta. *Process as punishment: an American history of political spectacle*. 2025. URL: https://www.lawfaremedia.org/article/process-as-punishment--an-american-history-of-political-spectacle.

[DK13] Timothy Derdenger and Vineet Kumar. "The Dynamic Effects of Bundling as a Product Strategy". In: *Marketing Science* 32(6) (2013), pp. 927–859.

[Eub02] Donna R. Euben. *Academic Freedom of Professors and Institutions: The Current Legal Landscape*. 2002. URL: https://www.aaup.org/academic-freedom-professors-and-institutions.

[GMR18] N. Gandal, S. Markovich, and M.H. Riordan. "Ain't it "suite"? Bundling in the PC office software market". In: *Strategic Management Journal* 39(8) (2018), pp. 2120–2151.

[Ho25] Jennifer Ho. *Opinion: As a CU professor with non-native parents, I ask — When will you speak out?* 2025. URL: https://coloradosun.com/2025/05/09/opinion-colorado-professor-speak-out-federal-administration/.

[Kos25] Edward Kost. *The state of university cybersecurity: 3 major problems in 2025*. 2025. URL: https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges.

[KSC05] K.U. Kühn, R. Stillman, and C. Caffarra. "Economic theories of bundling and their policy implications in abuse cases: an assessment in light of the Microsoft case". In: *European Competition Journal* 1(1) (2005), pp. 85–121.

[Lak25] Nina Lakhani. "Scientists warn US will lose a generation of talent because of Trump cuts". In: *The Guardian* (2025). URL: https://www.theguardian.com/us-news/2025/jul/03/national-science-foundation-trump-cuts.

[Man25] Mandiant. *M-Trends 2025 Report*. Tech. rep. 2025. URL: https://services.google.com/fh/files/misc/m-trends-2025-en.pdf.

[Nat22] National Labor Relations Board. *Memorandum GC 23-02: Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights*. 2022. URL: https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and.

[Nat48] United Nations. *Universal Declaration of Human Rights*. 1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[NL23] Avital N. Nathman and Jake Lowe. “Protecting Academic Freedom with Transparent Funding: Challenging harmful donor influence”. In: *Academe Magazine* (2023). URL: https://www.aaup.org/academe/issues/winter-2023/protecting-academic-freedom-transparent-funding.

[Pea24] Joshua M Pearce. “Do Universities Investing In Technology Transfer Via Patenting Lose Money?” In: *Transfer Technológií Bulletin* 2 (2024), pp. 11–21. DOI: 10.52036/TTb2024211.

[Pea25] James Pearson. *Microsoft knew of SharePoint security flaw but failed to effectively patch it, timeline shows*. Reuters. 2025. URL: https://www.reuters.com/sustainability/boards-policy-regulation/microsoft-knew-sharepoint-security-flaw-failed-effectively-patch-it-timeline-2025-07-22/.

[PK25] Sachin S. Pandya and Isaac Kamola. *Responding to Freedom of Information (FOI) Requests at Public Universities*. 2025. URL: https://www.aaup.org/sites/default/files/Responding_to_FOI_Requests.pdf.

[PST25] Stephanie K. Pell, Josie Steward, and Brooke Tanner. *Privacy under siege: DOGE’s one big, beautiful database*. 2025. URL: https://www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/.

[SC10] Lisa Sutlieff and Jackie Chelin. “An absolute prerequisite: The importance of user privacy and trust in maintaining academic freedom at the library”. In: *Journal of Librarianship and Information Science* 42.3 (2010), pp. 163–177. DOI: 10.1177/0961000610368916.

[Uni25a] University of California Academic Senate. *Resolution on Use of Trellix and Similar Monitoring Software*. 2025. URL: https://senate.universityofcalifornia.edu/_files/reports/assembly-to-president-resolution-on-trellix.pdf.

[Uni25b] University of California Faculty. *Delay the UC cybersecurity mandate*. 2025. URL: https://sites.google.com/view/delay-mandate/.

[Uni25c] American Association of University Professors. *FAQs on Academic Freedom*. 2025. URL: https://www.aaup.org/issues-higher-education/academic-freedom/faqs-academic-freedom.

[Vic22] Office of the Vice Chancellor for IT at CU Boulder. *Secure Computing Standard for Computers*. 2022. URL: https://www.colorado.edu/information-technology/policy/it-standards/secure-computing-standard-computers.