

Academic Server Governance Policy

Background

Cleveland State University (CSU) has offered faculty access to an on-site server to host HTML based websites to be used as teaching supplements in academic courses. The server was located on the CSU network inside the firewall. The websites varied in nature from articles and book chapters to computational practice activities and code snippets. The websites have been traditionally supported by individual faculty members and many use custom HTML or similar coding and custom access configurations. The customized coding and settings made it very difficult for IS&T to centrally maintain appropriate safety and security standards, especially when websites fall out of use or are not regularly maintained by faculty and are mostly unmonitored by central administration. Websites were not required to use CSU branding or adhere to American with Disabilities Act requirements. The websites are accessible by the public and should represent CSU in a positive fashion. On occasion, the websites have hosted inappropriate or personal content that may have reflected poorly on the CSU image or branding.

The legacy code-based server is being phased out and replaced with a cloud-based content management system using WordPress. The new academic server system will offer a selection of CSU Branded templates to choose from and offer central security and account management. A selection of pre-approved functional WordPress plugins will be available for faculty to install. The templates will allow for a more standardized look to the webpages. The new academic server will not support customized HTML or similar code to avoid security access, virus and malware issues.

Further, there is a current initiative to advance the High Performance Computing (HPC) infrastructure at CSU. HPC machines are powerful, and users will need to act responsibly.

Purpose of the policy

This policy provides guidance for establishing expectations and limitations for responsible use and monitoring of the CSU Academic Technology resources to include the Academic Web Server at <https://academic.csuohio.edu>, also known as the Academic Multisite, the HPC cluster initiative and any future academic servers/resources implemented for general faculty use. The guiding principle behind the policy is that CSU will provide access for full-time faculty to a university system to post online content that must comply with professional standards, ADA law, responsible use of State assets, CSU digital identity guidelines, generally applicable laws, rules, and policies.

Policy details

As a part of the physical and social learning infrastructure, CSU acquires, develops, and maintains computers, computer systems, and networks. These computing resources are intended for university-related purposes, including direct and indirect support of the university's teaching, research/scholarship/creative activities, and service missions.

Cloud-based and hosted on a WordPress instance, the academic web server will provide online information to support faculty pursuit of teaching, scholarship, creative activity, innovation and service through the free exchange of ideas among members of the university community and between the university community and the wider local, national, and world communities. The webpages created on

the Academic web server are an extension of the CSU identity and should always adhere to professional standards.

The rights of academic freedom and freedom of expression apply to the use of university computing resources. So, too, however, do the responsibilities and limitations associated with those rights. The use of university computing resources, like the use of any other university-provided resource and like any other university-related activity, is subject to the requirements of legal, regulatory, and ethical behavior within the university community. Responsible use of a computing resource does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

All users of university computing resources must:

1. Comply with all federal, Ohio, and other applicable law; all generally applicable university rules, policies, and other governing documents; and all applicable contracts and licenses.
 - a. Examples of such laws, rules, policies, contracts, and licenses include: the Family Educational Rights and Privacy Act (FERPA); Health Insurance Portability and Accountability Act (HIPAA); laws governing libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit hacking, and similar activities; the Americans With Disabilities Act as reflected in the University's Digital Accessibility policy; Code of Student Conduct; Sexual Misconduct policy; Institutional Data policy; Information Security Incident Response Management policy; and all applicable software licenses.
2. Use only those computing resources faculty are authorized to use and use them only in the manner and to the extent authorized. For instance, they should not use the academic web server for personal content such as family photos, home videos or non-work-related data storage
3. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
4. Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
5. Respect the finite capacity of the computing resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there are no set bandwidths, disk space, CPU time, or other limitations applicable to all uses of university computing resources, the university may require users of

those computing resources to limit or refrain from specific uses in accordance with this principle, using only those resources authorized for use. The reasonableness of any particular use will be judged by the university in the context of the relevant circumstances.

6. Refrain from using those resources for personal commercial purposes or for personal financial or other gain.
7. Refrain from stating or implying that they speak on behalf of the university and from using university trademarks and logos without authorization to do so. Affiliation with the university does not, by itself, imply authorization to speak on behalf of the university.
8. The Academic web server has been established to utilize several pre-designed webpage templates. These templates comply with ADA color contrast, size and visual component requirements and align with CSU digital identity color schemes. As such, layouts, color pallets and content design may be limited to items allowed by the template.
9. The Academic web server shall not be used to run or host databases or custom code projects. Databases and custom code cannot be monitored for security risks by the IS&T team and may produce access points for data breaches, viruses, malware or intrusion.

Access, Termination of Access and Archival of Academic Server Resources

- Access to the Academic web server resources will be provided to all full-time faculty, including visitors.
- Login to the CSU servers will utilize the CSU Single Sign On (SSO) service
- Access to the CSU servers will terminate at time of separation, or 6 months after retirement from CSU
- Faculty granted Emeriti status will retain access to the CSU servers for an amount of time determined in the CSU Faculty Personnel policies 3344-16-08, which is currently 3 years
- After faculty access to the server has been terminated, the faculty website will be retained in the data archive per the data retention policy, or a minimum of 10 years, to comply with accreditation review cycles.

Monitoring and Usage

The CSU server usage will be monitored by IS&T through periodic security and maintenance scans. Any faculty activity found to pose an imminent security risk to the CSU computing infrastructure will immediately be deactivated and referred to the Office of the Provost and IS&T (as appropriate) for mitigation. Faculty activities that do not comply with this policy will be referred to the Office of the Provost for review, mitigation and/or revision.

Approval History:

11/18/2022 Approved by Academic Technology Committee

2/2/2023 Approved as Faculty Senate Policy by Faculty Senate