Background

A trusted and effective information technology environment (“IT environment”) is vital to the mission of University of Cincinnati. To that end, the university provides an IT environment which includes an array of institutional electronic business systems, computing services, networks, databases, and other resources (collectively, “IT@UC resources” or “resources”). These resources are intended to support the educational and work activities of members of the university’s academic community and their external collaborators, to support the operations of the university, to provide access to services of the university and other publicly available information, and to ensure a safe and secure IT operating environment to all members of the university community.

This policy is intended to define and promote the responsible use of information technology at the University of Cincinnati. Access to and usage of IT@UC resources entails certain expectations and responsibilities for both users and managers of the IT environment. These are stated below.

I. Applicability

1.1. This Policy applies to all individuals using IT@UC resources (“Users”), regardless of affiliation and irrespective of whether these resources are accessed from UC’s campus or from remote locations. Individuals covered by the policy include (but are not limited to) UC faculty and visiting faculty, staff, students, alumni, affiliates, guests or agents of the administration, external individuals and organizations accessing network services via UC’s computing facilities.

1.2. Within UC’s IT environment, additional rules will apply to specific computers, computer systems or facilities, software applications, databases and data sources, data types, or networks, and to the uses thereof, or to college/departmental workplaces, or to specific types of activities (collectively, “departmental rules”). Departmental rules must be consistent with this Policy, but also will impose additional or more specific requirements or responsibilities on Users.

II. Purposes and Appropriate Uses

2.1. IT@UC resources are provided for university-related purposes, including support for the university’s teaching, research, and public service missions, its administrative functions, and student and campus life activities.

2.2. Users are granted access to IT@UC resources for the purposes described in this Policy. Use is limited to those purposes, subject to Section 2.3.
2.3. Incidental Personal Use

2.3.1. Users may make incidental personal use of IT@UC resources, provided that such use is subject to and consistent with this Policy, including Article 3 of this Policy. In addition, incidental personal use of IT@UC resources by a User may not interfere with the fulfillment of that User’s job responsibilities or disrupt the work environment. Incidental personal use that inaccurately creates the appearance that the university is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

2.3.2. Users who make incidental personal use of IT@UC resources do so at their own risk. The university cannot guarantee the security or continued operation of any IT@UC resource.

III. User Responsibilities

3.1. When a User accesses university computing services, and accepts any university issued computing accounts, they agree to comply with this and all other computing related policies. All members of the university community are responsible for familiarizing themselves with any applicable policy prior to use.

3.2. Use of Resources Accessed through IT@UC Resources

3.2.1. When using IT@UC resources or resources owned by third parties that are accessed using IT@UC resources, Users must comply with all applicable federal and state laws, all applicable university rules, ordinances, and policies, and the terms of any contract or license which governs the use of the third-party resource and by which the User or the university is bound.

3.2.2. Intellectual honesty is of vital importance in the academic community. Users must not utilize IT@UC resources to violate copyright, patent, trademark, other intellectual property rights, or engage in plagiarism.

3.3. Users will not engage in unauthorized use of IT@UC resources, regardless of whether the resource used is securely protected against unauthorized use. Users will use only the computers, computer accounts, and computer files for which they have authorization.

3.4. Privacy of Other Users

3.4.1. Users are expected to respect the privacy of other Users, even if the devices and systems by which other Users access UC’s IT resources, the content other Users place on IT@UC resources, or the identities and privileges (rights to access and use certain systems and/or data), of other Users are not securely protected.

3.4.2. Unauthorized use by a User of another User’s personal identity or access (log-in) credentials is prohibited as is sharing of credentials between two or more Users per the UC Password Policy.

3.4.3 The university does not routinely monitor or inspect individual accounts, files, or communications.
3.5. IT@UC resources have a finite capacity. Users will limit their use of IT@UC resources accordingly and must abide by any limits UC places on the use of its IT resources or on the use of any specific IT resource. In particular, no User will use any IT resource in a manner which interferes with the core activities of the university or of other Users.

3.6 The university is bound by its contractual and license agreements respecting certain third party resources; Users are expected to comply with all such agreements when using such resources.

3.7. IT@UC resources will not be used to fundraise, advertise, or solicit unless that use is approved in advance by the university.

3.8. Partisan Political Activities

3.8.1. IT@UC resources will not be used to engage in partisan political activities on behalf of, or in opposition to, a candidate for public office.

3.8.2. IT@UC resources will not be used to promote or oppose the qualification, passage, or defeat of a ballot question that does not affect the university’s interests. IT@UC resources will not be used to promote or oppose the qualification, passage, or defeat of a ballot question that affects the university’s interests unless that use is approved in advance by the Office of the President.

3.8.3. These prohibitions do not apply to private devices that are attached to the university’s network, provided that IT@UC resources are not used in a way that suggests the university endorses or supports the activity originating on the private device. Personal devices will not disrupt university services and/or bypass university established controls and safeguards.

3.9. IT@UC resources will not be used to operate a business or for commercial purposes unless that use is approved in advance by the university.

3.10. IT@UC resources will not be used to support the operations or activities of organizations that are not affiliated with the university unless that use is approved in advance by the university.

3.11. Pornography and Sexually Explicit Content

3.11.1. Intentional access or dissemination of pornographic or other sexually explicit content by the members of university community is prohibited unless (1) such use is specific to work-related functions and has been approved by the respective manager (2) such use is pursuant to a formal university investigation or (3) such use is specifically related to an academic discipline, grant, or research project.

3.11.2. Certain types of pornographic material are deemed illegal by state or federal laws. The use of IT@UC resources to store, display, or disseminate contraband is absolutely prohibited. Any such use must be reported immediately to the UC Police Department.

3.12. Legal compliance

All members of the university community must obey:

- All relevant federal, state, and local laws. These include laws of general application, such as libel, copyright, trademark, privacy, obscenity, as well as laws that are specific to computers and
communication systems, such as the Computer Fraud and Abuse Act (CFAA), the Federal anti-hacking statute that prohibits unauthorized access to computers and the Electronic Communications Privacy Act (ECPA), currently under review by the Senate Judicial Committee to update the 1986 legislation especially with regards to digital due process and timelines.

- All relevant university rules and regulations. These include the Rules of the University, the Student Code of Conduct, the various collective bargaining agreements between the university and its employees, and all other university policies.
- All contracts and licenses to the resources made available to the users of information technology.
- This policy, as well as other policies issued for specific systems.
- All other applicable laws and regulations.

3.13. In operating its IT environment, the university expects Users to engage in "safe computing" practices, such as establishing appropriate access restrictions for their accounts, setting strong passwords and guarding those passwords, keeping their personal operating systems and software applications up-to-date and patched, and employing security measures on their personal devices. Additional measures are described in the Data Protection Policy, Password Policy, and Vulnerable Electronic Systems Policy, and other policies approved and posted on the IT@UC Office of Information Security website.

IV. Reporting and Enforcement

4.1. Use of IT@UC resources is a privilege and not a right. A User’s access to IT@UC resources may be limited, suspended, or terminated if that User violates this, or any other university policy. Alleged or suspected violations of this Policy will be addressed by the Office of Information Security and referred to the appropriate UC staff.

4.2. Reporting Violations

4.2.1 Anyone who becomes aware of a possible violation of this policy, other applicable policies, or the more specific regulations of the systems that comprise the virtual campus must notify the IT@UC Office of Information Security immediately.

4.3. Users who violate this Policy, other university policies, or external laws may also be subject to disciplinary action and/or other penalties. If an investigation involving review of the content of a faculty member, staff member, or student's files is required, written permission will be obtained from the Office of General Counsel and other departments, as necessary. Disciplinary action for violation of this Policy is handled through the university's normal student and employee disciplinary procedures and through unit heads, Human Resources, Office of General Counsel, UC Police Department, and other applicable departments.

4.4. In addition to its own administrative review of possible violations of this Policy and other university policies, the university is obligated to report certain uses of IT@UC resources to law enforcement agencies. See, e.g., Section 3.11.2.

4.5. Investigations of IT@UC systems or services misuse is limited only to the IT@UC Office of Information Security, or their designee.
4.6. If the IT@UC Office of Information Security determines that a User has violated this Policy, suspension, removal or disabling of the User account may occur. The IT@UC Office of Information Security will temporarily suspend or deny a User’s access to IT@UC resources when it is determined that such action is necessary to protect such resources, the university, or other Users from harm.

4.7. IT@UC Office of Information Security reserves the right to remove and/or disconnect any device from IT@UC resources/services if such device negatively impacts, or has the potential to negatively impact, university operations, as determined by the IT@UC Office of Information Security and later reviewed with the corresponding unit management.

V. Security and Operations

5.1. The university may, without further notice to Users, take any action it deems necessary to protect the interests of the university and to maintain the stability, security, and operational effectiveness of its IT resources. Such actions may be taken at the institutional or local level, and may include, but are not limited to, scanning, sanitizing, or monitoring of stored data, network traffic, usage patterns, and other uses of its information technology, and block of unauthorized access to, and unauthorized uses of, its networks, systems, and data. Additionally, the IT@UC Office of Information Security may investigate based on the request of Office of General Counsel, UC Police Department, Human Resources, Student Judicial Affairs, Research Integrity Officer, Office of Internal Audit, IT@UC leadership, Senior VP of Administration and Finance, Provost, or Office of the President.

5.2. Undetermined abnormalities in system, service, user, or network behavior can be investigated by the IT@UC Office of Information Security to determine implications on university resources. If a violation of any applicable laws, regulations, or policies is discovered during such an investigation, the IT@UC Office of Information Security will contact other appropriate university departments for further follow-up.

VI. Privacy


6.1.1. Responsible authorities at all levels of the IT@UC environment will perform management tasks in a manner that is respectful of individual privacy and promotes User trust.

6.1.2. Monitoring and Routine System Maintenance

6.1.2.1. The university will access IT resources as necessary for system maintenance, including security measures. The Network Operations Center (NOC), the IT@UC Office of Information Security and formally designated UCIT managers are authorized to monitor network traffic for malicious activity, suspicious patterns, and in the course of investigation. Additional campus IT administrators can be approved to access and monitor specific traffic on specific networks for which they are responsible. Authorization must be attained from the IT@UC Office of Information Security and the appropriate Network Operations Staff. The individual(s) must also complete a Non-Disclosure form and undergo a standard background check, if not already completed. This approval will also be communicated to the IT@UC Office of Information Security.
and the Network Operation Center (NOC). Authorized personnel must demonstrate a need for and an understanding of the operation of network monitoring devices.

6.1.2.2. The university’s routine operation of its IT resources may result in the creation of log files and other records about usage. This information is necessary to analyze trends, balance traffic, and perform other essential administrative tasks. The IT@UC Office of Information Security may store incident related data as required. The IT@UC Office of Information Security may store aggregated data and usage logs for operational, compliance, and statistical purposes.

6.1.2.3. No authorized personnel will use network monitoring devices to monitor employee electronic transmissions, conduct network scans, or access user data for job performance evaluation, or as part of an unofficial investigation, without first receiving approval from the IT@UC Office of Information Security. This requirement is not intended to interfere with routine operations of staff who are required to perform monitoring services to maintain the availability and integrity of the IT infrastructure.

6.1.3. The university may be compelled to disclose Users’ electronic records in response to various legal requirements, including subpoenas, court orders, search warrants, discovery requests in litigation, and requests for public records under the Ohio Public Records Law or by request of Office of General Counsel.

6.1.5. The university may disclose, at Office of General Counsel discretion, the results of any general or individual monitoring or inspection of any User’s record, account, or device to appropriate university authorities and law enforcement agencies. The university may also use these results in its disciplinary proceedings.

6.2. Provisions Regarding Inspections and Disclosure of Personal Information

6.2.1. The university will never disclose contents of communications to an outside entity unless formally instructed to do so by the Office of General Counsel and:

6.2.2.1. When so required by law. If necessary to comply with the applicable legal requirement, such disclosures may occur without notice to the User and/or without the User’s consent, as determined by the Office of General Counsel.

6.2.2.2. In connection with an investigation by the university or an external legal authority into any violation of law or of any university policy, rule, or ordinance. When the investigational process requires the preservation of the contents of a User’s electronic records to prevent their destruction, the Office of General Counsel may authorize such an action.

6.2.2.3. If it determines that access to information in an employee’s electronic account or file is essential to the operational effectiveness of a university unit or program and the employee is unavailable or refuses to provide access to the information.

6.2.2.4. If it receives an appropriately prepared and presented written request for access to information from an immediate family member or the lawful representative of a deceased or incapacitated User.
6.2.2.5. If it must use or disclose personally identifiable information about Users without their consent to protect the health and well-being of students, employees, or other persons in emergency situations, as formally instructed by UC Police Department, or to preserve property from imminent loss or damage, or as instructed by Office of General Counsel, to prosecute or defend its legal actions and rights.