THE UNIVERSITY OF TOLEDO
1872

Reset Form

Complete this application to request access to the University of Toledo's Financial Records System, known as FRS. An FRS user account is only necessary **when the generic user account 6999 is not sufficient**. You can obtain password information for 6999 by visiting https://utssl.utoledo.edu/university/FRSPsw.asp with a valid faculty or staff utad account.

Send the completed form to: FRS Security Officer, Mail Stop 454. Questions can be directed to Amanda Ki at 530-1375 or amanda.ki@utoledo.edu.

To be completed by applicant:			
Name (Last, First, Middle Initial):			
Social Security Number:			
Title/Position:			
Employee Status (Check One):	○ Faculty ○Staff ○Student Worker		
College/Department:			
Building/Room Number:		**Phone #:**	
Please tell us, why you need FRS: ☒ Look at Eprint phone bill reports.			
To be approved by Dept. Chair or Director:			
Print Name:			
Signature & Date:			
To be completed by Business System Support Office:			
Assigned ID/Pswd:		**Officer/Date:**	

Applicant MUST read and sign the Computer Usage Policy on the next page.

The University of Toledo Computer Usage Policy

Responsible Use of Information Technology

As a part of the physical and social learning infrastructure, The University of Toledo 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 instruction, research and service missions; of University administrative functions; of student and campus life activities; and of 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 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 and ethical behavior within the University community. Thus, legitimate use of a computer, computer system or network 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.

Applicability

This policy applies to all users of University computing resources, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems or networks provided or operated by specific units of the University. Consult the operators or managers of the specific computer, computer system or network in which you are interested for further information.

Policy

All users of University computing resources must:

- **Comply with all federal, Ohio and other applicable law**, all generally applicable University rules and policies, and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts and licenses include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking," and similar activities; the University's Code of Conduct; the University's sexual harassment policy; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.

- **Use only those computing resources which they are authorized to use** and use them only in the manner and to the extent authorized. 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. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the University.

- **Respect the privacy of other users and their accounts**, regardless of whether those accounts are securely protected. Again, 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.

- **Respect the finite capacity of those 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 is no set bandwidth, disk space, CPU time or other limit applicable to all uses of University computing resources, the University may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

- **Refrain from using those resources for personal commercial purposes** or for personal financial or other gain. Personal use of University computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other University responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

- **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. Authorization to use University trademarks and logos on University computing resources may be granted only by the Public Information Office. The use of appropriate disclaimers is encouraged.

Enforcement

Users who violate this policy may be denied access to University computing resources and may be subject to other penalties and disciplinary action, both within and outside of the University. Violations will normally be handled through the University disciplinary procedures applicable to the relevant user. For examples, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, by the Office of Student Judicial Affairs. However, the University may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of University or other computing resources or to protect the University from liability. The University may also refer suspect violations of applicable law to appropriate law enforcement agencies.

Security and Privacy

The University employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the University cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly.

Users should also be aware that their uses of University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities which are necessary for the rendition of service. The University may also specifically monitor the activity and accounts of individual users of University computing resources, including individual log in sessions and communications, without notice, when (1) the user has voluntarily made them accessible to the public, as by posting to Usenet or a web page; (2) it reasonably appears necessary to do so to protect the integrity, security or functionality of University of other computing resources or to protect the University from liability; (3) there is reasonable cause to believe that the user has violated, or is violating, this policy; (4) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (5) it is otherwise required or permitted by law. Any such individual monitoring, other than that specified in (1) above or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer or the Chief Information Officer's designee. The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings. Communications made by means of University computing resources are also generally subject to Ohio's Public Records Statute to the same extent as they would be if made on paper.

Sign to indicate acknowledgement and agreement to the computer usage policy	
Applicant Signature & Date:	