FERRIS STATE UNIVERSITY

DIVISION OF ADMINISTRATION AND FINANCE

Proper Use of Information Technology Resources

Administration and Finance Business Policy

Policy Number: 2025:05
Supersedes: 2017:04

SCOPE

This policy applies to anyone using any University Information Technology (IT) Resource. This includes, but is not limited to, University employees, affiliates, student employees, students, alumni, vendors, emeriti, retirees, guests, and contractors.

POLICY STATEMENT

Intended Uses

The intended uses of University IT Resources are to support the University's educational mission, daily operations, and legitimate business needs.

Personal use of IT Resources is acceptable as part of the daily learning and work of all members of the University community, if the use does not violate any University policies or applicable local, state, or federal laws and/or regulations. Use by an employee for other than work-related matters must not prevent the employee from attending to and completing work effectively and efficiently. Individual departments or units may place additional restrictions on employees' personal use of IT resources.

Service providers may have their own acceptable use policies or agreements. It is the user's responsibility to adhere to their agreements or policies. The University cannot and will not extend any protection to a user should the user knowingly violate the policies of an external network.

Any individual or entity using IT Resources consents and agrees to comply with all of the terms and conditions set forth in this policy, all other applicable University policies, and applicable local, state, or federal laws and regulations.

Prohibited Acts

The following are prohibited:

1. Any attempt to circumvent any security measure of the University or another entity.
2. Intentional use, distribution, or creation of viruses, worms, or other malicious software.
3. Unauthorized copying or distributing of licensed software, or copyright-protected or patent-protected material.
4. Any attempt to access IT Resources or data without appropriate authorization and authentication.
5. Without authorization, destroying, altering, dismantling, disfiguring, preventing rightful access to, or otherwise interfering with the integrity of IT Resources.
6. Without authorization, invading the privacy of individuals or entities that are creators, authors, users, or subjects of the IT Resources.
7. Use of IT Resources that disables other IT Resources, negatively impacts University business or materially increases the costs of IT Resources or interferes with the intended use of the IT Resources.
8. Develop or use any unauthorized mechanisms to alter or avoid charges levied by the University, or its service providers, for computing, network, printing, or other services.
9. Use of IT Resources for financial gain and/or commercial purposes, without prior authorization.
10. Network scanning, or doing security research (University People, Processes or Technology), without explicit, written permission from the CIO, Vice President for Administration and Finance, or Office of the General Counsel is prohibited.

The above list is not intended to be exhaustive but rather provides some illustrative examples.

IT Equipment

Damage: If computing equipment is damaged, it should be reported immediately to the Information Technology Solution Center. The IT Solution Center will generate a work order to assess the damage. The guardian department may be charged for the repair or replacement if the damage is not covered under warranty. Repair and replacement costs vary and are subject to change. This includes, but is not limited to, desktops, laptops, monitors, mobile devices and other IT equipment.

Negligence: In cases of negligence the guardian department may seek reimbursement from the employee to cover the cost of repair or replacement.

Any damage to or negligent use of IT equipment by University employees may be subject to the Violations/Sanctions section of this policy.

IT SECURITY ASSESSMENT & ACTIVITIES

Anyone under contract with the University to perform IT security assessments will need to have written authorization from the Chief Information Officer or designee, a defined scope, and defined rules of engagement before performing any work on University owned systems, services, or equipment.

Educational, academic, and other IT security research (University People, Processes or Technology) activities using University IT Resources may only be conducted in a controlled, designated, and segmented network environment. This means that any work being done will not access any services or systems the rest of the University uses.

IT Services Security Team will collaborate with the Institutional Review Board to ensure the protection of intellectual property of research projects through an IT Security Assessment (University People, Processes, or Technology).

Warranty of Service
The University makes no warranties of any kind, whether expressed or implied, with respect to the IT Resources it provides. The University will not be responsible for damage resulting from the use of IT Resources, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a University employee, or by any user's error or omission. The University specifically denies any responsibility for the accuracy or quality of information obtained through IT Resources, except material that is presented as an official University record.

Violations/Sanctions

Suspected or known violations of this policy or applicable laws must be reported to Information Technology Services (the IT Solution Center), and if applicable, an employee's supervisor. Suspension of access to University IT Resources may occur while a suspected violation is investigated.

Any person found to have knowingly violated this policy will be subject to appropriate disciplinary action as defined by current University policy, student code of conduct, and/or collective bargaining agreements. Access to University IT Resources may also be permanently removed. When appropriate, University authorities and/or law enforcement agencies may conduct an investigation into the incident. Legal action may be taken when local, state, federal, or other laws or regulations have been violated.

DEFINITIONS

Information Technology Resources (IT Resources)
All facilities, technologies, equipment, devices, data, and information Resources used for University information processing, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic communications devices and services, e-mail, networks, telephones (including cellular), voicemail, fax transmissions, video, multimedia, and instructional materials. This also includes services that are University owned, leased, operated, or provided by the University or otherwise used as a University IT Resource, such as cloud and Software-as-a-Service (SaaS), third party hosted web pages, or any other connected/hosted service. Note that this definition is not all-inclusive, but rather reflects examples of electronic Resources, equipment, and services.

Security Measure
Processes, software, and hardware used by system and network administrators to ensure the confidentiality, integrity, and availability of information technology resources and data. Security measures may include reviewing files for potential or actual policy violations and investigating security-related issues.

University
Includes Ferris State University, Kendall College of Art and Design, on-line and statewide campuses.

User
Individuals or entities permitted to use University IT Resources.

Service Provider
Any group or organization that enables technology for our Users, including vendors that provide cloud solutions, contracted services, etc.

Data
Information collected, stored, transferred, or reported for any purpose, whether electronically or hard copy.

Guardian Department
The Ferris State University Department that is assigned the equipment for use in university related work.

RESPONSIBILITIES

Users

- Use University IT Resources in compliance with all applicable laws and regulations, as well as University policies.
- Report violations of this policy and/or suspected IT Security Incidents immediately to the IT Solution Center.
- Be familiar with and consult online security standards and technical reference materials as applicable to their use of IT Resources.
- Physically secure and safeguard IT Resources within the user's possession and control depending on the classification of the data that they process, and the systems they access.

Information Technology Services and other IT Resource Owners

- Implement and monitor compliance with this policy and related standards on IT Resources within their areas of responsibility.
- Ensure that reasonable measures have been taken to secure IT Resources within their areas of responsibility. IT Resources may require differing levels of security depending on the classification of the data that they process, and the systems they access.

Service Providers

- All entities connected to or accessing University owned networks, systems, services, or equipment must comply with this policy and extend compliance to users in the systems and services they provide.

OTHER RESOURCES

Please see the University Business Policy site for related policies, guidelines, and more
https://www.ferris.edu/policies/

Employee Dignity/Harassment/Discrimination
https://www.ferris.edu/policies/docs/EmployeeDignity.pdf

Code of Student Community Standards
https://www.ferris.edu/student-life/student-conduct/Student-Code.htm

Confidential Data Security Agreement Form
https://www.ferris.edu/administration/adminandfinance/human/Forms/NewEmployee/SecurityAgreement.pdf

FEDERAL, STATE & OTHER APPLICABLE LAWS & REGULATIONS

Computer Fraud and Abuse Act
https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

IRB requirement for research
http://www.ferris.edu/HTMLS/administration/academicaffairs/vpoffice/IRB/homepage.htm

CONTACTS

For more information, please contact the following departments:
Associate Vice President & Chief Information Officer

Amanda Matheson
Vice President for Administration & Finance