Acceptable Use of Information Technology Resources Policy

Authority: Information Technology

Date Enacted or Revised: Enacted February 2016; Revised July 2016; October 24, 2018; May 15, 2019; June 7, 2022; February 2, 2023

Overview

McNeese State University provides access to Information Technology (IT) resources in support of its vision, mission, philosophy and responsibility for education, research and service in Southwest Louisiana. Accordingly, the University encourages and promotes the use of these resources by the University community, within institutional priorities and financial capabilities. Access to, and use of, these resources and services are privileges which must be accepted in strict compliance with all applicable laws and with the highest standards of ethical and professional behavior.

Purpose

The purpose of this policy is to guide all users in the acceptable use of IT resources at McNeese State University.

Definition

IT resources at McNeese State University include, but are not limited to, the following:

- Computers and mobile devices;
- Network infrastructure, both wired and wireless;
- Software;
- Physical facilities;
- Data communications systems and services; and
- Support personnel.

Scope

This policy applies to anyone utilizing McNeese IT resources, whether affiliated with the University or not. This policy is applicable to all users regardless of the following:

- Ownership (University or personally owned computer or device);
- Location (on or off campus); and
- Method of connectivity (wired or wireless).

Policy

User Responsibilities

- Users must abide by all federal, state, and local laws.
- Users must abide by all applicable copyright laws and may be held personally liable for any infractions.
- Users must abide by all license agreements including legal restrictions of use and copying.
- Use of IT resources for the purpose of lobbying that connotes University involvement or endorsement of any political candidate or ballot initiative is not permitted.
- Use of IT resources for personal commercial purposes or for personal economic gain is not permitted.
- Use of IT resources to gain unauthorized access to anything is not permitted.
- Disruptive use of University IT resources is not permitted.
- Users may not manipulate or augment the University network infrastructure without prior approval.
- Users may not intentionally damage, or render useless, any equipment, software, or data.
- Users shall only use equipment, accounts, passwords, and services for which they have authorization.

- Users shall not allow unauthorized users to access IT resources, which includes sharing login credentials for any accounts for which they have authorization.
- Users are reminded that use of IT resources may not materially and substantially disrupt University functions or another University member's use of technology resources, or violate the law.

Note: While McNeese strives to provide access to computer labs and other technology, it is the student's responsibility to ensure adequate access to the technology required for a course. This may include access to a computer (not Chromebooks, iPads, etc.), webcam, internet, adequate bandwidth, etc. This requirement is a standard expectation for all courses regardless of initial course delivery format.

Policy Administration

- The University does not generally monitor or limit access to the campus network. However, it reserves the right to monitor, access, and review information under certain conditions such as a court order, subpoena, or other legally enforceable discovery request.
- The University may suspend, block, or restrict access to an account when it appears necessary to do so.
- Communications made concerning University business are subject to Louisiana Public Records Law and retention requirements.
- Individual units within the University may define additional conditions for acceptable use of resources under their control which are consistent with this policy statement, and which may provide additional detail, guidelines, and restrictions.

Internet Monitoring and Filtering

Website Monitoring

The Office of Information Technology shall monitor Internet use of all computers and devices used for instructional and University business purposes and connected to the corporate network. For all traffic, the monitoring system will record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

Internet Use Filtering System

The Office of Information Technology shall block access to Internet websites and protocols that violate state, local, or federal law or that substantially disrupt or interfere with the University's educational mission. The following protocols and categories of websites should be blocked:

- Advertisements and pop-ups;
- Gambling;
- Hacking;
- Illegal drugs;
- Unlawful peer-to-peer file sharing;
- Spam, phishing, and fraud; and
- Spyware.

Internet Use Filtering Rule Changes

The Office of Information Technology shall periodically review and recommend changes to web and protocol filtering rules to the chief information technology officer (CITO). The CITO will recommend any changes to Senior Staff, which shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in this policy.

Internet Use Filtering Exceptions

If a site is misclassified as inappropriate, employees may request the site be unblocked by submitting a ticket to the Information Technology help desk. The CITO will review the request and unblock the site only if it is misclassified.

Employees may access blocked websites, with permission, if appropriate and necessary for business purposes. If an employee has a business need to access a website that is blocked and appropriately categorized, the employee may submit a written request for approval to their immediate supervisor who will request approval from their division's vice president. The request shall include the person making the request, the website name, a website content description narrative, the business reason for the request, and the time period that access is needed. Once appropriately approved, the requesting employee shall present the approved exception request to the Office of Information Technology in writing. The Office of Information Technology will unblock that site or category for that employee and for the approved time period only. If approval is for a specific time period, IT will re-establish the website block when time expires.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any student who violates this policy will be subject to appropriate disciplinary action in accordance with the Student Handbook.

Any individual affiliated with the University who violates this policy will be subject to appropriate corrective action, including but not limited to termination of the individual’s relationship with the University.

Policy Compliance

Users found to have violated this policy may be subject to the following:

- Suspension of access to IT resources
- Penalties and disciplinary action, including expulsion or dismissal
- Referral of suspected violations of law to appropriate law enforcement agencies for further investigation or action

Inquiries or Reporting Violations

Office of Information Technology

West Annex (IT Building), 106-C

337-475-5524

Communication

This policy is distributed via the Administrative Advisory Council and the University Policies webpage.