

[DONATE](#)

Information Technology Policy and Procedures

- [Acceptable Use Policy](#)
- [Acceptable Encryption Policy](#)
- [Data Center Access Policy](#)
- [Email Policy](#)
- [IT Audit Policy](#)
- [Lab Policies](#)

ACCEPTABLE USE POLICY

1. OVERVIEW

Information Technology's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Nicholls State University's established culture of openness, trust and integrity. Information Technology is committed to protecting Nicholls State University's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Nicholls State University. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Nicholls State University employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at Nicholls State University. These rules are in place to protect the employee and Nicholls State University. Inappropriate use exposes Nicholls State University to risks including virus attacks, compromise of network systems and services, and legal issues.

3. SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Nicholls State University business or interact with internal networks and business systems, whether owned or leased by Nicholls State University, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Nicholls State University and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Nicholls State University policies and standards, and local laws and regulations. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Nicholls State University, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Nicholls State University.

4. POLICY

4.1 General Use and Ownership

4.1.1 Nicholls State University proprietary information stored on electronic and computing devices whether owned or leased by Nicholls State University, the employee or a third party, remains the sole property of Nicholls State University. You must ensure through legal or technical means that proprietary information is secured and protected.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Nicholls State University proprietary information.

4.1.3 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult the Department of Information Technology.

4.1.4 For security and network maintenance purposes, authorized individuals within Nicholls State University may monitor equipment, systems and network traffic at any time, per Information Technology's **Audit Policy**.

4.1.5 Nicholls State University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as public, internal or confidential as defined guidelines, details of which can be found in this series of documents. Examples of confidential information include but are not limited to: student information (grades, transcripts, enrollment, identification numbers, etc.) financial information, identification information of employees, and research data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.

4.2.2 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4. Postings by employees from a Nicholls State University email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Nicholls State University, unless posting is in the course of business duties. d not necessarily those of Nicholls State University, unless posting is in the course of business duties.

4.2.5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.2.6. Use encryption of information in compliance with the Office of Information Technology Security's Acceptable Encryption Use policy.

4.2.7. All hosts used by the employee that are connected to the Nicholls State University Internet/Intranet/Extranet, whether owned by the employee or Nicholls State University, shall be continually executing approved virus-scanning software with a current virus database.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Nicholls State University authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Nicholls State University-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Nicholls State University.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Nicholls State University or the end user does not have an

software for which Nicholls State University or the end user does not have an active license is strictly prohibited.

- Accessing data, a server or an account for any purpose other than conducting Nicholls State University business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Nicholls State University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Nicholls State University account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to Information Technology is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account

- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Nicholls State University network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Nicholls State University employees to parties outside Nicholls State University.
- Commercial use of IT Systems and equipment for non-Nicholls State University purposes is generally prohibited, except if specifically authorized and permitted under University conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of ideas that furthers the University's educational, administrative, research, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.
- Violations of Nicholls State University, University of Louisiana System, or Board of Regents policies, or local, state, or federal laws.

4.3.2 Email and Communication Activities

- When using University resources to access and use the Internet, users must realize they represent the University. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of Nicholls State University". Questions may be addressed to the IT Department
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.

- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Nicholls State University's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Nicholls State University or connected via Nicholls State University's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5. POLICY COMPLIANCE

5.1 Compliance Measurement

The Information Technology team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Information Technology team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. In addition to University discipline, users may be subject to criminal prosecution under federal, state or local laws; civil liability; or both for unlawful use of any IT System.

6. RELATED STANDARDS, POLICIES AND PROCEDURES

- [IT Audit Policy](#)
- [Acceptable Encryption Policy](#)

LAST REVISED: 09.2019

APPLY


DONATE

Follow Us



 **1-877-NICHOLLS**

 **CONTACT US**

 **906 East 1st Street**
Thibodaux, LA 70301

QUICK LINKS

[Nicholls Email](#)

[Moodle](#)

[Banner](#)

[Grades First](#)

[Faculty & Staff Directory](#)

[Employment](#)

CAMPUS LINKS

[Library](#)

[Emergency Preparedness](#)

[IT Help Desk](#)

[Nicholls Police](#)

[Book Store](#)

[Athletics](#)

[Rec Center](#)

[Housing](#)

RESOURCES

[A-Z Index](#)

[Non-Discrimination Policy](#)

[Privacy Notice](#)

[Title IX](#)

[Campus Safety Statistics](#)

[ADA Information](#)

[Diversity & Inclusion](#)

[Calendars](#)

SIGN-UP FOR INSIDE NICHOLLS NEWSLETTER

Inside Nicholls State University is a weekly email newsletter that is distributed to the campus community communicating Nicholls News and Events.

SUBSCRIBE TODAY!

Member of the University of Louisiana System