PLAN for the PROTECTION of the INSTITUTION’S TECHNICAL INFRASTRUCTURE

REID STATE

TECHNICAL COLLEGE

2023

The Reid State Technical College plan for the protection of the institution’s technical infrastructure governs electronic communication conducted through the College’s structured and wireless computing and telephone services, including local area, wide area and interconnected networks, owned host systems, personal computers, laptops, printers, software, communication devices, and network resources. Reid State Technical College strives to provide high-speed access to the Internet, email, and network services for its students, faculty, staff, and community partners. Its usage is intended for individuals legitimately affiliated with the College to facilitate the exchange of information consistent with the academic, educational, and research purposes of the institution.

The college’s network/Internet provides students with a quality learning environment by promoting a flexible delivery method of instruction, innovative technology, and state-of-the-art concepts in instruction. It also contributes to a growth-oriented learning environment for employees by promoting faculty and staff professional development opportunities. Through efficient management of the college’s network/Internet resources and facilities, Reid State Technical College serves as a learning partner for its community and regional stakeholders. In addition, the college’s technology infrastructure and resources support the college’s administrative and operational processes, thereby strengthening its outreach, programs, and services.

Access to the Reid State Technical College Network System shall be provided on an as-is basis with no guarantee of quality or availability. Network access is dependent on the availability of network bandwidth and related equipment. Instructional classes are given priority in the usage of equipment, bandwidth, and all other technology resources. As a condition of access to the network/Internet resources, employees are required to use their User ID and password provided by the Computer Services Department. Employees, students, and Community members who engage in use of the Reid State Technical College Network System are doing so under the College's Statement of Network Use Policy.

Employees who violate this agreement are subject to disciplinary actions, up to and including discharge in accordance with institutional and state policies. Students who violate this agreement are subject to disciplinary action as stated in the Student Handbook. Community members who violate this agreement while utilizing open campus computers and/or Wi-Fi are subject to being banned from using the college's equipment and Internet access.

All network access using Reid State Technical College time, equipment and/or resources will be administered by and coordinated through the Computer Services Department. Reid State Technical College reserves the right to monitor, collect and store all electronic activity conducted on the Reid State Technical College Network without consent or notification. Use of the Reid State Technical College network or computer resources constitutes acceptance of such monitoring. The Computer Services Department reserves the right to access any user's account, electronic files, or transmissions for administrative purposes including archiving, system maintenance and repair, or as directed by the college president, designee, or employee's supervisor. The Computer Services Department also reserves the right to suspend use of an account in the event the employee's password has been compromised, the employee is in violation of this network access policy, or as directed by the college president, designee, or employee's supervisor.

Statement of Network Use Policy:

1. Ethical and Responsible Use of the Network/Internet

a. Usage of the Reid State Technical College Network System is on an at-will basis. Reid State Technical College and the Computer Services Department will not be responsible for any damage to personal property from the use of the Reid State Technical College Network System.

b. The Reid State Technical College Network System – including email service, internet service, and college-provided equipment – is the property of the State of Alabama and is not intended for personal use. It is not acceptable to use College resources for purposes which violate any federal or state law or College Policy; are harmful or harassing to others; disrupt normal network use and service; execute for-profit commercial activities or business transactions; or constitute political campaigning.

c. All users are accountable for use of resources in an effective, ethical, and lawful manner. Users are prohibited from accessing the Internet for any unethical or immoral purpose, including any activity associated with pornography, obscenity, violence, gambling, racism, harassment, personal gain, or any illegal activity. Users are discouraged from using profanity or vulgarity when posting electronic mail via the Internet or posting to public forums (i.e., newsgroups, social media, etc.). Any electronic mail sent through postings to public newsgroups, social media, etc. must fall within these ethical standards.

d. All users must abide by all federal and state laws with regard to information sent through the Internet. Unauthorized release or disclosure of information through the Internet or through any other means is strictly prohibited. Proprietary or confidential information pertaining to the college shall not be transmitted over the Internet.

e. Users are forbidden from engaging in any activity which is in violation of the Code of Alabama (1975) §§ 36-25-1 through 36-25-30, as amended (the “State Ethics Law”), or which, in the opinion of the Reid State Technical College administration, may be contrary to such law.

2. User Access/Password Assignment, Confidentiality and Security

a. Under the terms of this policy, employees and students of the College are given access to the Reid State Technical College Network System. If network resource access (such as network attached storage or email) is required, a user ID and password will be assigned to the employee or student by the Computer Services Department.

b. The username and password, including those used to access email or an instructional platform such as CANVAS, are the responsibility of the individual to whom they are assigned. All individuals are responsible for network account use and password confidentiality. Use of an employee account by another employee or student is prohibited. Any individual other than the person to whom they are assigned shall not use the username and password or any other assigned authorization. Violations of this policy or any other policy through the unauthorized use of the username and password subjects the individual to whom the username and password are assigned to disciplinary actions, up to and including discharge.

c. Users should not leave a computer logged on when vacating a workstation. The user is responsible for his or her account and any content left on the computer.

Leaving an unattended logged-on computer puts the user and the institution at risk.

d. In the event Reid State Technical College no longer employs an individual, it is the responsibility of the Computer Services Department to close the former employee’s account.

e. Proper identification must be used in any electronic correspondence, and valid, traceable identification provided if required by applications or servers within the Reid State Technical College computing facilities.

3. Software

a. To prevent computer viruses from being transmitted through the system, no unauthorized downloading or installation of any software is permitted. Software downloads and installation shall be done only after approval and/or assistance from the appropriate Computer Services Personnel.

b. Streaming media and music and video downloads are prohibited unless authorized by the appropriate Computer Services Personnel.

c. Point to point (P2P) file sharing is prohibited unless authorized by the appropriate Computer Services Personnel.

4. Copyright Issues

a. All college network/Internet users must adhere to the copyright laws regarding software, data, and authored files. Users may not transmit copyrighted materials belonging to entities other than this college. Users should exercise caution when downloading material from an Internet source as such action may constitute violation of copyright laws.

b. It is permitted for Web pages to be printed and material downloaded from the Internet for informational purposes as long as the purpose for such copying falls into the category of "fair use." "Fair use" is defined as the doctrine that copyright material may be quoted verbatim, provided that attribution is clearly given and that the material quoted is reasonably brief in extent.

c. The college is not responsible for copyright infringement by a user. Such responsibility shall lie solely with the user.

d. Users found guilty of copyright infringement shall be subject to disciplinary action, including possible suspension, expulsion, or termination.

e. Congress enacted the No Electronic Theft (NET) Act in 1997. The NET Act makes it a federal crime to reproduce, distribute, or share copies of electronic copyrighted works such as songs, movies, or software programs, even if the person copying or distributing the material acts has no intention of receiving profit. Electronic copyright infringement carries a maximum penalty of up to three years in prison and a $250,000 fine.

   For more information on the NET Act, go to http://www.riaa.com/physicalpiracy.php?content_selector=piracy_online_the_law

5. Personally Owned Computer Hardware/Software

   a. Personally owned software cannot be loaded onto a college-owned computer unless it is directly related to the job position and is approved by the appropriate Computer Services Personnel. If any approved personally owned computer software is loaded onto a college-owned computer, the license and documents must remain with the college computer on campus in the event of an audit. Computer hard drives may not be installed or removed without the express written consent of authorized Computer Services Personnel.

6. Privacy of Information
    a. Information passing through or stored on any Reid State Technical College electronic network or computer system may be seen by others for a variety of reasons. Routine administration, management, or audit functions may require information stored or transmitted via Reid State Technical College computers and networks to be intercepted or monitored. Electronic transactions may be subject to seizure and inspection by Reid State Technical College without notice. All users should fully understand that except where protected by state or federal law, or by college policy, no expectation of privacy may be assumed concerning information communicated over or stored on Reid State Technical College electronic systems.
7. Users should respect the privacy of others, including, but not limited to, abstaining from unauthorized access to email, files, data, and transmissions.
8. All users should be aware of and comply with the safety of information as applies to the Family Educational Rights and Privacy Act (FERPA) as well as its restrictions on the use and dissemination of personal and academic information.
9. Best Security Practices helps to decrease the risk of information security breaches. It is the responsibility of each individual with access to the network to follow basic computer safety guidelines listed below. These best practices are a general guideline based on industry standards for information security. All users of the network should familiarize themselves with the following guidelines:

- Use complex passwords that cannot be easily guessed and protect the passwords.
- Beware of scams.
- Secure your area before leaving it unattended.
- Secure laptops and mobile devices at all times.
- Secure memory sticks.
- Lock or log off computers or other devices before leaving them unattended, and make sure they require a password to start up or wake up.
- Make sure your computer has adequate anti-virus software and that patches and updates are current.
- Protect portable and mobile devices.
- Do not install or download unknown or unsolicited programs to Reid State Technical College computers.
- File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing private or confidential information should be immediately removed from the printer.
- Upon disposal, restricted and/or sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Only install apps from trusted sources.
- Keep your device's operating system updated.
- Don't click on links or attachments from unsolicited emails or texts.
- Avoid transmitting or storing personal information on any device.

- Keep sensitive data (e.g., SSN's, credit card information, student records, health information, etc.) off of your workstation, laptop, or mobile devices.
- Securely remove sensitive data files from your system when they are no longer needed.
- Always use encryption when storing or transmitting sensitive data.
- A void visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically, and often silently, compromise your computer.
- If attachments or links in an email are unexpected or suspicious for any reason, don't click on them.
- Phishing scams can be carried out by phone, text, or through social networking sites -but most commonly by email.
- Be suspicious of any official-looking email message or phone call that asks for personal or financial information.

Measures of Protection

Reid State Technical College utilizes the following measure to protect the privacy, safety, and security of the network and the information contained therein:

- Firewall, Governed in the Data Center by Alabama Community College System Office.
- Secure login of an eight-character complex rule password.
- Off Site Back-up Storage and recovery through Software vendors and contract with The Solutions Team
- Antivirus, spyware, malware, and security software with FortiEDR and Windows Defender
- College approved software installed by the IT department.

Computer Crimes

The Alabama Computer Crime Act, codified at Code of Alabama (1975) § 3A-8-100 through 13A-8-103, makes it a crime for a person to damage, or without authorization to modify computer equipment, computer networks, and computer programs and supplies or without authorization to access, examine, or use computer data and programs, and provides for punishment up to a Class B Felony. Federal law also makes it a crime to access computers or computer networks devoted in part to Federal purposes without proper authorization.

Furthermore, this policy prohibits various actions (described below) which may or may not constitute a crime.

Backup and Recovery

All covered data and information is copied onto secure storage media on a regular basis for the purpose of recovery. The Backup Policies and Procedures state that requirements for backup and recovery. Reid State technical College also has an off-site back up that backs up all covered data and information and most of the high-volume file shares nightly.

Unacceptable Use

The following activities are prohibited on all Reid State Technical College technology resources. The activities listed are for reference and are not intended to be all-inclusive.

- Altering system software or hardware configurations without authorization of the Reid State Technical College Computer Services Department.
- Accessing, via the internet or any other means of broadcasting, pornographic, obscene, or violent images or content or any other material in violation of local, state, and federal statutes. Use of resources for gambling, racism, harassment or political campaigning is also prohibited.
- Using technology resources for illegal activities.
- Accessing or attempting to access another user's files, email or other resources

without his or her permission except as otherwise provided herein.

- Allowing unauthorized persons to utilize an authorized user’s account, username, or password.
- Using technology resources for commercial or profit-making purposes without written authorization from Reid State Technical College.
- Installing, copying, distributing or using software that has not been authorized by the Reid State Technical College Computer Services Department.
- Originating or proliferating electronic mail, broadcasts, or other messages that may be deemed as obscene, abusive, racist, or harassing.
- Creating and/or distribution of viruses or other destructive programs.
- Unauthorized release or disclosure of any confidential college, personnel, or student information.
- Using any computer technology in a manner that violates patent protection or license agreements. Engaging in any activity that violates copyright laws.
- Such activity may include utilizing Reid State Technical College technology to copy and/or distribute copyrighted materials without authorization.
- Using Reid State Technical College computer technology to support or oppose any candidate or candidates for public office or for any other political purposes. (Use of state property for political purposes constitutes a violation of Alabama law).

Disciplinary Action

Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as discipline or legal sanctions under federal, state, and local laws. Students who violate this policy are subject to disciplinary actions, up to and including expulsion from the college.

Employees who violate this policy are subject to disciplinary actions, up to and including discharge in accordance with guidelines provided by institutional and state policies.

Plan Governance

The plan shall be governed by the policies of Reid State Technical College and the laws of the state of Alabama and is created and amended under the authority of the Technical Infrastructure/Technology Committee. The plan is evaluated annually, revised as necessary, and is available to the administration, faculty, and staff of Reid State Technical College. The plan can be accessed via the Reid State Technical College Website > About RSTC > College Reports/Data and Plans. Failure to enforce any provision of this agreement shall not constitute nor be construed as a waiver of such provision or of the right to enforce such provision.