Saint Augustine's University Security Policy
Center for Information Technology

Contents

1. Scope

All employees and personnel that have access to University computer systems, databases, network and data must adhere to the approved application policy to protect the security of the network, data integrity, and computer systems.

2. Purpose

The purpose of this policy is to protect University resources on and accessed to the network by requiring all network users to only run or install application programs deemed safe by the Center for Information Technology (CIT) department.

3. Definitions

- **CIT:** Center for Information Technology
- **Sensitive Data, Confidential Data or Confidential Information:** All University data that is required to be maintained as private or confidential by applicable law. This includes but not limited to:

  The Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA/GLB), Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Social Security Numbers (SSN) ,University Student ID numbers, credit card numbers, health and employment records, human subject data, user IDs, passwords, financial information, bank routing numbers, ethnicity, religious affiliation, sexual orientation, political party affiliation, and all FERPA non-directory information about students and former students.

- **FTE:** Full-Time Employee
- **SAUITR:** Saint Augustine's University Information Technology Resources
- **SID:** Student Identification
- **System:** Saint Augustine's University System(s)
- **University**: Saint Augustine's University

- **University Data:** All data or information held on behalf of Saint Augustine's University, created as result and/or in support of University business, or residing on University Information Technology Resources, including paper records.
- **University Information Technology Resources:** All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf.
- **User:** Any individual granted access to University Center for Information Technology Resources.

4. Introduction

The purpose of this Policy is to ensure sound governance and adherence to accepted standards toward securing the information assets held and exchanged within the Saint Augustine's University computer network. Information is a vital university asset and requires protection from unauthorized access, modification, disclosure or destruction. This policy sets forth requirements for incorporation of information security practices into the design and management of the Saint Augustine's University network, applications, systems and procedures.

This Policy covers information security as it relates to network management and transfer of data and/or information inside and outside of Saint Augustine's University and applies to all employees, faculty, staff, vendors, and agents (collectively "Individuals") operating on behalf of Saint Augustine's University. Specifically, the Policy includes, but is not limited to the following:

- File servers, database servers, mail servers, collaboration servers or services, and other devices or systems that provide centralized computing or storage capabilities.
- Workstations, which includes desktops and laptops, tablets, smart phones, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

The Policy was created to provide guidance toward the management of Saint Augustine's University network resources and to establish guidelines regarding the handling of Saint Augustine's University information residing within the network environment. Unapproved use of or access to network resources

or information may expose Saint Augustine's University to unnecessary risks including but not limited to breaches of confidentiality, legal liability, loss of productivity, and damages to Saint Augustine's University reputation and brand.

4.1 Applicable Laws and Regulations

While every effort has been made to comply with all legal and regulatory requirements, should any part of this Policy conflict with applicable local, state, or federal law or regulation, the latter shall take precedence.

4.2 Policy Governance

Saint Augustine's University IT department is responsible for the development and ongoing maintenance of this Policy.

4.3 General

University Information Technology Resources are provided for conducting the business of University and/or System. However, Users are permitted to use University Information Technology Resources for use that is incidental to the User's official duties to University or System (Incidental Use) as permitted by this policy. See Exceptions. Anyone using any University Information Technology Resource or system expressly consents to monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to campus officials or law enforcement agencies. By continuing to use any University Information Technology Resource or system you indicate your awareness of and consent to these terms and conditions of use.

4.4 Changes in Policy

Saint Augustine's University policy directives are subject to change over time. As the user of SAUITR, you will be notified via email, SAU website, CAMS Student Portal or other broadcast communication options of any change in the policy that directly relate to you.

5. Exceptions

Special exception may be made to this policy by the CIT for specific employees. Any exceptions will be dependent on job function and employee expertise and skill level. Some reasons for exception may include, but not limited to:

1) Executing test cases developed by the CIT. The employee is the person who will be required to test new applications on a test network, then on the main network.

2) The employee will be testing their own work. The testing will be on an application or software the employee has developed.

3) User testing. Prior to deployment of an application or software, an employee may be part of the user test group.

6. Applications and Software

All employees may operate programs on the CIT Approved Application Listing or CIT Software List. If an employee desires to use an application or software not on the respective list, they must submit the application program or software to the CIT department for approval. The application or software **must** be approved by the CIT prior to its use on a system connected to the university network.
If the employee causes a security problem on the network by installing and running an unapproved application or unapproved software, they risk disciplinary action up to and including dismissal.

6.1 Approved CIT Applications and Software List

- Microsoft Office Suite 2007, 2010, 2013, 2016
- Internet Explorer 9, 10, 11
- Adobe Acrobat
- Microsoft Visio
- MS Endpoint Antivirus
- Office 365
- AutoCAD
- SPSS
- Matlab
- Smartboard

6.2 New Applications and Software

Network administrators and other CIT personnel (only) can operate and test *new* software unless "Exceptions" criteria applies. See 5.0 Exceptions.

6.3 Request to add a New Application or Software

If an employee has a request to utilize a new application or new software, the employee must submit a Support Request. The Support request should include:

- Name of application or software
- Business case for platform and circumstances where the application or software will be used (includes rationale, who will be affected, timeline for intended use, etc.)
- How to access the application or software *(link preferred)*

7. Change Management

Information Resources infrastructure at University is expanding and therefore becoming more complex. As a result, there will be more individuals that depend upon the network, administrative systems and web applications. From time to time, University Information Resources require an outage for planned upgrades and maintenance. In addition, unplanned outages may occur because of necessary upgrades and maintenance activities. This university policy applies to all individuals that install, operate, administer or maintain Information Resources.

Every change to a University Information Resource such as, but not limited to: operating systems, computer hardware, networks and applications is subject to the Change Management Policy and must follow the Change Management Procedures.

- All changes affecting computing environmental facilities (such as water, HVAC, plumbing, electricity or alarms) need to be reported to or coordinated with the leader of the change management process.
- A formal written change request must be submitted for any scheduled or unscheduled changes.
- Any change request must be submitted in accordance with the change management procedures so that the Change Management Committee has ample time to review the request and determine potential impacts to any Information Resources that may affect the decision to delay the request.
- The Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to inadequate planning, inadequate backup plans, where the change will

negatively impact key business process or University events. A Change Management Log must be maintained for all changes. The log must contain as a minimum:

- Date of submission and date of change
- Change owner and contact information
- System administrator or contact information
- Nature of the change
- Indication of success or failure of the change

All University information systems must comply with the Information Resource Change Management Process that meets the standards outlined above.

8. Computing Requirements

All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Technology Resources, including email, must be password protected in accordance with university requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.

- Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted.
- University Data created and/or stored on personal computers, other devices and/or non-University databases should be transferred to University Intranet (SharePoint) as soon as feasible.
- All remote access to networks owned or managed by University or System must be accomplished using a remote access method approved by the University or System, as applicable.

9. Personnel Security

Saint Augustine's University will protect its assets from insider threat by implementing the personnel security policy.

- The IT department will ensure the information security education is up to date and completed annually by all staff and faculty.
- The IT department will regularly perform audits on privileged accounts.
- The IT department will configure firewalls to detect unusual traffic patterns.

- The IT department ensure user accounts are assigned the correct access based on the Access Control Policy.

In addition, the IT department will

- Terminate access to all applications within twenty-four (24) hours of separation.
- Lock the device from connecting to the network within twenty-four (24) hours of separation.
- Retrieve all assigned Saint Augustine's University equipment.

10. Network and System Security Management

To the extent practical, Saint Augustine's University will adhere to the following guidelines in designing and implementing network security:

- Network segregation will be utilized to segregate high-risk systems or resources, services and individuals from those with lower risk that require less restrictive controls.
- Network ports, protocols, and services will be limited to only what is necessary.
- Controls will be implemented to protect systems and information from unauthorized access. A non-exhaustive list of examples of such controls are as follows:
    - Responsibility for securing information and equipment will be established.
    - Where appropriate, special controls will be established to safeguard the confidentiality and integrity of sensitive, protected or confidential information.
    - Logging and monitoring will record system events and access to support the detection of actions relevant to information security.

All employees of Saint Augustine's University are responsible for protecting resources and the information processed, stored or transmitted as set forth in this policy and all other Saint Augustine's University policies.

Saint Augustine's University IT department will ensure internal and external vulnerability assessments of information systems, virtualized environments, and networked environments, including both network- and application-layer test are performed. The assessments will be performed by a qualified individual on an annual basis or after significant changes.

11. Data and/or Information Transfer

- All parties external to Saint Augustine's University, including contractors and vendors, must agree to the secure transfer of business data and/or information with Saint Augustine's University.
- Any and all data and/or information transferred in electronic messaging formats must be properly protected, and encrypted.
- The soundness and completeness of information on Saint Augustine's University systems must be maintained during its transmission, storage, generation, and/or handling. Information that is corrupted or modified may be impossible to use or lead to errors in decision-making. To maximize the integrity of data, IT resource users must adhere to the following:
    - Ensure that all files downloaded from the Internet are scanned with anti-virus software prior to usage to minimize the risk of corruption, modification or loss of data. If there is a question about a file please contact IT Support.
    - Notify the Director of IT immediately if a password or other system access is lost, stolen or disclosed, or is suspected of the same.
    - Forward suspicious email messages to IT Support immediately. Do not further distribute the information.
    - Use information obtained from the Internet with caution. Before using free Internet-supplied information for business decision-making purposes corroborate and confirm the information by consulting other reliable sources.

All employees are obligated to protect sensitive personal, financial or health-related data belonging to employees or students as well as Saint Augustine's University confidential information. Saint Augustine's University expressly prohibits storage of any confidential or sensitive data on any computer or device that has not been explicitly approved by the IT Department. Employees using Saint Augustine's University network resources must adhere to the following:

- Employ adequate encryption technology as directed by the IT department.
- Notify the Information Technology department immediately if sensitive information is lost or disclosed to unauthorized parties or if any unauthorized use of Saint Augustine's University systems has taken place, or if there is suspicion of such loss, disclosure or unauthorized use.
- Do not post any Saint Augustine's University material such as software, internal memos, or other non-public information on any publicly-accessible computer or website, unless first approved by an authorized Saint Augustine's University manager.

- Do not store company confidential information in any personal computer.
- Do not connect personal computers to the Saint Augustine's University network. Personal computers are allowed on the SAU network. Vendors are required to connect to the SAU vendor network.
- Do not save passwords in Web browsers or e-mail systems used to access or transmit Saint Augustine's University information.
- Do not establish or use an unapproved Internet connections into the Saint Augustine's University environment that could allow external individuals to gain access to company systems and information. All connections into and from Saint Augustine's University must be through the VPN.
- Do not discuss or communicate information security-related incidents or information with individuals outside of Saint Augustine's University or with those inside the company who do not have a need-to-know.
- Do not share unencrypted sensitive information via email.

12. Data Security and Confidentiality

Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with University's Records Retention Policy and Records Management Guidelines.

Users must not use or disclose Confidential University Data, or data that is otherwise confidential or restricted, without appropriate authorization. Examples of groups that can provide appropriate authorization include, but are not limited to Office of Admissions, Registrar, Human Resources, Financial Aid, Business and Finance, the Center for Information Technology, Gordon Health Center, Marketing and Communications, Athletics, Financial Aid, Academic Affairs, Academic Leadership, Division of Military Science and The Prezell R. Robinson Library.

- Users must ensure any individual with whom Confidential University Data is shared is authorized to receive the information.
- Users may not share University Confidential Data with friends or family members.

- Users may not share university business data that may be classified as Confidential Data, such as the status of negotiations, terms of contracts, and new research or products or relationships under development.
- Users will comply with the university's agreements to protect vendor information such as software code, proprietary methodologies, and contract pricing.
- If User's office routinely receives requests for University Confidential Data, work with an appropriate group within the university to develop formal processes for documenting, reviewing, and responding to these requests.
- If Users receive a non-routine request for University Confidential Data from a third party outside of the university, check with an appropriate group within the university to make sure the release of the data is permitted.
- Users must report violations of university policies regarding use and/or disclosure of confidential or restricted information to the Center for Information Technology (919-516-4000).
- Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on centrally managed services (i.e. SharePoint), rather than local hard drives or portable devices.
- Confidential or essential University Data and information stored on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, must be encrypted in accordance with University, System's, and any other applicable requirements.
- Access to confidential information on University computers, servers and databases must require a combination of a unique login ID and a secret password that is known only to the user.
- All Confidential University Data must be encrypted during transmission over a network.
- Users who store University Data using commercial cloud services must use services provided or sanctioned by the University, rather than personally obtained cloud services.
- Users must not try to circumvent login procedures on any University Information Resource or otherwise attempt to gain access where they are not allowed. Users may not deliberately scan or probe any University Information Resources without prior authorization. Such activities are not acceptable under any circumstances and can result in serious consequences up to and including dismissal from the university.
- All computers connecting to a University's network must run security software prescribed by the director of IT as necessary to properly secure University Information Technology

Resources. Computers left on while unattended shall have a screen saver enabled that is password-protected.

- Devices determined by University to lack required security software or to otherwise pose a threat to University Information Technology Resources may be immediately disconnected by the University from a University network without notice.

13. Security Training

Saint Augustine's University employees and contractors will receive documented initial (as part of their onboarding within sixty (60) days of hire), annual and ongoing training on their roles related to security and privacy.

Saint Augustine's University employees and contractors will be informed in writing, that violations of the security policies will result in sanctions or disciplinary action.

Personnel using mobile computing devices will be trained on the risks, the controls implemented, and their responsibilities, e.g., shoulder surfing, physical protections.

Personnel who telework will be trained on the risks, the controls implemented, and their responsibilities.

Saint Augustine's University will provide training on Bring-Your-Own-Device (BYOD) usage, which includes providing an approved list of applications, application stores, and application extensions and plugins

14. Access Control

Saint Augustine's University policies are designed to provide only authorized access to Saint Augustine's University information in order to maintain confidentiality, integrity and availability. All access and permissions are reviewed on a regular basis and unauthorized attempts at accessing systems or files is logged.

The IT department is responsible for performing periodic audits of active user accounts, physical access rights and allocated assets.

- User Accounts: Human Resources will provide IT with a list of user accounts that are to be disabled monthly. IT will work with HR to ensure these accounts have been disabled and submit this list confirming disablement back to HR. Human Resources will alert the IT department within 24 hours of an employee's last day of employment.

- User Access Rights: On a quarterly basis, the IT will work in tandem with Human Resources to verify the access rights of user accounts is accurate. Human Resources will sign off and report to the IT department that access rights of user accounts are accurate.
- Physical Access Rights: On a quarterly basis, the IT department will work in tandem with HR and the Registrar to review the physical access rights of students, faculty and staff. HR and the Registrar will sign off and report to the IT department that the physical access rights of students, faculty and staff is accurate.
- Allocated Assets: On a quarterly basis, the IT department will work in tandem with Human Resources to review the allocated asset list. Human Resources will sign off and report to the IT department that the allocated asset list is accurate.

Audit logs of all systems are sent to a central collection server to minimize the effects of tampering.

Segregation of duties is maintained as request, approval and implementation of access is done by separate individuals within the organization, with IT responsible for executing the approved requests. Access will be granted on a need-to-know and need-to-do basis.

A closed circuit digital video system monitors all areas of the facility. Server room access is limited to IT personnel only and all access is logged and monitored by security cameras.

The Saint Augustine's University Password Policy requires complex passwords and unique accounts for all systems. Passwords are changed every 90 days and cannot be one of the last 10 passwords used.

14.1 Identification and Authentication

Saint Augustine's University IT department requires proper identification for requests to establish information system accounts and approval of all such requests. User identities will be verified prior to establishing accounts.

Saint Augustine's University IT department will provision unique IDs that can be used to trace activities to the associated individual.

Any individual accessing Saint Augustine's University information system will use their own account to login

Shared/group and generic user IDs shall only used in exceptional circumstances where there is a clear business benefit, when user functions do not need to be traced, additional accountability controls are implemented, and after approval by IT management.

Actions to be performed without identification and authentication are permitted only to the extent necessary to accomplish mission objectives and require prior approval by IT management.

15. Antivirus

Saint Augustine's University utilizes antivirus on all computers and servers within the environment. Saint Augustine's University policy requires that a computer must have an up to date functioning antivirus before it can be connected to the network, physically or through a VPN tunnel. Antivirus software is configured with real-time protections in addition to scheduled weekly scans of all systems. Any systems found to be infected with any type of malware/virus are immediately quarantined from the network. Only after the computer has been cleaned and reviewed by IT Support is it allowed to connect to the network, either physically or through VPN.

16. Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for Full-Time Employees (FTE) and temporary employees. In the case of contractors or consultants, violations may result in termination of employment relationship and dismissal for interns or volunteers. In the case of students, violations may result in suspension or expulsion depending on the severity of the violation. In addition, all individuals are subject to loss of University resources access, privileges, civil and criminal prosecution.

17. Email

Emails sent or received by users while conducting University business are University Data that are subject to state records retention and security requirements.

Users are to use University provided email accounts, rather than personal email accounts, for conducting all course and University business.

The following email activities are prohibited when using a University provided email account:

- Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.
- Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of the University.
- Sending or forwarding any email that is suspected by the User to contain computer viruses.
- Any Incidental Use prohibited by this policy.
- Any use prohibited by applicable university or System policy.

The University President, Vice Presidents, Provost, Deans, Directors, or Chairs may sponsor an email account for non-University personnel who are affiliated with the University and are assisting the university in meeting its mission. However, all email requests must be submitted from Human Resources to the Center for Information Technology. The requestor must provide the person's name, date of birth, estimated period the account will be needed, and phone number. Upon approval, an ID and password will be provided. The name of the sponsor will be recorded along with the owner of the account for possible renewal. Sponsored accounts will expire in December of every year. The sponsor will be notified of an upcoming expiration date or in November asking if they wish to renew the sponsorship. If no response is received, the account will be deactivated as specified above.

18. Food, Drinks and Cell/Mobile Phones in Labs

Food and drinks are prohibited in the computer labs with no exceptions. This policy protects the equipment from spills and debris that could disable the computer systems. Use of cell or mobile phones needs to be at a level that does not disturb or interfere with any other end-user and conversations should be kept at a minimum using the headset or an earpiece. Use of the speaker on the phone is strictly prohibited unless it is for the use of a class or presentation where the entire lab environment is being used for that purpose.

19. Acceptable Use

19.1 Individuals Responsibilities

All Saint Augustine's University staff, contractors, third parties and faculty shall:

a) Not use Saint Augustine's University Data for any illegal purpose, violation of university policy or in a manner contrary to Saint Augustine's University's best interests.
b) Avoid unnecessarily disclosing Saint Augustine's University data to unauthorized third parties.
c) Ensure that they understand that Saint Augustine's University accounts and access to Saint Augustine's University network devices are subject to monitoring and enforcement for unauthorized activities or unsanctioned university activities.
d) Report any loss of data, policy violation or system malfunction that may present a risk for Saint Augustine's University.
e) Authenticate with their own accounts prior to accessing Saint Augustine's University data.
f) Not to share their account credentials with other users.
g) Protect Saint Augustine's University data, including any sensitive information stored or processed on Saint Augustine's University information systems, from unauthorized access. Saint Augustine's University employees, faculty and students shall ensure that no unauthorized persons can access sensitive information unless explicitly approved by Saint Augustine's University management.

19.2 Intellectual Property Rights and Copyright Material and Information

The following are prohibited at Saint Augustine's University with no exceptions:

a) Improper and/or unauthorized use of material that infringes on intellectual property rights, including copyright, trademark, patent, design, and moral rights.
b) Unauthorized copying and/or use 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 Saint Augustine's University or the individual does not have an active license.
c) The use (includes: copying, assigning, selling, or passing on or sharing activation keys) of proprietary software or products covered by copyrights without either a valid license or the explicit consent of the owner and approval from Saint Augustine's University's IT department.

19.3 Systems and Resource Ownership

Systems and/or resources shall remain in Saint Augustine's University's ownership, regardless of who is using and/or operating them and for whatever period of time or purpose, unless or until Saint Augustine's University has agreed in writing to waive or transfer ownership to another party.

Upon termination of employment or contract completion, individuals shall return all equipment, information, digital assets and resources back to Saint Augustine's University. Additionally, Saint Augustine's University reserves the right to request the return of any university-owned property at any time prior to termination.

Staff, contractors, third parties, faculty and students shall store all university records on designated storage locations within the Saint Augustine's University network or with approved online services at all times.

19.4 IT Account Ownership

Saint Augustine's University provides each staff, faculty and student with at least one IT account. IT accounts shall remain the property of Saint Augustine's University. They can be suspended, modified, withdrawn, or cancelled at any time. Staff and faculty are prohibited from using their IT account credentials to register with non-business-related Web sites or unauthorized social media services.

19.5 Lost or Stolen IT Resources

As soon as an individual becomes aware of a loss or theft of an Saint Augustine's University computer, mobile device or information, whether paper or electronic, IT should be notified. If a mobile device is lost or stolen, service will be terminated immediately, the device will be wiped, and then locked to prevent further access to the device.

19.6 Business Use of IT Systems or Resources

Saint Augustine's University IT systems shall be used solely for the purpose of conducting university business. Incidental Use of University Information Technology Resources must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or System policy.

- User's action on Saint Augustine's University computer systems is monitored. Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including University email accounts.
- Users may not be paid, or otherwise profit, from the use of any university-provided information resource or from any output produced using it. Users may not promote any commercial activity using university Information Technology Resources. Examples include, attempting to sell football

tickets or advertising a "Make Money Fast" scheme via a newsgroup. Such promotions are considered unsolicited commercial spam and may be illegal as well.

- Incidental Use for purposes of political lobbying or campaigning is prohibited.

19.7 Non-Permitted Use of IT Systems or Resources

The use of Saint Augustine's University IT systems or resources in an unlawful, unethical, or unauthorized manner is strictly forbidden and may result in disciplinary action. Unlawful, unethical, or unauthorized manner may mean, but is not limited to, accessing, viewing, installing, downloading, processing, or creating any materials in any form or format that:

- Violates laws, regulations or agreements.
- Displays, creates or transmits harassing, embarrassing, defamatory, derogatory, indecent, obscene, profane, intimidating, racist, sexually-oriented, illegal drug-related, or sexist content using Saint Augustine's University IT resources.
- Impersonates other users
- Is copyrighted and explicitly or implicitly states that use is prohibited.
- Breaches another university policy.
- Is disclosed, destroyed or altered without proper authorization.
- Introduces harmful or malicious programs (e.g., viruses, Malware) into the Saint Augustine's University IT environment.
- Is not explicitly approved by Saint Augustine's University management.

Saint Augustine's University users that have been issued privileged accounts have an even greater responsibility to adhere to this policy. Compromised privileged accounts could pose a great risk to Saint Augustine's University since attackers could potentially have the ability to install malicious software and bypass information security safeguards. Thus, Saint Augustine's University management will be strict in its dealing with the abuse of privileged account usage.

19.8 Use of Private Devices

Individuals are allowed to use personal devices while on Saint Augustine's University premises; however, personal devices shall not connect to the Saint Augustine's University network. Individuals may only connect personal devices to the Saint Augustine's University guest "SAU" wireless network

19.9 Internet

Saint Augustine's University acknowledges the value and potential of information published via the internet. This acknowledgement encourages all faculty, staff, and students to develop innovative uses of web technologies to pursue the university's mission. To achieve this purpose, the university owns and operates web servers to facilitate the educational process and enhance research and publication by university employees and students. Because the university recognizes the value of the internet as a resource for information and communication, students and employees may make incidental use of university resources to access the web for co-curricular or personal purposes provided they abide by the general policies and procedures governing use of Information Resources and there is no direct cost to the university related to this incidental use.

- Official Web Pages
    - Official web pages and sites are provided exclusively for:
        - The dissemination of official policies and procedures.
        - The description of university offices and departments, their services, programs and activities, including identification of associated faculty or staff members.
        - Operational instructions or information necessary to assist students, employees, and entities with which the university conducts business.
        - Administrative divisions and offices.
        - Academic departments.
        - Other activity or informational centers authorized by the University.
- Individual Web Pages
    - All faculty, staff and students are provided space for personal information on the server via SharePoint OneDrive. Individual web pages are the responsibility of the page creator and do not reflect the opinions, positions, policies or procedures of the university. Anonymous web pages are prohibited and all individual web pages must prominently display the name(s) of the creators who assume full legal and ethical responsibility for the content thereof. (See Acceptable Use)

- Acceptable Use
    - To facilitate communication and dissemination of information to University faculty, staff, and students regarding services, programs and events.

- To facilitate communication with current and prospective business partners for the daily operation of university business or academics.
- To promote university programs and services to prospective students, professional colleagues, and the general population.
- To announce or advertise products or services for use within the scope of university business.
- For communications or activities in direct support of university-related research, instruction, learning, dissemination of scholarly information, and administrative activities.
- For personal sites, internal collaboration any other communications or activities that are not in violation of this or any other university policy, or applicable federal, state or local law.

- Unacceptable Use
  - Publishing or linking to any material prohibited by law or university regulations, material that violates the terms of any university license or contract or uses copyrighted material without required permission (also known as plagiarism).
  - Publishing or linking to legally restricted or confidential material.
  - Publishing or linking to material that is obscene, libelous, physically threatening or otherwise in violation of standards for university publications.
  - Publishing or linking to material that intentionally or negligently may lead to damage to a university or other computer system;
  - Using the University seal, logos or other registered university marks without the review and approval of the university Communication Office. Such approval will not be granted for individual web pages.
  - Use of loud or obscene audio or video images (i.e., photographs, paintings, or derivatives thereof), videos, or movies of individuals
  - Use of any personal information that is not public record pertaining to other individuals without their express written consent.
  - Use of any images, data, vulgar websites, that is or could be interpreted as abusive, obscene, harassing, threatening, or discriminatory in in any context.

- Use of any images or data that violate Saint Augustine's University policies (e.g., Sexual Harassment Policy) or local, state, or Federal laws.
- Creation of direct hypertext links to abusive, obscene, harassing, threatening, or discriminatory material.
- Use of materials whose nature or volume compromises the ability of the system to serve other users' documents and individual home pages.
- Any use which constitutes academic dishonesty.

19.10 Use of Email and Collaboration Services

Saint Augustine's University's email and collaboration services are for university business use only. Email messages shall be regarded as, and considered no different than, a signed hard copy correspondence. Email communications are not considered private. Saint Augustine's University staff, contractors, third parties, faculty and students shall not use Saint Augustine's University's email systems for non-university business related purposes (e.g. Forwarding non-business-related emails or chain emails).

Individuals who are granted Saint Augustine's University email accounts are not allowed to forward, either manually or automatically, any business-related emails to personal accounts.

From time to time it may be necessary to grant others permission to access individual email accounts or collaboration accounts. The methods by which you can accomplish this include: (1) setting up delegation rights in the email services; or, (2) editing the sharing rights in the collaboration services. It is not permitted, however, to provide another individual with your IT account credentials.

From time to time, Saint Augustine's University may need to access individual emails (e.g., to retrieve business-critical information, implement improvements, migrate data, investigate a complaint or comply with a legal or regulatory demand).

Saint Augustine's University employees are not allowed to store sensitive Saint Augustine's University data on:

- Personal cloud-based services (DropBox, OneDrive, etc.)
- Local hard drives

Removable media usage is only allowed for business purposes with manager approval.
Saint Augustine's University users should not send unencrypted sensitive information using email.

19.11 Social Media

Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether associated or affiliated with Saint Augustine's University, as well as any other form of electronic communication.

The same principles and guidelines found in Saint Augustine's University's policies regarding workplace conduct apply to online activities.

Saint Augustine's University staff, contractors, third parties, faculty and students shall:

- Not post content that includes discriminatory or harassing messages, threats of violence or similar inappropriate or unlawful conduct.
- Maintain the confidentiality of Saint Augustine's University trade secrets and private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology.
- Not post internal reports, policies, procedures or other internal business-related confidential communications.
- Not include any personally identifiable information or other information that could otherwise identify students in any social media communications or on employees' personal social networking sites.
- Intellectual property and copyright laws apply to the Internet and what is posted. Never use the Saint Augustine's University logo or reproduce Saint Augustine's University's written material without first obtaining written permission.
- Refrain from using social media while on work time or on Saint Augustine's University equipment and refrain from discussion of Saint Augustine's University, unless it is work-related as authorized by your supervisor or manager.

20. Notices

At various intervals, updates and instructions impacting lab computing systems may be posted outside of labs, communicated through email on "Good Day SAU" and placed in the information section within the

CAMS Student Portal. Additional notifications impacting labs may be posted at the lab entrances of scheduled opening and closings.

21. Password Management

University issued or required passwords, including digital certificate passwords, Student Identification (SID), Digital Certificates or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.

- Users must not give others access to University Information Technology Resources unless they are authorized and authenticated for such access. Users may not extend access to University Information Technology Resources to others without permission (e.g., proxy services, accounts for non-university personnel, etc.).
- Each User will be held responsible for all activities conducted using the User's password or other credentials.
- Student, faculty and staff ID cards must be returned on demand upon termination of the relationship with University.
- If the security of a password is in question, the password much be changed immediately.
- Computing devices must not be left unattended without enabling a password-protected screensaver or logging off the device.
- Do not use "Remember Password" feature of applications (i.e. Outlook).
- Do not write passwords down and store them in your office.
- Do not store unencrypted passwords in a file on ANY computer system.
- If an account or password is suspected of have been compromised, report the incident immediately to the Center of Information Technology and change all passwords immediately.
    - In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery immediately to the Center for Information Technology
    - Transfer the passwords to an authorized person as directed by the Center of Information Technology to the Chief Technology Officer.

21.1 <u>Password Security</u>

All passwords, including initial passwords, must be constructed and implemented according to the following rules:

- Passwords must be between 8 and 20 characters in length
- Your password must contain letters, numbers and special characters. Special characters permitted are:
  ! @ # $ % & * ( ) - + =, < > : ; " ' ..

- Passwords cannot contain letter transpositions (for example @ for a, ! for I or zero for 0).
- Your password cannot contain your first or last name
- Your password cannot contain your birthday in any form
- Your password cannot contain your Social Security Number

Passwords will be changed at least every ninety (90) days and passwords are prohibited from being reused for at least six (6) generations.

22. Physical Access

Technical support staff, security administrators, system administrators and others may have Information Resource physical facility access requirements as part of their function. The granting, controlling and monitoring of the physical access to Information Resources facilities is vital to an overall security program. The University Physical Access Policy applies to all individuals within University that are responsible for installation and support of Information Resources, individuals charged with Information Security and data owners.

- All physical security systems must comply with all applicable regulations such as, but not limited to build codes and fire prevention codes.
- Physical access to all Information Resources restricted facilities must be documented and managed.
- All Information Resources facilities must be physically protected in proportion to the criticality or importance of their function at University.
- Access to Information Resources facilities must be granted only to University support personnel and contractors, whose job responsibilities require access to that facility.

- The process for granting card/key access to Information Resources facilities must include the approval of the person responsible for the facility.
- Everyone that is granted access right to an Information Resources facility must sign the appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared of loaned to others.

23. Policy Violations

Saint Augustine's University Information Technology Resources (SAUITR) are provided for conducting the business of University and/or System. However, users are permitted to use SAUITR for use that is incidental to the user's official duties to University or System (incidental use) as permitted by this policy. Anyone using any SAUITR or System expressly consents to monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to campus officials or law enforcement agencies. By continuing to use any SAUITR or system you indicate your awareness of and consent to these terms and conditions of use.

Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University have no expectation of privacy regarding any University Data they create, send, receive, or store on University owned computers, servers, or other SAUITR owned by, or held on behalf, of University. University may access and monitor its SAUITR for any purpose consistent with University's duties and/or mission without notice.

Users have no expectation of privacy regarding any university data residing on personally owned devices, regardless of why the data was placed on the personal device.

All Users must comply with applicable SAUITR Use and Security policies at all times.

Users are prohibited from sharing password, login or any information that allows access to University information or resources.

Users shall never use SAUITR to deprive access to individuals otherwise entitled to access University information; to circumvent University computer security measures; or, in any way that is contrary to the University's mission(s) or applicable law.

Users must not interfere with the activities of others. Examples of inappropriate use of resources are shown below. These actions frequently result in complaints and subsequent disciplinary action.

- Sending an unsolicited message(s) to a large number of recipients (known as "spamming the network").
- Consuming an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer applications).
- Deliberately causing any denial of service, including flooding, ICMP attacks, or the unauthorized automated use of a service intended solely for human interaction.
- The act of piracy is strictly prohibited.

Use of SAUITR to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the user's official duties as an employee of the University and is approved in writing by the President or a specific designee. Viewing, accessing, storage, and/or transmission of sexually explicit materials as Incidental Use is strictly prohibited.

Users should report misuse of SAUITR or violations of this policy. How an incident is reported depends upon the nature of the incident:

- If Users believe that their personal safety is threatened, they should call SAU Security, 919-516-4911.
- For other incidents, including "spam" or unsolicited mail, users should submit a support request to: support@st-aug.edu or contact the Center for Information Technology at 919-516-4009.

Violation of this policy may result in disciplinary action which may include termination for Full Time-Employees (FTE), Part-Time Employees (PTE) and temporary employees. In the case of contractors or consultants, violations may result in termination of employment relationships and dismissal for interns or volunteers. In the case of students, violations may result in suspension or expulsion depending on the

severity of the violation. In addition, all individuals (including visitors) are subject to loss of University resources access, privileges, civil and criminal prosecution.

23.1 Enforcement

Running safe software and applications is critical to the security of the university. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

24. Problems and Help

The Center for Information Technology (CIT) is responsible for ensuring access to the campus's computing and telecommunication resources. Information regarding technology applications can be found on the University website and department SharePoint sites. Support tickets request should be submitted via email to: support@st-aug.edu or by clicking the "Submit Support Ticket" button found on the Technology Support link (Quick Links) on the Saint Augustine's University homepage.

All students must have a valid User ID and password to access the Saint Augustine's University network, CAMS Student Portal, Wireless Access Areas, RAVE Emergency Alert System and SAUITR. For User ID requests, password resets, students with ID can solicit support from the CIT team located in the Benson building. All other requests should be submitted via the "Submit Support Request" located on the University homepage. It should be noted that sharing login information in any capacity with other students or non-students is strictly prohibited. Any violation is subject to disciplinary action outlined per the University policy. (See Policy Violations)