FACILITIES, OPERATIONS, AND INFORMATION TECHNOLOGY
SECTION 300

Section 300/2.1 Information Technology
Subject: Overview

Policy
The following policies and procedures govern the Office of Information Technology (OIT) Department and the use of information technology at Jacksonville University. In addition to general policies that govern all IT users at Jacksonville University, there are also policies that apply specifically to students and specifically to faculty and employees. Questions about any individual policy may be sent via email to dveneto@ju.edu.

Section 300/2.2 Information Technology
Subject: Privacy

Policy
All data, email, files, documents contained on University assets are considered to be under University care and are treated as University property unless there is an explicit, written

policy or agreement stating otherwise. As a result, users should not expect any personal privacy for any email or other data contained on University assets. IT personnel are bound by JU's IT Professional Code of Ethics which limits their use of special permissions for maintenance purposes only.

Section 300/2.3 Information Technology
Subject: Prohibited/Illegal Activities

Policy
Usage of the JU network is also governed by local, state, federal and international laws. The paragraphs below touch on some specific items but **should not be considered all inclusive**. Some links worth exploring are The Florida Computer Crimes Act, U.S. Copyright Law, and the Digital Millennium Copyright Act. JU will provide all possible assistance to law enforcement agencies in the location and identification of individuals suspected of committing a crime via the university network.

1. Computer Attacks: Users found to be attacking other computer systems on or off campus will have their network connection disabled without notice. Attacks include attempts to break into a system, probing systems to detect vulnerabilities, traffic "sniffing", Denial of Service attacks, phishing and spamming. Unintentional attacks caused by viruses/trojans/worms will be passed on to the IT Helpdesk for correction. Intentional attacks will result in termination and possible criminal prosecution.

2. *Copyrighted Material*: It is prohibited to distribute over the network or store on University owned computers any copyrighted material not created by you or without express permission, typically in writing, of the author of the copyrighted material. Examples are music files (MP3's), movies and e-books. A common method of unlawfully distributing these materials is with Peer-to-Peer software. The University may assist organizations (RIAA, MPAA, etc.) who are involved with protecting the rights of copyright owners with the location and identification of individuals suspected of distributing it. Any copyrighted material found on University owned computers will be deleted without notice to the user. If a user requires this material for class use and are covered by the laws governing Fair Use or has permission from the copyright holder, the user must notify the Network Administrator prior to storing the files on a network server. Users will be responsible for immediately removing these files once they are no longer needed. Illegal distribution of copyrighted material will result in the loss of your network privileges.

3. *Pornography*: It is forbidden to view or store pornographic material on University owned computers. JU runs programs for minors and the exposure to them of these materials, inadvertent or not, may make the student or University subject to criminal prosecution. Any pornography found on University owned computers will be deleted without notice to the user. Repeat offenders may be referred for disciplinary action. If this material is required for a class project, the System Administrators must be notified prior to storing the files on a network server. The student will be responsible for immediately removing these files once they are no longer needed. Child pornography is absolutely forbidden on any computer on campus. If child pornography is found on any computer, the CIO will immediately notify local law enforcement authorities.

Section 300/2.4 Information Technology
Subject: Network Services

Policy
JU makes a wide variety of network services available from email to online network storage. Users should consult the list of network services by visiting the IT website; http://it.ju.edu.

1. Internet Gateway: JU's network includes a connection to the Internet. This very popular resource is limited in its ability to handle traffic. To ensure equal access for all, certain types of traffic may be rate limited or even blocked periodically. Peer-to Peer traffic is always blocked.

2. *Network Maintenance*: JU reserves the right to take down network services for maintenance without notice. Planned maintenance that will impact services over a long period of time will be announced prior to the event via JU email. Planned maintenance that will impact services for less than 15 minutes will not be announced, however, all efforts will be made to accomplish the maintenance after classes complete for the day. IT constantly monitors the network for performance and security reasons. Automated devices are used as well as manual means. Selected individuals in the IT Department have full access to University owned systems in order to fulfill the requirements of their job. Information transmitted over the network or stored on university owned computers may be viewed by those individuals during the performance of their duties.

Section 300/2.5 Information Technology
Subject: Policy Review

Policy
These policies will be reviewed and revised annually reflect changes to technology. Suggestions and proposed changes to the policies should be submitted to the Chief Information Officer. Changes to the policy shall be approved by the Chief Information Officer.

Section 300/2.6 Information Technology
Subject: Students; Overview

Policy
Jacksonville University provides and supports technology across campus and across the Internet to support students in their pursuit of a college degree. These policies apply to all current, former, and prospective students. JU provides computers throughout campus for use by the students in open labs and classrooms. These computers are configured to provide students with services tailored to the tasks needed to assist them with their studies. Additionally, students living on campus are provided access to the campus Internet gateway from their residence.

The network at Jacksonville University consists of computers, networking devices, telecommunications systems, and the Internet gateway. The primary purpose of the network is to support the mission and ongoing business of the University. Access to and use of the network is a privilege subject to strict compliance with these policies. Their purpose is to protect this valuable resource as well as ensure fair and equitable access for all members of the campus community.

Section 300/2.7 Information Technology
Subject: Students; Network Access

I. Policy
All students will be issued a network account that consists of a username and password. The network account is your key to a multitude of network and Internet based services. Usernames are unique to each person. A username cannot be changed as various services and data are tied to it, and these would become inaccessible. The Display Name on an account can be changed to reflect a changed name instead. All students will also receive an email account that is tied to their network account. That email account will exist as long as the network account it is associated with exists. (See the NOTE at the end of this section for important information) Your password is not to be shared with others.

II. Procedure
The username consists of the first initial of the nickname and the first six characters of the last name, or, if no nickname is supplied, the first initial of the first name and the first six characters of the last name. In cases where there are multiple users with the same username, a number will be appended. The network account will remain active the entire time students are enrolled in classes at JU. It will expire 9 months after the student leaves the university or if 9 months passes between finishing a class and registering for another. An email will be sent to the student's JU email before the account is deleted. Exceptions to this policy include On-Line Nursing students which will remain active for a year and a half, and Dual Degree Engineering students which will remain active for 2 years. Students graduating from the university will have their username transition to an Alumni account with no expiration.

Student network accounts will be created with an initial password. This password will be sent to the student by either email or a letter. The password should be changed at the earliest opportunity. Students are required to choose a password that follows the guidelines on the Password website. Passwords may be changed by going to the Password website (http://password.ju.edu) or logging on to a university computer running Microsoft Windows and pressing CTRL-ALT-DEL. Students should change their passwords often to protect their account. Passwords will automatically expire every 90 days. Passwords obtained from contacting the IT Helpdesk WILL expire in 24 hours unless changed at the Password website. Students should not share their passwords with anyone. Students are responsible for their account. Malicious activity by someone using a student's account may result in disciplinary action for the student.

NOTE: If you become employed by Jacksonville University or one of its on-campus contractors, you will lose your student/alumni @jacksonville.edu email account and will be given a @ju.edu email account. When your employment is terminated and your status returns to student or alumni, you will receive a new @jacksonville.edu email account. In either case, the emails in your old account will not be recoverable.

Section 300/2.8 Information Technology
Subject: Students; Integrity of Computer Systems

Policy
JU provides computers throughout campus for the use of our students. These computers are configured to provide students with services tailored to the area they are located in. Students shall not alter that configuration or install additional software on these computers. Doing so may result in the student losing their privileges to use University owned computers.

Section 300/2.9 Information Technology
Subject: Students; Use of Non-Institutional Hardware and Software

Policy
Students bringing computers, smartphones, tablets, and gaming devices to campus must register them and verify their security before they will be allowed to access network resources such as the Internet. Jacksonville University uses a system called SafeConnect to allow students to perform the registration and security check on their own. To pass the security check, computers must have antivirus software installed and updated, have all security patches recommended by the Operating System manufacturer installed, and have the SafeConnect agent installed.

JU will aid those students needing help with the registration process and connecting to the network. The student is responsible for any software issues or hardware repair required to ensure their computer or device is ready to connect to the JU network. Students should contact the IT Help Desk to find out when and where this assistance is available.

Computers that threaten the network because of viruses/trojans/worms, improper configurations or hardware/software problems will have their network connection terminated without notice. Network access will be restored only after the computer is certified safe by a representative of the IT Department. The user assumes all risk when connecting to the JU network. JU will not be responsible for any damage to a privately owned computer due to it being connected to the network. Students living on campus may use the network for recreational purposes and conducting personal business on a “not to interfere” basis with JU business requirements.

Students may not use the network for personal financial gain.
Switches, routers, hubs, and wireless access points are prohibited. If these devices are detected, the owner's network access will be terminated without notice. Students assigned as a single in a two-person room may use both network ports in that room.

Section 300/2.10 Information Technology
Subject: Faculty/Employees; Overview

Policy
Jacksonville University provides technology to its employees to support the University's business goals and objectives. These technologies range from desktop computers and printers to land-based telephone. This document outlines the responsibilities of both the end user and the university in support of that use. These policies apply to all employees of the University and are in accord with the various Employee Handbooks maintained by the Human Resources Department.

Section 300/2.11 Information Technology
Subject: Faculty/Employees; Integrity of Computer Systems

Policy
JU provides computers for the use of our employees. These computers are configured to provide employees with services required to perform for their job. Employees shall not alter that configuration or install additional software on these computers. If additional software is required, employees must submit a request to the IT Help Desk. All employees will allow free and unfettered access to all JU owned IT assets for maintenance, hardware/software upgrade and inventory purposes. It is prohibited to use JU network resources for personal business, personal financial gain or for recreational purposes. Doing so may result in the employee's termination.

Section 300/2.12 Information Technology
Subject: Faculty/Employees; Network Access

I. Policy
All university employees are assigned a username and password that allows them access to the various University information systems. Usernames typically consists of the employee's first initial and the first six characters of their last name. In cases where there are multiple users with the same username, a number will be appended to it. A username cannot be changed as various services and data are tied to it, and these would become inaccessible. The Display Name on an account can be changed to reflect a changed name instead. Employee network accounts will

remain active for the duration of employment at JU. It will expire at 5:00 pm on the day the employment is terminated.

Employees who retire from JU may retain certain access delineated in Network Services for Employees. Employees who remain at the university as a student will fall under the Student Network Policy.

It is prohibited to share your password with anyone. Failure to protect your password can result in the immediate termination of your network account.

II. Procedure
Employee network accounts are created with an initial password assigned during the account creation process. Call the Help Desk at 904-256-7200 to obtain this password. Employees should change initial passwords at their earliest opportunity, choosing a password that follows the suggested guidelines. Passwords can be changed by going to the website http://password.ju.edu or logging on to a University computer and pressing CTRL-ALT-DEL. Employees should change passwords often to protect their account. Passwords will automatically expire every 90 days. Employees will receive an email notification that your password is about to expire.

Section 300/2.13 Information Technology
Subject: Faculty/Employees; Institutional Data

Policy
All employees are to be aware of and abide by local, state, and federal regulations that apply to data they create, handle or access. Employees should be aware of the various privacy and confidentiality requirements for data they access through JU's systems. **It is prohibited to store any file containing FERPA, HIPAA or Privacy Act data on a personally owned computer/mobile device, a portable storage device, or on a privately held cloud storage account.** Ensuring compliance with the regulatory requirements for the security, storage and archiving of data is the responsibility of each Department's supervisory personnel.

Section 300/2.14 Information Technology
Subject: Faculty/Employees; Technology Training

Policy
The IT Department self-paced Web based training for the Microsoft Office group of applications. Limited training for Ellucian and the SharePoint Portal is also available. Due to the large number of applications in use on campus and their limited audience, employees desiring training other than the above must contract with the product vendor or an outside training facility.

Section 300/2.15 Information Technology
Subject: Faculty/Employees; Donated Items

Policy
In addition to the requirements set forth in section 700; Developmental Fundraising, accepting donations of IT related equipment such as computer systems, printers, PDAs, smart phones, etc., without approval of the Gift Acceptance Committee is prohibited.

Section 300/2.16 Information Technology
Subject: Faculty/Employees; Personally, Owned Equipment

Policy
Jacksonville University's IT Department is charged with maintaining the technology of the University. As such, it does not provide support or assistance with personally owned equipment. Employees may not bring personally owned computers on campus for business use. Employees required to work from home should have their supervisor contact IT for information on the approved methods for telecommuting. Employees desiring to use their personally owned tablet or smart phone to check their JU email and calendar may do so with the understanding that their device will require a self-assigned passcode every time they use it. IT will provide the information required to connect to these services but will not set the device up. The employee is responsible for providing his/her own support. Requests for software installation on JU computers for support of a personally owned device must come from the supervisor. All configuration, operation and support of this software are the responsibility of the employee.

Section 300/2.17 Information Technology
Subject: Faculty/Employees; Administrative Rights

Policy
This policy addresses the voluntary use of the University's electronic resources and the internet via the University's network to provide guidance to faculty and staff. Every member of the University community is covered by this policy and expected to be familiar with its provisions. We recognize the value of computer and other electronic resources to enhance the administration and operation of the University. To this end, we encourage the responsible use of computers, computer networks, including the Internet, and other electronic resources, which must be in support of educational and research objectives consistent with our mission and goals. Use of our electronic media offers a wealth of information and resources for research. ***In addition, users are expected to exercise good judgment in interpreting these guidelines and discretion in making decisions about the appropriate use of our resources. Any person with questions regarding the application or meaning of these guidelines should seek clarification from the Information Technology Department.***

Monitoring and Privacy. It is the University's policy to maintain an environment that promotes ethical and responsible conduct in all network activities, including activities on the Internet and the privacy of others. However, we need to monitor network activities to maintain network security and for other lawful reasons. The University retains the right to inspect your hard drive and the files it contains. In addition, an Internet firewall automatically checks all data moving between the local area network and the internet and logs the sending and receiving destinations.

Use of the University's technology resources constitutes consent for the information technology and other administrative staff to monitor and/or inspect any files that users create, any messages they post or receive, and any web sites they access. Please remember that you have no expectation of privacy. Among the things we may do to ensure compliance, we may log network use and to monitor fileserver space utilization by users. We assume no responsibility or liability for files deleted due to violation of fileserver space allotments. We may also monitor the use of online activities. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review. You are advised that messages in discussion forums, including deleted messages, are regularly archived, and can be retrieved. It is a violation of this policy to engage in any activity that does not conform to the University's established purpose and general rules and policies regarding use of the network.

The University reserves the right, in its sole discretion, to request an explanation and justification regarding any hardware or software not provided by the University's Information Technology Department that is installed on any computer or the network, and at any time to remove the hardware or software from the computer (or the network). It is each user's responsibility to ensure that no one is granted access to the network via the user's computer and that only you have access via your account.

Compliance. Each of us must exhibit exemplary behavior on the network and the internet as a representative of the University community. Good judgment by each of us is primary in maintaining control of the use of our resources; however, we will provide internal and external controls as appropriate and feasible. The controls include the right to determine who is granted access to University-owned equipment and, specifically, to exclude those who do not abide by this or other applicable policies. The University reserves the right to restrict online destinations through software or other means.

From time to time, the University may make determinations on whether specific uses of the network are consistent with University policies. Any use of the network for any purpose that is contrary to University policy is prohibited. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials (including unauthorized copies of software) without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when the duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law. The network may not be used for downloading software or other files not related

to our mission and objectives or for transfer to other computers, personal computer, or other media. This prohibition pertains to freeware, shareware, copyrighted commercial and noncommercial software, and all other forms of software and files not directly related to our instructional and administrative purposes. Use of the network in furtherance of any unlawful purpose is prohibited, including infringing on any intellectual property rights.

Installation of applications or hardware. The installation of applications on our computers is prohibited as discussed above and includes the installation of software or downloading an application through the internet. This section of the policy is intended to provide for permitted discretionary use of applications on our computers consistent with our mission and goals.

If you wish to be granted administrative privileges, which will allow you to create and/or install applications, please contact the Helpdesk and explain how your needs meet the educational mission of the university, and how using the IT office's services will not allow you to easily and fully perform your educational and research mission. A follow-up meeting with the IT department will be scheduled to determine if administrative rights should be granted or not.

Disclaimer. *Even though the University may use technical or manual means to limit access and monitor use, these means are not foolproof and cannot be relied upon to enforce the provisions of this policy. Further, technical issues may arise and there is no guarantee that we can restore any lost data (or repair other damage) that may be caused by the installation or use of unauthorized programs or otherwise. All provisions of this policy are subordinate to local, state and federal statutes. The University reserves the right to change its policies and rules at any time with appropriate notification to affected parties.*

Section 300/2.18 Information Technology
Subject: Audio Visual

Policy
The Help Desk is the central point of contact for all computer, network, telephone, and A/V related support requests. When you contact the help desk for service or support; a ticket is created and assigned to the appropriate department.

While several JU departments work in tandem to provide campus A/V support, it is always best to start at the help desk. This helps ensure there is a record of your request and all the correct parties are notified. Most importantly, if a primary support staff member is out of the office, your request will be rerouted to someone else who can help in his or her absence.

Using the 25Live System to Request Technology Support for Events. When you request A/V or technology support for an event via 25Live, the help desk is contacted on your behalf during this process, so a duplicate request is not necessary.

Section 300/2.19 Information Technology
Subject: Requesting IT Assistance

Policy
All requests for IT services and support must be initiated through the Help Desk. Requests should not be made directly to members of the IT Department.

Section 300/2.20 Information Technology
Subject: Printer Support

Policy
DELL LASER PRINTERS
Dell laser printers are maintained by Saxon Business Systems. If the printer needs to be serviced or repaired, Saxon's contact information can be found on the sticker affixed to the printer.
DELL LASER MULTIFUNCTION PRINTERS
All Dell laser multifunction printers purchased through the IT department have a 3-year warranty from the manufacturer. If the printer needs to be serviced or repaired and is out of warranty, the IT department will evaluate the costs of service or repair and inform the user or department if a new printer purchase is a more cost effective solution. All printers that are still under warranty will be repaired by the IT department if required. Servicing the printer such as new toner, cleaning, fuser replacements, etc, are not covered under the manufacturer warranty and these costs will be covered by the department that owns the printer. The IT department will always help the user or department troubleshoot any printer issues with software or connectivity.
INKJET PRINTERS AND INKJET MULTIFUNCTION PRINTERS
The IT department does not service or repair InkJet printers. Any service or repair will have to go through the manufacturer. The IT department can evaluate the printer and inform the user or department if a new purchase would be a more cost-effective solution in any situation. IT will help the user install the necessary software and verify that a test page can be sent to the printer. However, any printer problems that seem to be related to the printer itself will not be analyzed or repaired by the IT department.
MULTIFUNCTION CORPORATE PRINTERS/COPIERS – Konica Minolta/Xerox
These systems are maintained by Dex Imaging (Konica Minolta) and Saxon Business Systems (Xerox). For service, use the contact information found on the sticker affixed to the copier/printer.

Section 300/2.21 Information Technology
Subject: Backup & Retention

Policy
The process to backup digital communications, data and other electronic files is an essential IT practice to insure against the loss of valuable information. The purpose of backing up the stored data is to allow the university to restore a system to a current state, in case of a system failure, or to restore individual files inadvertently deleted or lost. The backup media is not intended to serve as a short or long-term storage information vault.

The purpose of this policy is to establish a limit on the length of the time backups are maintained and to encourage departments to distinguish between the purposes and practices of backing-up data vs. the retrieval (archive) of data.

Email and File Backup Policy
• Backup procedures will be established to maintain data long enough to provide a reasonable level of insurance against major data losses. Procedures will be based on the nature of the data, the volatility of the data, etc., and will be carefully coordinated with retrieval storage practices (All departments will have their own procedures on the way they keep their data for archiving/compliance).
• Email (Office 365) is not backed up. Email deleted from employee accounts will be recoverable for a period of 60 days. Email deleted from non-employee, student and alumni accounts will be recoverable for 14 days.
• Backups of files including Microsoft Office 365 OneDrive for Business should be retained for no more than 60 days. Files that fall under the university electronic records retention policy are the responsibility of the user and department. Such files must be maintained in a retrievable form independent of backups. Backups are only intended for disaster recovery or deleted items retrieval that fall within the backup retention period. Therefore, the university backups are not intended to satisfy any compliance requirements.

Definitions:
Back-up - A copy of data from an original electronic source transferred to a separate medium (CD, tape, disk). The purpose of back-ups is to restore information lost because of purposeful or inadvertent user action or system failure. Example: Daily and weekly backups of an entire system.
Retrieval Storage (Archive/Compliance) – It is the movement of data from its original source to a separate system or media than from the source. The purpose of retrieval storage is to move data no longer needed on a day-to-day basis to another location from which it can be retrieved later, if needed. Example: Movement of dated transaction files to CD or all data from a completed research trial to zip-disk.
Retention policies - Legal requirements or policies dictating that records of specific types be maintained in retrievable form for a specific period. The purpose of retention policies is to maintain an audit trail or history of information.

Section 300/2.22 Information Technology
Subject: Personal, Departmental and Organizational Websites

Policy
JU maintains a webserver for the purpose of hosting personal websites created by students, faculty, and staff. To protect the university against attacks due to poorly coded websites or vulnerabilities in web utilities, personal websites will be limited to using only HTML, XHTML, CSS, and Java Script. No WordPress, PHP or MySQL database backed sites will be allowed. Content upload to the website will be done via FTPS. Each website will be allowed up to 100MB of storage space.
To request server space for a personal website, contact the Help Desk.

JU has replaced website hosting for faculty, staff and students with Microsoft Office 365 SharePoint for content sharing and OneDrive for storage and file sharing. 4TB of storage space is available per user with this new service. Existing personal websites hosted by JU will be turned off no later than December 31st, 2020.

All SharePoint sites should maintain a common appearance and professional content and are subject to all other standards and policies of the University.

Section 300/2.23 Information Technology
Subject: Wireless Network

Policy
JU provides a wireless network for the benefit of our students, faculty, staff, and alumni. Visitors to the campus are provided with limited Internet access.

The IT department provided the initial provisioning of wireless on campus. We concentrated on classrooms, student residences, study areas and selected outdoor areas. Departments wanting additional wireless coverage for their offices or buildings without wireless will need to provide funding for the hardware and wiring. Wireless for new construction should be factored into the budget for the project.

Students, faculty, staff, and alumni may gain full JU network access via the DolphinNet or JU_Beta SSIDs. DolphinNet is the most secure wireless network. It will work with computers, tablets, and mobile phones. JU_Beta is less secure and used for wireless devices that cannot support the security method used on DolphinNet. Typically, IoT devices (e.g. Smart TVs, gaming devices, smart speakers, etc.) All wireless devices must be registered in our SafeConnect system before they can connect. Go to the IT website (https://www.ju.edu/it/). Look in the How-To section for help with Computer & Device Registration.
Visitors to the campus can connect to our wireless system via the Public SSID. This is a fully open network with no security. This network does not allow any access to our on-campus network and websites. It only allows access to off-campus websites, both regular and secured. Users need to open their web browser and supply their email address to use the Public SSID.

Section 300 / 2.24 Information Technology
Subject: Social Media Policy

Policy
Purpose:
The purpose of this policy is to provide guidance for employees choosing to use social media to communicate, collaborate, and interact with students, faculty, staff, stakeholders, and the general public on matters concerning or impacting Jacksonville University.

Scope:
This policy applies to Jacksonville University employees — representing JU or its programs in an official capacity — who create or contribute to blogs, wikis, social networks or any other kind of social media (both on and off JU.edu). These guidelines also apply to other people (such as volunteers and appointees) who use internally managed university computing resources. This policy applies to all forms of social media, including, for example, Facebook, Twitter, Instagram, Snapchat, YouTube, LinkedIn, blogs, online comments, etc. This policy may apply to employees outside of work hours and while using personal accounts when use of social media affects an individual's professional responsibilities, violates an applicable law, or constitutes a violation of JU regulation or policy. Your online persona, and the content you publish, should be consistent with the Jacksonville University's values, brand guidelines, social media guidelines, policies and professional standards.

Policy Statement:
Jacksonville University is committed to the highest standards of freedom of speech and expression. JU recognizes the vital role that social media can play in both expressing free speech and also in communicating, collaborating, and interacting with students, faculty, staff, non-JU colleagues, and the general public.

This policy intends to protect the appropriate use of social media, while prohibiting conduct through social media that may be unlawful, violative of professional standards, contrary to the University mission, policies, and its culture of respect for all individuals.

Procedures:
During working hours, JU employees may not spend more than minimal work time on personal activities, including the use of social media. Use during breaks and meal period is permitted. In some supervisors may authorize use of personal social media sites and accounts that further university interests.

1. Public communications concerning the Jacksonville University, faculty, staff and all employees of the University and any other affiliates of Jacksonville University must follow JU policies. Accordingly, employee complaints regarding alleged discrimination, unlawful harassment, or safety issues should be made consistent with the complaint procedures in the employee handbook.

2. Social media communications are individual interactions, not organizational communications, unless managing a University's sponsored site in an official capacity. Employees can be held personally liable for their posts. For this reason, employees should use common sense and

exercise caution with regards to exaggeration, obscenity, guesswork, copyrighted materials, legal conclusions and derogatory remarks or characterizations.

3. If you discuss work-related matters online that are within your job responsibility, must disclose your affiliation with the University.

4. You may not disclose any sensitive, proprietary, confidential, legal or financial information about the University or individuals affiliated with the University. You may not disclose information protected under FERPA, HIPAA, or other laws or regulations.

5. While you may respectfully disagree with the University actions, policies or leadership decisions, you may not attack personally or post material that is obscene, defamatory, discriminatory, harassing, libelous or threatening with regard to the University, employees of the University or any affiliates of the University.

6. All Jacksonville University social media accounts must be registered with University Communications and follow Jacksonville University brand guidelines. Please consult with Human Resources if you have any questions about the appropriateness of publishing information relating to the University, its faculty, staff or any affiliates.

For consideration: Possible hyperlinks, relevant policies to consider including

- State and federal laws regarding privacy, defamation, copyright, trademark, obscenity, and child pornography.
- The Florida Computer Crimes Act, The Electronic Communications Privacy Act and the Computer Fraud and Abuse Act
- The JU Student Code of Conduct, Sexual Harassment Policy, Workplace Violence Policy, JU Branding Guidelines, Web Page Policy, Electronic Mail Policy, Acceptable Use Policy.
- Laws from other countries or jurisdictions when communication with persons in other states or countries or using systems or networks that are under another jurisdiction, including GDPR guidelines.

Approved By:
The Office of Information Technology
07/07/2020
Rev 7-20