JSU IT Policies and Procedures

1. General Provisions

    1.1 Purpose
    1.2 Ownership of Hardware, Software and Data
    1.3 Responsibilities
        1.3.1 President
        1.3.2 Computer Policy and Coordinating Committee
        1.3.3 Computer Advisory Committee
        1.3.4 Vice President for Information Technology
        1.3.5 Department of Academic Computing and Network Support
        1.3.6 Department of Administrative Computing and System Support
    1.4 Procedure for Requesting Services
    1.5 Computer Labs
    1.6 Software and Hardware Acquisition
        1.6.1 Procedure for Preparing Request for Purchase of Hardware/Software
    1.7 Software and Hardware Disposition
    1.8 Mail Accounts
    1.9 Release of Information Concerning Computing Facilities
    1.10 Acceptable Use
    1.11 Computer Supplies
    1.12 World Wide Web Pages
        1.12.1 Procedure for Obtaining a Web Site
    1.13 Support for Obsolete Hardware and Software

2. Information Systems Security Plans and Policies

    2.1 Purpose
    2.2 Policy Statement
    2.3 Security Measures
        2.3.1 Unacceptable Use
        2.3.2 System and Network Activities
        2.3.3 Email and Communications Activities
        2.3.4 Use of Removable Media
        2.3.5 Enforcement
    2.4 Breaches of Security
        2.4.1 Monitoring
        2.4.2 Incident Reporting
        2.4.3 Enforcement
        2.4.4 Legal Implications
        2.4.5 Disciplinary Procedures

2.5 Risk Assessment and Compliance
2.5.1 Risk Assessment
2.6 Roles and Responsibilities
2.6.1 JSU Computer Advisory Committee
2.6.2 Vice Presidents, Deans, Directors and Department Heads
2.6.3 Division of Information Technology (DIT)
2.6.4 University Staff and Students
2.6.5 Those Purchasing, Commissioning, Developing an Information System
2.6.6 Third Parties
2.7 Laptop Security
2.7.1 Basic Security Measures

3. Wireless Communication

3.1 Purpose
3.2 Scope
3.3 Registration of Wireless Devices
3.4 Loss or Theft of Wireless Devices
3.5 Approved Technology
3.6 VPN Encryption and Authentication
3.7 Maintenance of Wireless Networks
3.8 Roles and Responsibilities
3.8.1 Users' responsibility
3.8.2 Vice Presidents, Deans, and Department Heads
3.8.5 Division of Information Technology (DIT)
3.9 Enforcement

4. Responsibility for Policy

5. Evaluation

1. General Provisions

1.1 Purpose

Jacksonville State University (JSU) has a wide range of computing and networking facilities available for academic instruction, administrative information processing, and faculty and student research. The Division of Information Technology (DIT) has the responsibility for extending these services on campus. The purpose of the Computer Services policy and the administrative procedures which it prescribes are as follows:

- To ensure that JSU's computers and networks, as well as the information they store and process, are operated and maintained in a secure and responsible manner.
- To establish responsible parties for providing assistance to users in the selection, acquisition and use of computer resources;
- To avoid redundant computer equipment, software and services;
- To maximize the efficient and effective use of available hardware and software systems;
- To insure maximum compatibility among hardware and software systems;
- To improve communication between users of computer services and those who provide the services;
- To maintain the integrity of the information stored in University databases.

This policy establishes general guidelines and procedures for the utilization of the computer facilities of the University and the acquisition of additional hardware and software. In addition, this policy will undergo periodic evaluations and adjustments as required by changes in University business requirements and technological advancements.

1.2 Ownership of Hardware, Software and Data

All University purchased computer equipment, regardless of location or source of funding, is the property of the University and as such will be shared with approved users upon the agreement of the University. All University computer equipment, software and data will be used for University business only. All revenue derived from the sale of computer services, e.g., computer time, equipment, software, program development, documentation, etc., shall be the property of Jacksonville State University and be receipted to the University. Any person or persons found to be in violation of this policy will be subject to disciplinary actions.

1.3 Responsibilities

1.3.1 President

The President has the ultimate responsibility for establishing general policies in the area of computer acquisitions and utilization at Jacksonville State University.

1.3.2 Computer Policy and Coordinating Committee

The Computer Policy and Coordinating Committee has the responsibility for policy guidance, review of and input to long-range planning and coordination of interdepartmental data. This Committee will from time to time receive and review such information and make recommendations to the President. The committee will work with the Vice President for Information Technology (IT) to resolve any user disagreements on priorities for software development work schedules. The Committee will be composed of the Vice Presidents.

1.3.3 Computer Advisory Committee

The Computer Advisory Committee is appointed by the President and has responsibility for providing broad based advisory information from the university community in the form of recommendations to the Vice President, IT and the Computer Policy and Coordinating Committee in the following areas:

- The development of strategic Information Technology goals for the university;
- The establishment of computer-related standards;
- The user procedures for obtaining computer support;
- The planning for supercomputer usage and the prioritization of allotted time;
- The selection of computer systems and software;

1.3.4 Vice President for Information Technology

The Vice President for Information Technology has responsibility for the management of centralized computing resources and for the administration of computer-related activities as specified in this Policy. Included in those responsibilities are:

- Academic Computing and Network Services;
- Administrative Computing and System Support;
- Preparing the annual Information Technology plan;
- Developing the annual Information Technology budgets;
- Establishing routine priorities for scheduled work. Consults with Computer Policy and Coordinating Committee as required to resolve user disagreements on priorities for major software development projects;
- Computer support for externally funded projects;
- Computer support for other agencies;
- Computer hardware and software acquisitions;
- Microcomputer installation/maintenance/repair;
- Desk side assistance for microcomputer users;
- Security of centralized computing facilities and information;
- Control of access to central computing facilities;
- Release of information concerning computing facilities;
- Advising on assessment of needs for computer services;
- Advising on the hardware/software and methods for implementing a computer

service;
- Administration of systems hardware and software.

1.3.5 Department of Academic Computing and Network Support (ACNS)

The Department of Academic Computing and Network Support is responsible for supporting computing and network facilities to be used primarily for academic purposes at the University. A broad range of equipment and software representing up-to-date technology is available through a network of microcomputers distributed in labs across the Campus. The functions assigned to Academic Computing and Network Support includes the following:

- Maintain Luminis campus portal system;
- Establish remote computing labs for instruction and research;
- Purchase, install and maintain equipment and software used in the academic labs;
- Provide personnel required for technical support of faculty, staff and students and for the operation of labs;
- Control access to ACNS-managed labs;
- Provide security of equipment, software and supplies in ACNS-managed labs;
- Assign and administer email accounts and other accounts for various servers;
- Administer the University's World Wide Web site;
- Design and maintain the campus network;
- Maintain the campus network software, hardware, and communication lines;
- Install, diagnose problems and repair supported computer hardware and peripherals throughout the campus;
- Establish and maintain campus network security.

1.3.6 Department of Administrative Computing and System Support

The Department of Administrative Computing and System Support provides a full range of services to the administrative user community of the University. These services are extended through the use of computers, campus networks, and the internet.

This department develops and maintains a variety of systems that support the information processing requirements of the University. The systems accommodate a wide range of forms to maintain and retrieve information that is necessary for effective administrative processes. Software systems are designed to protect the integrity of the data. Individual administrative offices have access to forms that are pertinent to their function. Other offices with a justifiable need may view the data for information only, but are prohibited from changing the data belonging to another functional area of the University**.** The administrative system by design encourages standardization of data campus-wide, provides a timely means of storing and retrieving data, performs extensive edits of input data to keep erroneous data out of the databases, and provides many standard reports and documents required for the successful operation of the administrative functions of the University.

Administrative application software functions are in a constant state of change. Changing policies, procedures, regulations and advancements in technology result in the need for changes in administrative software. A major function of Administrative Computing and System Support is to interact with the administrative users to identify the need for changes in application software, as well as the need for new software, and to develop procedures and programs to meet those needs.

The functions assigned to the Department of Administrative Computing and System Support include the following:

- Maintain integrity of University data through a common data dictionary (database administration);
- Consult with end-users concerning their needs for automation;
- Develop and maintain efficient application software that is responsive to user needs;
- Develop and maintain user guides for software developed by Administrative Computing;
- Conduct training for end-users on the hardware and software available for their support;
- Provide University-wide technical assistance in automation targeted toward improving user productivity;
- Develop and maintain databases of University activity;
- Develop and maintain security systems (physical hardware and software) to safeguard University information and its use;
- Maintain the central computer system and vendor software in a manner which minimizes downtime;
- Manage and operate the central computer systems, maintain computer supplies, etc.;
- Provide reporting capability to authorized representatives of the various administrative offices;

1.4 Procedure for Requesting Services

Requests for Computer Services must be submitted to Information Technology using the online Computer Services Request (CSR) form (http://jsuis.jsu.edu/). The form contains space to identify the requester, describe the request, communicate a justification for the services requested, and obtain proper approval through administrative channels. Each request will be reviewed to insure that the following requirements have been met:

- The request has been properly approved through the administrative channels. The CSR form provides the requester with the capability to electronically route the form to various levels in the organization (e.g., Department Head, Dean/Director, Vice President) or directly to the Computer Center for approval. In general, requests that require the allocation of funds or that require significant human resources should be routed through the organizational channels. If a

request is received in Information Technology without the appropriate level of approval, the request will be electronically rerouted by Information Technology to the appropriate person for approval. It should be noted that approval by the head of the office responsible for requested information is also required (e.g., a request for faculty/staff mailing labels will require approval of the Director of Human Resources and a request for information on student financial aid will require the approval of the Director of Financial Aid).
- The request will not generate redundant work (Example: request for a report or service that already exists);
- The request is feasible, procedurally and economically;
- Resources are available to perform the request;

If the request meets all of the above requirements for approval, it will be given a priority to be scheduled for implementation.

If the request fails to meet one of the requirements for approval, it will be noted on the request and returned to the requester.

The requester may appeal to the Computer Policy and Coordinating Committee for a reconsideration regarding the decision from the approval process.

Examples of requests that should be submitted using the online Computer Services Request (CSR) system are:

- Request for New Application
- Request for New Program
- Request for a Change to a Program
- Request for Information
- Request for Microcomputer Training
- Request for Consultant in Area of Automation
- Request for Computer Installation, Maintenance, and Repair Service

1.5 Computer Labs

Academic computing labs managed by the Division of Information Technology (http://www.jsu.edu/dit/acns/general/labs.html) will be available on an “open use” basis to authorized users, except when specifically reserved in advance. All lab facility reservations and scheduling will be accomplished in a manner to insure the most effective use of the facilities. Priority for unscheduled resources will be given to regular academic programs.

Department heads or other administrative personnel will coordinate the scheduling of open use academic computing labs with the Director of Academic Computing and Network Support. Details on scheduling labs can be found at: http://www.jsu.edu/dit/acns/general/labs.html.

It is essential that requests for software installation in the labs be submitted well in advance of the required date of use. The schedule for requesting software installations for the labs can be found at:
http://www.jsu.edu/dit/acns/policies/labsoftwarerequest.html

All requests for software changes in the labs after the specified dates will require approval by the Vice President of Information Technology.

1.6 Software and Hardware Acquisition

The proliferation of technology has led to the availability of a host of hardware and software systems. The use of computers for the support of information processing in routine office administration has created a high demand for computers and peripherals. Jacksonville State University has experienced this rise in the use of computers for office administration. Being an institution of higher learning, the requirement for computers to be used in academic programs has also increased significantly.

The use of computers in virtually all phases of University operations necessitates implementation of a policy regarding the acquisition of computer hardware and software. The policy must have the objectives of:

- Minimizing the total cost for products of automation while maximizing the efficiency of their use;
- Providing a method for requesting computer equipment that will flow easily through the necessary channels for approval;
- Providing a degree of control on the diversity of computer equipment and software purchased to minimize the cost of training and support of the products.

The Division of Information Technology has been given the responsibility for administering the acquisition, use, control, training and support as related to automation at the University**.** The Computer User Advisory Committee will serve in an advisory capacity as required to administer the acquisition of computers, peripherals and software.

1.6.1 Procedure for Preparing Request for Purchase of Hardware/Software

The policy will apply to any purchase or lease of computer hardware or software, with an accumulated cost which exceeds $500.00 and will be administered according to the procedures outlined below:

- If not sure of the hardware or software needed, request consultant service from Information Technology using the online Computer Services Request form (http://jsuis.jsu.edu/).
- Determine the hardware or software required.
- Determine if the desired hardware and/or software is on the standard purchase list of computers and software supported by the Division of Information Technology (http://www.jsu.edu/dit/acns/general/purchasing.html).
- Prepare form CAQ: 01: “Request for Approval to Purchase Computer Hardware

and Software form" (http://www.jsu.edu/depart/acsv/purchase.pdf). Fully explain the requirement and how the requested items will be used to satisfy the requirement. Justification will be required. If the requested items are not on the standard purchase list, state the reason a substitute is required.

- Submit the request form to the Vice President for Information Technology through the appropriate channels for approval. The request form must be approved by the dean/director/department head who serves as budget manager of the funding account prior to submission to the Vice President for Information Technology.

The Vice President for Information Technology will review the request. If the request is approved, the requester is authorized to prepare a requisition for the purchase. A copy of Form CAQ:01 must be attached to the purchase requisition. (Any purchase which exceeds $7,500 must be bid.)

If the recommendation of the Vice President for Information Technology is for disapproval, the request will be returned to the requester. The requester may submit an appeal to the Computer Policy and Coordinating Committee. The appeal will consist of a memorandum of justification for the appeal and an attached copy of the disapproved request. The Computer Policy and Coordinating Committee will make a recommendation to approve or disapprove the appeal and forward the request to the President for final decision.

1.7 Software and Hardware Disposition

All computer systems, electronic devices, and electronic media must be properly cleaned of sensitive data and software before being transferred outside JSU either as surplus property or trash, Computer hard drives must be sanitized by using software that is compliant with Department of Defense standards. Non-rewritable media, such as CDs or non-usable hard drives, must be physically destroyed. The Division of Information Technology will perform this service upon request, but the primary responsibility for sanitizing computer systems, electronic devices, and media rests with the units that purchase them.

1.8 Email Accounts

Jacksonville State University employees and currently enrolled students are provided with email accounts on the university's web-based email system. If an email account is required for JSU business purposes by someone other than a JSU employee or currently enrolled student, a Computer Services Request (CSR) must be submitted by the appropriate vice president. The CSR must include the name of the requesting individual or organization and the name of a JSU employee who will be responsible for the account. A JSU email account is a privilege, not a right, and use of the email account may be withdrawn for violations of JSU's requirements for responsible use of university computing resources as set forth in this policy.

Email left in the inbox or sent-mail folder on the mail server will eventually expire if not moved to a folder for permanent storage. Details on JSU's mail expiration policy can be found at: http://www.jsu.edu/dit/acns/email/gemhelp.html#inbox.

1.9 Release of Information Concerning Computing Facilities

No party shall release technical specifications of software or computer-based systems at Jacksonville State University without prior approval. Anyone who wishes to release information concerning systems, to make presentations that require release of data or systems procedures in part or in whole, or to entertain visitors with the intent of viewing computing procedures, will submit an online Computer Services Request (http://jsuis.jsu.edu/) to the Vice President for Information Technology one week prior to the event. Upon approval, Information Technology will provide support staff, if deemed necessary, to the requesting party.

1.10 Acceptable Use

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

As a part of the physical and social learning infrastructure and to further the educational purposes of the University, Jacksonville State University often acquires, develops, and maintains computers, computer systems, and networks. These computing resources are the property of Jacksonville State University intended for University-related purposes, including direct and indirect support of the University's instruction, research, and service missions; of University administrative functions; of campus activities; and of the exchange of ideas among members of the University community and between the University community and broader academic communities.

Generally, academic freedoms apply to the use of University computing resources. So too, however, do the responsibilities and limitations associated with those privileges. The use of University computing resources, like the use of any other University-provided resource and like any other University-related activity, is subject to the requirements of legal and ethical behavior within the University community. Thus, legitimate use of a computer, computer system, "email" or network does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

All users of university computing resources must comply with all federal, Alabama, and other applicable law; all generally applicable university rules and policies; and all applicable contracts and licenses.

This policy applies to all users of University computing resources, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations.

1.11 Computer Supplies

Procurement of storage media and supplies is the responsibility of individual users. Printing supplies required by computing labs using the Uniprint system will be provided from funds generated by that system. Uniprint funds provided for any lab will be limited to the Uniprint revenue produced by that lab.

Custom forms to be printed on printers attached to the central administrative computing system must be approved by Information Technology prior to placing the order to the vendor. This is necessary to insure compatibility with the hardware and software specifications. Information Technology will provide assistance in the design of forms. Requests for assistance in form design should be submitted on an online Computer Services Request (http://jsuis.jsu.edu/).

1.12 World Wide Web Pages

The design and implementation of JSU's World Wide Web Site is a highly collaborative, cross-disciplinary activity. JSU is converting its web pages to the Luminis Content Management System (LCMS). Guidelines and standards are being developed by the Luminis Project Team. Web pages must be developed to conform to the guidelines established by the Project Team. Any deviation from the university standards must be approved by the Project Team.

1.12.1 Procedure for Obtaining a Web Site

JSU's policy for World Wide Web pages can be found at:
http://www.jsu.edu/dit/acns/policies/webpolicy.html.

1.13 Support for Obsolete Hardware and Software

Due to rapidly changing technology and constraints on resources available for computer support, it is necessary to limit the support of older technologies. Information regarding the support level of hardware and software can be found at the following web pages:
http://www.jsu.edu/dit/acns/policies/obsoletecomputerpolicy.html
http://www.jsu.edu/dit/acns/policies/printerpolicy.html

2. Information Systems Security Plans and Policies

2.1 Purpose

The purpose of this Information Systems Security Policy and its supporting policies is to define the security controls necessary to safeguard Jacksonville State University's, hereafter referred to as "JSU", "JSUNet" or the "University", Information Systems and ensure the security, confidentiality, and integrity of the information held therein.

Effective security is a team effort involving the participation and support of every JSU employee, student and affiliate who deals with information and/or information systems. This can only be achieved if all staff and students observe the highest standards of ethical, personal and professional conduct. Effective security is achieved by working with a proper discipline, in compliance with legislation and University policies.

The Information Systems Security Policy and supporting policies are designed to:

- Ensure that information is created, used and maintained in a secure environment.
- Ensure that all of Jacksonville State University's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse.
- Ensure that all users are aware of and fully comply with this Policy Statement and the supporting policies and procedures.
- Ensure that all users are aware of and fully comply with the relevant government legislation.
- Create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure all University owned assets have an identified owner /administrator.

2.2 Policy Statement

Information is a critical asset of Jacksonville State University. Accurate, timely, relevant, and properly protected information is essential to the success of JSU's academic and administrative activities. JSU is committed to ensuring all accesses to, uses of, and processing of University information is performed in a secure manner.

Technological Information Systems hereafter referred to as 'Information Systems' play a major role in supporting the day-to-day activities of JSU. These Information Systems include but are not limited to all infrastructure, networks, hardware, and software, which are used to manipulate process, transport or store Information owned by JSU.

The Policy provides a framework in which security threats to JSU Information Systems can be identified and managed on a risk basis and establishes terms of reference, which are to ensure uniform implementation of Information security controls throughout JSU.

JSU recognizes that failure to implement adequate Information security controls could potentially lead to:

- Financial loss
- Irretrievable loss of Important University Data
- Damage to the reputation of JSU
- Legal consequences

Therefore measures must be in place, which will minimize the risk to JSU from unauthorized modification, destruction or disclosure of data, whether accidental or deliberate. This can only be achieved if all staff and students observe the highest standards of ethical, personal and professional conduct. Effective security is achieved by working with a proper discipline, in compliance with legislation and University policies, and by adherence to the Terms and Conditions for use of JSUNet.

The VP of Information Technology and his/her delegated agents will enforce the Information Security Policy and associated supporting policies. The day to day enforcement of the Security Policy will be overseen by the Information Security Officer. This role is typically held by the Director of Academic Computing and Network Support.

2.3 Security Measures

While JSU's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of JSU. Because of the need to protect JSU's network, management cannot guarantee the confidentiality of information stored on any network device belonging to JSU.

1. For security and network maintenance purposes, DIT may monitor equipment, systems and network traffic at any time.
2. JSU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
3. Employees and students should take all necessary steps outlined in this and other supporting policies to prevent access to confidential information. Examples of confidential information include but are not limited to University private information, University strategies, sensitive research data, trade secrets, or student and employee personal information.
4. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
5. All PCs, laptops and workstations should be secured with password protection with the automatic activation feature, or by logging-off when the host will be unattended.
6. Because information contained on laptop computers and other mobile devices is especially vulnerable, special care must be exercised. Protect laptops in accordance with the Laptop Security section of this policy.
7. Postings by employees/students from a JSU email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of JSU, unless posting is in the course of business duties.
8. All hosts used by the employee that are connected to the JSU Internet/Intranet/Extranet, whether owned by the employee or JSU, shall be continually executing approved virus-scanning software with a current virus database.

9. Employees/students must use extreme caution when downloading from the internet or when opening e-mail attachments received from unknown senders. All data, programs and emails must be scanned before downloading or opening.
10. Access to JSU administrative systems (e.g., systems containing student records, employee data, or other confidential information) must be configured and administered by DIT on JSU-owned equipment.

2.3.1 Unacceptable Use

The following activities are, in general, prohibited. Employees/students may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee or student of JSU authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing JSU-owned resources.

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

2.3.2 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or University protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by JSU.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which JSU or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a JSU computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any JSU account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to DIT is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, JSU employees/students to parties outside JSU.

2.3.3 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within JSU's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by JSU or connected via JSU's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.3.4 Use of Removable Media

Removable media is defined as any portable storage medium. Removable media examples include, but are not limited to, the following: CDs, DVDs, Flash Cards, Jump Drives, and Hard Drives. In general, the use of removable media is allowed for JSU employees to conduct appropriate University business within the bounds of the JSU Information Technology Policy. The exception to this is the use of removable media to transport sensitive data (i.e. employee or student records that could specifically identify an individual). In this case, the use of removable media is not allowed unless no other means exists to transport the data – in such cases encryption must be used if to guard against the compromise of data on media that is misplaced. Users are encouraged to use the disk storage that is available on University servers and to consult with the Division of Information Technology personnel if assistance is needed in transferring data.

2.3.5 Enforcement

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

2.4 Breaches of Security

2.4.1 Monitoring

The Division of Information Technology (DIT) will monitor network activity and take action/make recommendations consistent with maintaining the security of JSU information systems.

2.4.2 Incident Reporting

All suspected information security incidents must be reported as quickly as possible to DIT. All University staff and students have a duty to report information security violations and problems to DIT on a timely basis so that prompt remedial action may be taken. The VPIT or his appointee will be responsible for dealing with all incidents. Records describing all reported information, security problems and violations will be created. These records will be stored securely for five years after which time all information pertaining to individuals will be removed.

2.4.3 Enforcement

DIT has the authority to invoke the appropriate University disciplinary procedures to protect JSU against breaches of security. In the event of a suspected or actual breach of security, DIT may, after informing the relevant Administrator, make inaccessible/remove any unsafe user accounts, data and/or programs on the system from the network.

2.4.4 Legal Implications

Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of data protection laws and could lead to civil or criminal proceedings. It is vital, therefore, that users of JSU Information Systems comply with this and other related policies.

2.4.5 Disciplinary Procedures

Failure of an individual student or employee to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken.

Failure of a contractor to comply may lead to the cancellation of contract and/or legal action.

2.5 Risk Assessment and Compliance

2.5.1 Risk Assessment

It is the responsibility of individual departments to carry out risk assessments of the business value of the information being handled and the security controls in place for protecting this information. DIT will weigh security risks vs. practicality when recommending updates/upgrades (i.e. to operating systems, software packages, etc.). Department Heads and/or Directors must establish effective contingency plans appropriate to the outcome of any risk assessment.

2.6 Roles and Responsibilities

2.6.1 JSU Computer Advisory Committee

1. Evaluate and make recommendations regarding IT Security Policies,
2. Support the Division of Information Technology (DIT) in the enforcement of the policies where necessary.

2.6.2 Vice Presidents, Deans, Directors and Department Heads

The Vice Presidents, Deans, Directors, Department Heads and their staff who have computer hardware and software in their area are responsible for the security of the data, equipment, software, documentation and the prevention of unauthorized use of their systems. Other responsibilities are as follows:

1. Implement the policies for Information Systems that are operated by their departments.
2. Ensure that staff, students and other persons authorized to use the systems are aware of and comply with the associated supporting policies and procedures.

3. Ensure their Information Systems are formally administered. (All IT systems must be formally administered either by an administrator appointed by the Department Head and/or Director or centrally by the Division of Information Technology (DIT)).
4. Where a department operates an autonomous network with a connection to the JSU Backbone, then the respective Network Administrator's Department Head or their nominated agents will implement the policies.
5. Establish effective contingency plans appropriate to the outcome of any risk assessment.
6. Maintain a backup of computer files used by their offices.

2.6.3 Division of Information Technology (DIT)

The Vice President for Information Technology has responsibility for establishing and maintaining the physical security of all central computing facilities. Central academic computing labs, during operating hours, fall under the jurisdiction of the Director of Academic Computing and Network Support, even though it is acknowledged that the building manager has, by JSU policy, overall responsibility for all facilities in the entire building. Student lab assistants working in central academic computing labs report to the Director of Academic Computing and Network Support. Other responsibilities include:

1. Advise JSU officers, Administrators and other appropriate persons on compliance with this policy and its associated supporting policies and procedures.
2. Review and update the Security policy and supporting policies and procedures.
3. Promote the policy throughout the University.
4. Periodically assess the security controls as outlined in the Security Policy and supporting policies and procedures.
5. Investigate Security Incidents as they arise.
6. Maintain Records of Security Incidents.
7. Report to the JSU Computer Advisory Committee, JSU officers, Administrators and other appropriate persons on the status of security controls within JSU.
8. Perform risk assessments, review all risk assessments completed by other parties and highlight any measures needed to reduce risk in Information Security areas.
9. Maintain JSU's Networks and provide for the support and advice to all nominated individuals with responsibility for discharging these policies.
10. Monitor JSU’s Networks and take action where necessary to maintain the security of JSU’s Information Systems.
11. Remove any unsafe user accounts, data and/or programs when deemed necessary to safeguard the security of JSU’s Information Systems.
12. Maintain a file backup system of all files stored on centralized computing systems.
13. Ensure that data stored in the centralized computer files is available only to users who supply valid sign on and operator credentials.

2.6.4 University Staff and Students

1. It is the responsibility of each individual Information Systems user to ensure his/her understanding of and compliance with this Policy and supporting policies and any associated Codes of Conduct.
2. All individuals are responsible for the security of JSU Information Systems assigned to them. This includes but is not limited to infrastructure, networks, hardware and software. Users must ensure that any access to these assets, which they grant to others, is for University use only, is not excessive and is maintained in an appropriate manner.
3. Report security incidents to the DIT immediately.

2.6.5 Those Purchasing, Commissioning, Developing an Information System

1. All individuals who purchase, commission or develop an Information System for JSU are obliged to ensure that this system conforms to necessary security standards as defined in this Information Security Policy and supporting policies.
2. Individuals intending to collect, store or distribute data via an Information System must ensure that they conform to University defined policies and all relevant legislation.

2.6.6 Third Parties

1. Before any third party users are permitted access to JSU Information Systems, specific written approval from the VPIT is required.
2. Prior to being allowed to work with JSU Information systems, satisfactory references from reliable sources should be obtained and verified for all third parties which includes but is not limited to; administrative staff, software support companies, engineers, cleaners, contract and temporary appointments.
3. Data processing, service and maintenance contracts should contain an indemnity clause that offers cover in case of fraud or damage.
4. Independent third-party review of the adequacy of and compliance with information system controls must be periodically obtained.

2.7 Laptop Security

2.7.1 Basic Security Measures

Recommendations for basic security measures for laptop computers can be found at http://www.jsu.edu/dit/acns/policies/laptop-security.html.

3.0 Wireless Communication

3.1 Purpose

This policy prohibits access to Jacksonville State University (JSU) networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by JSU's Division of Information Technology (DIT) are approved for connectivity to JSU's networks or other related systems. Any wireless network access to JSU administrative systems (e.g. systems containing student records, employee data, or other confidential data) must be configured and administered by DIT on JSU-owned equipment. Wireless access will be granted only to those networks/resources deemed appropriate by DIT.

3.2 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of JSU's internal networks or other related systems. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to JSU's networks do not fall under the purview of this policy.

3.3 Registration of Wireless Devices

All wireless Access Points / Base Stations connected to JSU networks or other related systems must be registered and DIT-approved. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in university laptop or desktop computers must be registered with DIT. Any other wireless technologies that access JSU networks, or other related systems, must be approved and registered with DIT. All the above named devices must be labeled and inventoried.

3.4 Loss or Theft of Wireless Devices

Users must report any lost or stolen wireless devices to their supervisor or DIT as soon as possible. Access to JSU networks or other related systems must be immediately disabled for these devices.

3.5 Approved Technology

All wireless access to JSU networks, or other related systems, must use DIT-approved vendor products and security configurations.

3.6 Encryption and Authentication

Any wireless traffic traversing the JSU administrative network must be encrypted or use VPN technology as specified by DIT personnel. Furthermore, this equipment must be configured by DIT personnel or its installation inspected and approved by DIT personnel.

3.7 Maintenance of Wireless Networks

Security risks and controls should be evaluated more frequently for wireless technologies than for other networks and systems. Patches and security enhancements will be applied to wireless networks in accordance with JSU DIT policy.

3.8 Roles and Responsibilities

3.8.1 Users' responsibility

1. Adhere to JSU procedures and guidelines regarding the use of wireless technologies, both within JSU and when connecting to JSU from remote locations.
2. Safeguard wireless devices in their possession.
3. Safeguard JSU information resources being accessed or transmitted via any wireless technology.
4. Promptly report the loss or theft of wireless devices, or any other breach of wireless security, to their supervisor or DIT.
5. Obtain security approval prior to deploying any wireless technologies.

3.8.2 Vice Presidents, Deans, Directors and Department Heads

1. Ensure their employees understand and adhere to this policy.
2. Use risk management procedures to ensure that risks have been analyzed and appropriately mitigated prior to, and during, use of any wireless technology resources that they own.
3. Forward reports of loss or theft of wireless devices to DIT.

3.8.5 Division of Information Technology (DIT)

1. Maintain a list of approved Access Points / Base Stations.
2. Maintain a list of approved wireless technologies and security configurations.
3. Follow up on items reported as lost or stolen to ensure risk has been diminished.
4. Maintain a VPN encryption and authentication policy.
5. Maintain a list of patches and security enhancements related to wireless networks.
6. Maintain DIT-owned wireless infrastructure. Other departments who procure wireless equipment must maintain/support their own equipment.
7. Communicate wireless security policies and procedures to the users of their resources.
8. Maintain and facilitate a maintenance schedule to evaluate security risks and controls periodically and to implement any new patches or security enhancements.
9. Safeguard wireless information resources with which they have been entrusted.
10. Adhere to JSU policies and procedures for the administration of wireless devices, including:

    a. Labeling all wireless devices prior to deployment.
    b. Maintaining an inventory of all wireless devices.
    c. Disabling access or service for wireless devices that have been lost or stolen.
11. Perform penetration tests on Access Points / Base Stations.
12. Audit the use of wireless technologies at, or in connection to, JSU to ensure that appropriate security controls are in place and used to mitigate risk.
13. Audit the SSID setting to ensure it doesn't contain any identifying information.

3.9 Enforcement

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

4. Responsibility for Policy

The Vice President for Information Technology is responsible for this policy.

5. Evaluation

This policy will be reviewed biannually.