Valdosta State University

Emergency Policy

Title: **Information Resources Acceptable Use Policy**

Sunset: **December 10, 2011**

Philip L. Gunter, Provost & Vice President for Academic Affairs

Patrick J. Schloss, President

(signatures on file)

Valdosta State University

Information Resources Acceptable Use Policy

Date: December 10, 2010

1. Overview

University information and information resources shall be used in an approved, ethical, and lawful manner to avoid loss or damage to University operations, image, or financial interests and to comply with official policies and procedures. Students and personnel shall contact the Director of Information Technology prior to engaging in any activities not explicitly covered by these policies.

2. Scope

The University or University System owns all University information resources; use of such resources constitutes consent for the University to monitor, inspect, audit, collect, and remove any information without permission or further notice. Students and personnel shall be trained in what use is acceptable and what is prohibited. The university regards any violation of this policy as a serious offense. Violators of this policy are subject to university disciplinary action as prescribed in the undergraduate and graduate honor codes, and the student and employee handbooks. Offenders may be prosecuted under the Georgia Computer Systems Protection Act (O.C.G.A. 16-9-20) and other applicable state and federal laws.

3. Designation of Representatives

3.1 University President shall be responsible for the following:

- The President of Valdosta State University shall be responsible for ensuring appropriate and auditable security controls are in place.

3.2 Vice Presidents and Cabinet Members shall be responsible for the following:

- Informing personnel of University policies on acceptable use of information resources.
- Ensuring that application development personnel under their supervision comply with these policies and procedures.
- Ensuring that non-university contract personnel under their supervision comply with these policies and procedures.

3.3 Vice President for Student Affairs shall be responsible for the following:

- Informing current and new students of University policies on acceptable use of information resources.
- Ensuring that students comply with University policies and procedures.

3.4 System Administrators and Data Custodians shall be responsible for the following:

- Monitoring systems for integrity.
- Maintaining and ensuring data backups of critical electronic information.
- Promptly reporting suspicion or occurrence of any unauthorized activity to the Director of Information Technology or her or his designees.

3.5 The University Information Security Taskforce shall be responsible for the following:

- Developing and maintaining the University's information resource security policies.
- Developing and disseminating awareness and training materials.
- Assuring compliance through compliance auditing.
- Reporting compliance auditing findings to the University's Director of Information Technology.

3.6 All students and personnel shall be responsible for the following:

- Abiding by official University policies on acceptable use of information resources.
- Promptly reporting suspicion or occurrence of any unauthorized activities to the Director of Information Technology or one of her or his designees.
- Any use made of their accounts, logon IDs, passwords, PINs, and tokens.

3.7 The Director of Information Technology or one of her or his designees shall be responsible for the following:

- Ensuring the availability, integrity, and confidentiality of the University's information resources
- Addressing violations of University policies on information resources.
- Interpreting University policies on information resources.

4. Hardware and Software

4.1 Acquiring Hardware and Software

To prevent the introduction of malicious code and protect the integrity of University information resources, all hardware and software shall be obtained from official University sources. Users shall not be permitted to install and/or modify information resources in a manner that diminishes security standards set forth by the institution.

4.2 Complying with Copyright and Licensing

All software used on University information resources shall be procured in accordance with official University policies and procedures, and shall be licensed, and registered in the name of the University. All students and personnel shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

4.3 Using Personally Owned Software

To protect the integrity of the University information resources, students and personnel shall not use personally owned software on University owned equipment. This includes purchased and licensed applications; shareware; freeware; downloads from bulletin boards, Internet, Intranet, FTP sites, local area networks (LANs) or wide area networks (WANs); and other personally-owned or controlled software unless otherwise authorized by the Director of Information Technology or her or his designees (documented approval shall be secured prior to use and/or installation of personally owned software on University owned equipment).

5. Protecting Intellectual Property

To ensure the integrity of University and personal intellectual property, all students and personnel shall abide by the intellectual property protection policies of the University.

Copyrights are granted in order to give a copyright holder an incentive to be able to profit from their work. A copyright gives a copyright holder the sole right to distribute their creative work, and only the copyright holder has the legal right to control the distribution of a copyrighted file.

- Peer-to-Peer (P2P) applications work by sharing out files to others and at the same time allowing the user to download files from others.
- If a P2P file is copyrighted and the copyright owner prohibits free downloading, P2P sharing of the copyrighted work is a violation of federal copyright law.

- In addition, P2P file sharing software that is installed on your PC may share out more than intended, such as personal documents found on the hard drive or may even allow access into the system giving control of your PC to others.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. Penalties for copyright infringement may also include sanctions imposed by the student conduct process.

6. Electronic Mail and Messaging

Access to the University electronic mail (email) system is provided to all students and personnel for dissemination of information and conducting University business. Since email may be monitored, all students and personnel using University resources for the transmission or receipt of email shall have no expectation of privacy.

6.1 Acceptable Use

The University provides email to facilitate the conduct of University business. Use of electronic mail and/or electronic messaging resources shall not be done in a manner that interferes with the University's ability to perform its mission and shall meet the conditions outlined in official University directives, missions, and/or goals. However, while messages remain in the system, they shall be considered to be in the possession and control of the University.

6.2 Prohibited Use

Prohibited activities when using University electronic mail shall include, but not be limited to, sending or arranging to receive the following:

- Information that violates University policies, regulations, local, state, or federal laws.
- Unsolicited commercial announcements or advertising material, unless approved by management in advance.
- Any material that may defame, libel, abuse, tarnish, present a bad image of, or portray in false light, the University, the University System, the recipient, the sender, or any other person.
- Offensive material, chain letters, unauthorized mass mailings, email hoaxes, or malicious code.

6.3 Encryption

Encrypting electronic mail or messages shall comply with the following:

- Use encryption software and the methods approved by official University resources.
- Place the key or other similar file for all encrypted electronic mail in a directory or file system that can be accessed by authorized administrative personnel prior to encrypting email.
- Supply the key or other device needed to decrypt the electronic mail upon request by authorized University Administration.

7. Internet

Access to the Internet is available to students, faculty, staff, and approved guests, whose duties require it for the conduct of University business. Since Internet activities may be monitored; all students and personnel accessing the Internet shall have no expectation of privacy.

7.1 Acceptable Use

The University provides Internet access to facilitate the conduct of University business. Use of the Internet shall not be done in a manner that interferes with the work of students, personnel, or the University's ability to perform its mission, and shall meet the conditions outlined in official University directives or goals.

7.2 Prohibited Use

Prohibited activities when using the Internet include, but are not limited to, the following:

- Posting, sexually-explicit material, hate-based material, hacker-related material, or other material that may be deemed detrimental to the integrity and the mission of the University.
- Posting or sending restricted information outside of the University without proper or formal authorization.
- Using other services available on the Internet, such as FTP or Telnet, on systems for which the user does not have an account, or on systems that have no guest or anonymous account for the service being used.
- Posting commercial announcements or advertising material.
- Promoting or maintaining a personal or private business.
- Receiving news feeds and push-data updates, unless the material is required for University business.
- Using non-work or non-academic related applications or software that occupies excess workstation or network processing time.

8. University Supplied Anti-Virus Resources

The University provides a campus-wide license for computer anti-virus to alleviate the proliferation of computer viruses. All laptops, desktops, and workstation computers attached to other University supplied resources shall comply with the following:

- Have University supplied anti-virus software installed, updated, and active at all times of operation.
- Report if anti-virus software is not properly updated.

9. Credit Card Data

All University supplied services and/or materials offered by the University will comply with credit card industry standards. No credit card data will be stored on or transverse the University computer network in an unsecured manner.

10. Personally Identifiable Information

Personally Identifiable Information (PII) is defined by federal and state laws as a combination of two or more of the following: e.g., full name, birthdate, SSN, driver's license number, birth place, personal identification numbers. The combinations of these data are used to uniquely identify individuals. When two or more of these data types exist within the same data structure the data becomes confidential and will not be stored on individual user's desktop computers. Confidential and PII data must be securely stored on centrally managed server resources with designated Data Custodians.

11. Authorized Monitoring

System administrators and other personnel with unrestricted access to email, network usage systems, file or storage servers and similar services shall receive approval from the Director of Information Technology or her or his designees prior to decrypting or reading the data or traffic of students or personnel. If Administrative approval is not immediately available, then system administrators and other personnel that intercept, read, or restrict resources or accounts shall document their actions. All interceptions of data shall be documented and provided to the Director of Information Technology.

12. Generally Prohibited Uses of Information Resources

Generally prohibited activities when using University information resources shall include, but are not limited to, the following:

- Stealing or copying of electronic files without permission.
- Violating copyright laws.
- Browsing the private files or accounts of others, except as provided by appropriate authority.
- Performing unofficial activities that may degrade the performance of systems, such as the playing of electronic games.
- Performing activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.
- Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any University computer, network, or information.
- Installing or attaching communication device(s) on computers or networks that allow off-campus devices to attach to the University network or computers without authorization.
- Promoting or maintaining a personal or private business, or using University information resources for personal gain.
- Using someone else's logon ID and password.
- Conducting fraudulent or illegal activities.
- Conducting fundraising, endorsing any product or service inconsistent with the mission of the university, lobbying, or participating in any partisan political activity.
- Disclosing restricted University information.
- Performing any act that may defame, libel, abuse, or tarnish the University or any person.
- Engaging in conduct that is inconsistent with the stated goals and mission of the university.

13. References

USG Academic Affairs Handbook, Personnel Policies, etc.
http://www.usg.edu/policies/

Board of Regents Policy Manual
http://www.usg.edu/policymanual/

USG Board of Regents Information Security Policy
http://www.usg.edu/policymanual/section7/policy/7.12_information_security_policy/

USG Facilities Guidelines for Instructional Technology
http://www.usg.edu/ref/capital/it_guide.phtml

USG Peachnet Acceptable Use Policy
http://www.usg.edu/peachnet/policy.phtml

VSU Campus Homeland Security Policy
http://www.valdosta.edu/vsu/policies/cover_page_3801.shtml

VSU Email Policy
http://www.valdosta.edu/vsu/policies/cover_page_2101.shtml

VSU Fax Confidentiality and Security Policy:
http://www.valdosta.edu/vsu/policies/cover_page_2142.shtml

VSU Information Resources Acceptable Use Policy (this document)
http://www.valdosta.edu/vsu/policies/cover_page_2102.shtml

VSU Information Security Policy
http://www.valdosta.edu/vsu/policies/cover_page_2141.shtml

VSU Division of Information Technology
http://www.valdosta.edu/it/

VSU Electronic Accounts Quick Reference
http://www.valdosta.edu/helpdesk/accounts.shtml

VSU Intellectual Property Policy
http://www.valdosta.edu/vsu/policies/cover_page_2405.shtml

VSU Policy on Confidentiality and Privacy Policy under HIPAA
http://www.valdosta.edu/vsu/policies/cover_page_3607.shtml

VSU Policy Pursuant to the Gramm Leach Bliley Act
http://www.valdosta.edu/vsu/policies/cover_page_2143.shtml

VSU Records Retention Policy
http://www.valdosta.edu/vsu/policies/cover_page_2001.shtml

VSU Related Policies
http://www.valdosta.edu/vsu/policies/