Information Resources Acceptable Use

Information Resources Acceptable Use

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 Chief Information Officer 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. Personnel shall be trained in what use is acceptable and what is prohibited. Information Security will send regular security awareness bulletins to students to address that population as well. 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. 16-9-93) 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.
Assigning data stewards for data assets within their purview.

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 Data Stewards shall be responsible for the following:

Evaluating and authorizing requests for access to data and data systems.
Establishing data entry standards and ensuring data integrity.
Regularly auditing access for appropriateness employing principle of least privilege.

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

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 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 Chief Information Officer 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.

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

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

USG Board of Regents Cybersecurity Policy §10.4
https://www.usg.edu/policymanual/section10/C442/

USG Facilities Guidelines for Instructional Technology
https://www.usg.edu/facilities/assets/facilities/documents/facilities_it_guidelines.pdf

USG Peachnet Acceptable Use Policy
https://www.usg.edu/peachnet/network/acceptable_use_policy

VSU Homeland Security and Emergency Management Policy
https://www.valdosta.edu/administration/policies/documents/homeland-security-and-emergency-management.pdf

VSU Email Policy
https://www.valdosta.edu/administration/policies/documents/email-web-and-portal.pdf

VSU Information Security Policy
Information Security

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

VSU Electronic Accounts Quick Reference
http://www.valdosta.edu/administration/it/helpdesk/vsu-accounts/welcome.php

VSU Policy on Confidentiality and Privacy Policy under HIPAA
Confidentiality and Privacy Policy under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

VSU Policy Pursuant to the Gramm Leach Bliley Act
Security of Student Information (Gramm-Leach-Bliley Act)

Information Resources Acceptable Use