



# Information Resources Acceptable Use

Date: December 10, 2010

Revised: July 1, 202 TJ ET Q q 0.00000912 0 612 792 re W\* n I

13.	References.....	9
14.	Acknowledgement.....	10



# 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 ~~press~~ 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 ~~can~~ 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 ~~news~~ are 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 ~~code~~ codes, and the student and employee handbooks. Offenders may be prosecuted under the Georgia Computer Systems Protection Act (O.C.G.A. 16-93) 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 follo

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~~ personnel under their supervision comply with these policies and procedure

### 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.





# Information Resources Acceptable Use



# Information Resources Acceptable Use

## 6.3 Encryption

Encrypting electronic mail or messages shall comply with the following:

Use encryption software and the methods approved by official University resources. Approved methods can be found on the Information Security website.

## 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. 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, hacked material, or other material that may be deemed detrimental to the integrity, image, and mission of the University.

Posting or sending restricted information outside of the University without proper or formal authorization.

Using services available on the Internet, through systems the user does not have an account on, or on systems that have no guest or anonymous account for the service being used.

Posting commercial announcements or advertising matter

Promoting or maintaining a personal or private business.

Using nonwork or nonacademic related applications or software that occupies excess workstation resources.





# Information Resources Acceptable Use

## 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 access University information resources.





# Information Resources Acceptable Use

## 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 Cybersecurity Policy §10.4

<https://www.usg.edu/policymanual/section10/C442/>



# Information Resources Acceptable Use

## 14. Acknowledgement

I have read and understand the Third-Party Access Agreement and if I violate the rules outlined herein, may face legal or disciplinary action according to applicable law and/or university policy.

Name: \_\_\_\_\_ Date: \_\_\_\_\_

Signature: \_\_\_\_\_  
\_\_\_\_\_