

Valdosta State University

Information Security Policy

Date: December 15, 2003

1. PURPOSE	1
2. POLICY	1
2.1 GENERAL USE	2
2.2 POLICY ENFORCEMENT.....	2
3. GENERAL SECURITY CONCEPTS	2
3.1 USER-IDS AND PASSWORDS.....	2
3.2 ANONYMOUS USER-IDS	2
3.3 PHYSICAL SECURITY TO CONTROL INFORMATION ACCESS	3
3.4 INTERNAL NETWORK CONNECTIONS.....	3
3.5 EXTERNAL NETWORK CONNECTIONS.....	3
3.6 NETWORK CHANGES	3
3.7 SECURITY COMPROMISE TOOLS.....	3
3.8 EXTERNAL DISCLOSURE OF SECURITY INFORMATION.....	3
4. PROCEDURES	4
4.1 REPORTING SUSPECTED SECURITY BREACHES.....	4
5. INTERPRETATIONS	4
6. REFERENCES	5
7. APPROVAL	6

1. Purpose

This is a statement of policy regarding the use and administration of Valdosta State University computer and data communication facilities. It relates to the use and administration of data communications equipment (including computer networks involving wireless and traditional LANS, and the Internet) as well as mainframe, midrange, minicomputer, workstation, and personal computer systems. Thus, it covers all activities involving computing and data communication facilities of Valdosta State University. Every user of these systems is expected to know and follow this policy.

2. Policy

This policy applies to any individual using or administering Valdosta State University computer and/or data communication facilities. Not covered are activities solely involving personal property and therefore not connected in any manner to the data communication facilities of Valdosta State University. Related university policies and guidelines that must be respected by such individuals are listed in the references section of this document.

2.1 General Use

Data communication facilities at Valdosta State University have been developed to encourage widespread access and distribution of data and information. Computing systems facilitate manipulation and sharing of data and information. Together, these systems and facilities can be used in similar fashion to mail and telephone services, and so are governed by principles of appropriate use for those services.

University data communication and computing resources are used to support the educational, research, and public service missions of the institution. Activities involving these resources must be in accord with the university honor codes, Employee Handbook, student handbooks, and relevant local, state, federal, and international laws and regulations.

For use and administration to be acceptable, it must demonstrate respect of:

- The rights of others to privacy;
- Intellectual property rights (e.g., as reflected in licenses and copyrights);
- Ownership of data;
- System mechanisms designed to limit access; and
- Individuals' rights to be free of intimidation, harassment, and unwarranted annoyance.

2.2 Policy Enforcement

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. General Security Concepts

3.1 User-IDs and Passwords

Valdosta State University requires that each Student, Faculty, or Staff accessing multi-user information systems have a unique user-ID and a private password. Each user is personally responsible for the usage of his or her user-ID and password and should be aware of the applicable federal and state laws.

3.2 Anonymous User-IDs

With the exception of electronic bulletin boards, Internet web sites, intranet web sites, and other systems where all regular users are intended to be anonymous as approved by the university CIO or his/her designees, users are prohibited from logging into any Valdosta State University system or network anonymously.

3.3 Physical Security to Control Information Access

Access to every office, computer machine room, network closet, and other Valdosta State University work area containing sensitive information must be physically restricted to those people with a need-to-know.

3.4 Internal Network Connections

All Valdosta State University computers that store sensitive information and that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by the Chief Information Officer and the Information Security Taskforce.

3.5 External Network Connections

All in-bound session connections to Valdosta State University computers from external networks must be protected with an approved password access control system. In general terms, Valdosta State University workers must not establish connections with external networks (including Internet Service Providers) unless these connections have been approved by the Chief Information Officer and the Information Security Taskforce.

3.6 Network Changes

Changes to Valdosta State University internal networks include loading new data communications software, changing network addresses, reconfiguring routers, adding dial-up/ dial-in lines, and the like (with the exception of emergency situations) must be: (a) documented in a work order request, and (b) approved in advance by the Information Technology Division. All emergency changes to Valdosta State University networks must only be made by persons who are authorized by the Information Technology Division.

3.7 Security Compromise Tools

Unless specifically authorized by the Chief Information Officer, Valdosta State University workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those which defeat software copy-protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Similarly, without this type of approval, users are prohibited from using "sniffers" or any other hardware or software which monitors the traffic on a network or the activity on a computer.

3.8 External Disclosure of Security Information

Information about security measures for Valdosta State University computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless the permission of the Chief Information Officer or the Information Security Taskforce has first been obtained.

4. Procedures

4.1 Reporting Suspected Security Breaches

Anyone who has reason to suspect a deliberate or significant breach of established security policy or procedure should promptly report it to the appropriate Dean, Director, or Department Head, and who shall report the same information to the Department of Information Technology. If the breach is serious and needs immediate attention, the Valdosta State University Department of Public Safety should be contacted.

5. Interpretations

Any questions regarding the implementation of or the interpretation of this policy should be directed to Valdosta State University's Chief Information Officer or his or her designees.

DRAFT

6. References

Georgia Computer System Protection Act
<http://www.usg.edu/oiit/policy/proact.phtml>

USG Academic Affairs Handbook, Personnel Policies, etc.
<http://www.usg.edu/pubs/other.html>

USG Board of Regents Computer Security Policy Statement
<http://www.usg.edu/oiit/policy/security.phtml>

USG Facilities Guidelines for Instructional Technology
http://www.usg.edu/pubs/pdf/fac_glines_instr_tech.pdf

USG Peachnet Acceptable Use Policy
<http://www.usg.edu/peachnet/about/acceptable.html>

VSU Campus Homeland Security Policy
<http://www.valdosta.edu/legal/chs/>

VSU Email Policy
<http://www.valdosta.edu/it/email/>

VSU Fax Confidentiality and Security Policy:
http://www.valdosta.edu/legal/hipaa/fax_policy.pdf

VSU Information Resources Acceptable Use Policy (this document)
<http://www.valdosta.edu/security/aup.shtml>

VSU Information Security Policy
<http://www.valdosta.edu/security/isp.shtml>

VSU Intellectual Property Policy
<http://www.valdosta.edu/grants/ippolicy.html>

VSU Policy on Confidentiality and Privacy Policy under HIPAA
<http://www.valdosta.edu/legal/hipaa/pocsa.pdf>

VSU Policy Pursuant to the Gramm Leach Bliley Act
<http://www.valdosta.edu/legal/glb/glbairs.pdf>

VSU Records Retention Policy
<http://www.valdosta.edu/records/>

VSU Web Server Usage Policies
<http://www.valdosta.edu/it/web/usage.shtml>

7. Approval

Approved: _____
Dr. Ronald M. Zaccari

Effective: _____
Date

DRAFT