Valdosta State University

Information Security Policy Date: April 30, 2020

1. Purpose

This document and supporting documents represent the policy regarding the use and administration of Valdosta State University computer and data communication resources, including campus wireless and traditional LAN networks, workstations, lab computers, laptops, and mobile devices managed by the University. This policy also covers personal computer systems that are connected to networks managed by the University.

2. Scope

The Valdosta State University Information Security policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems, and networks which use or administer campus computing and/or data communication resources, including hardware, software, or network. Every user of resources provided by Information Security is expected to know and follow this policy. Not covered are activities solely involving personal property and therefore not connected in any manner to the data communication facilities of Valdosta State University.

3. Policy

It is the policy of Valdosta State University to provide computing and data communication facilities to encourage widespread access and distribution of data and information that facilitates accomplishment of the University's mission and strategic goals.

3.1 General Use

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 Code of Conduct, 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.

3.2 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.

4. General Security Concepts

4.1 User-IDs and Passwords

Valdosta State University requires that each student, faculty, or staff member who accesses multiuser information systems have a unique user-ID and a private password. Each authorized individual is personally responsible for the protection and security of his or her user-ID and password and should be aware of the applicable federal and state laws regarding access to authorized systems. Authorized users should not share their private passwords with other individuals or allow other individuals to perform activities on computers under another login.

4.2 Anonymous User-IDs

With the exception of Internet web sites and designated public access computer systems, where all regular users are intended to be anonymous as approved by the University's Chief Information Officer or his/her designees, individuals are prohibited from logging into any Valdosta State University system or network anonymously.

4.3 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.

4.4 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 or his/her designees.

4.5 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 authorized users must not establish connections with external networks (including but not limited to Internet Service Providers, Virtual Private Networks, and external cloud services) unless these connections have been approved by the Chief Information Officer or his/her designees.

4.6 Network Changes

Changes to Valdosta State University internal networks including installation of new data communications software, changing network addresses, reconfiguring networking components, and adding servers (with the exception of emergency situations) must be: (a) documented in a work order request and (b) approved in advance by-designated individuals in the Information Technology Division. Changes to the university’s infrastructure or firewalls must be (a) documented in a change request, and (b) approved in advance by designated individuals in 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.

4.7 Security Compromise Tools

Unless specifically authorized by the Chief Information Officer or his/her designees, Valdosta State University users 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, exfiltrate data, 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.

4.8 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 his/her designees has first been obtained.

4.9 Security Awareness Training

All authorized users of the University computing and data communications resources are required to complete compliance training at prescribed times of the year.

5. Procedures

Incident Response

The University Division of Information Technology manages computing and data communications technologies and monitors their compliance to University policy as well as federal, state, and local jurisdictional laws and statutory regulations. If computing and data communications technologies pose a threat to the remainder of the campus computing network, they may be restricted from network access until the threats no longer exist.

5.1 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, who shall report the same information to the Division of Information Technology’s Chief Information Security Officer. If the breach is serious and needs immediate attention, the Valdosta State University Department of Public Safety should be contacted.

6. 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/her designee.

7. Supporting Documentation

- Georgia Computer System Protection Act (http://ga.elaws.us/law/16-9%7C6)
- VSU Policy on Email, Web, and Portal for Office Communicaitons
- VSU Fax Confidentiality and Security Policy
- VSU Information Resources Acceptable Use Policy
- VSU Intellectual Property Policy
- VSU Policy on Health Insurance Portability and Accountability Act (HIPAA) Notice of Privacy Practices
- VSU Security of Student Information (Gramm-Leach-Bliley Act)

8. Affected Stakeholders

Indicate all entities and persons within the university affected by this policy:

☒Alumni ☒Graduate Students ☒Undergraduate Students

☒Staff ☒Faculty ☒Student Employees

☒Visitors ☒Vendors/Contractors ☐Other:_________________

9. Policy Attributes

Responsible Office(s)	Information Technology, 1410 N. Oak St., 229-245-4357, itvsu@valdosta.edu
Approving Officer or Body	President, President's Office, West Hall Suite 1004, 229-333-5952, president@valdosta.edu
Date Approved	10/26/2004
Last Reviewed	04/30/2020
Next Review Date	04/30/2022