



OLD DOMINION UNIVERSITY

University Policy

Policy #3505

INFORMATION TECHNOLOGY SECURITY POLICY

Responsible Oversight Executive: Executive Vice President for Enrollment, Transformation, and Technology and Chief Strategy and Innovation Officer

Date of Current Revision or Creation: February 2, 2023

A. PURPOSE

The purpose of this policy is to state the codes of practice with which the University aligns its information technology security program and to establish that the University aligns its security activities with internationally recognized best practices.

B. AUTHORITY

[Code of Virginia Section 23.1-1301, as amended](#), grants authority to the Board of Visitors to make rules and policies concerning the institution. Section 7.01(a)(6) of the [Board of Visitors Bylaws](#) grants authority to the President to implement the policies and procedures of the Board relating to University operations.

Restructured Higher Education Financial and Administrative Operations Act, [Code of Virginia Section 23.1-1000 et seq., as amended](#)

C. DEFINITIONS

[Code of Practice for Information Security Management \(ISO/IEC 27002:2013\)](#) - The international standard that defines guidelines and general principles for the effective management of information security within an organization. It is a risk-based framework widely used to guide establishment of security standards and management practices.

[EDUCAUSE Association](#) - A nonprofit association dedicated to the advancement of higher education through the effective use of information technology. Members include representatives from institutions of higher education, higher education technology companies, and other related organizations.

[Family Educational Rights and Privacy Act \(FERPA\)](#) – A Federal law enacted to protect access to student records and provide control over the disclosure of information from these records.

[Gramm-Leach-Bliley Act \(GLBA\)](#) - A Federal law enacted to control how financial institutions deal with the private information of individuals.

[Health Insurance Portability and Accountability Act \(HIPAA\)](#) – A Federal law enacted to set national standards for the security of electronic-protected health information.

[Information Security](#) - The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.

[Information Security Officer \(ISO\)](#) - The Old Dominion University employee, appointed by the President or designee, who is responsible for developing and managing Old Dominion University's information technology (IT) security program.

[Information Technology Security Program](#) – Provides a high-level view of the University's security controls and elements used to satisfy the laws and regulations relevant to information security. The Information Security Officer has delegated authority for the selection and implementation of security controls and manages the overall security program.

[International Electrotechnical Commission \(IEC\)](#) - A global organization that develops and publishes standards addressing electrical, electronic, and related technologies. Membership comes from government, the private sector, consumer groups, professional associations, and others.

[International Organization for Standardization \(ISO\)](#) - The world's largest developer of standards. The organization is made up of representatives from governmental and private sector standard bodies, e.g., the American National Standards Institute.

[Payment Card Industry Data Security Standard](#) - A comprehensive set of payment application security requirements designed to ensure the confidentiality and integrity of customer information.

[Virginia Alliance for Secure Computing and Networking \(VA SCAN\)](#) - An organization formed to help strengthen information technology security programs within Virginia. The Alliance was organized and is operated by security practitioners and researchers from several Virginia higher education institutions.

D. SCOPE

This policy applies to all users, decision makers, developers and planners of campus systems and operations related to the design, acquisition, maintenance, and use of information technology.

E. POLICY STATEMENT

The University's information technology security program is based on nationally and internationally recognized standards and frameworks appropriately tailored to the specific circumstances of the University, including but not limited to those recommended in the [Code of Practice for Information Security Management](#) published by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 27002:2013).

The program also incorporates security requirements of applicable regulations including, but not limited to, the Family Educational Rights and Privacy Act, Payment Card Industry Data Security Standard, Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act. Professional organizations, such as the national EDUCAUSE Association and the Virginia Alliance for Secure Computing and Networking, serve as resources for additional effective security practices.

The ISO/IEC 27002:2013 Code of Practice and other sources noted above are used to guide development and ongoing enhancement of additional information technology security policies as needed.

F. PROCEDURES

The specific standards to be utilized for compliance with this policy are published on the [Information Technology Services Computing Policies and Standards](#) website. For security purposes, procedures and guidelines are maintained internally and are available upon request to relevant parties as authorized by the Information Security Officer.

G. RECORDS RETENTION

Applicable records must be retained and then destroyed in accordance with the [Commonwealth's Records Retention Schedules](#).

H. RESPONSIBLE OFFICER

Chief Information Officer

I. RELATED INFORMATION

[University Policy 4100 – Student Record Policy](#)
[Information Technology Services Computing Policies and Standards](#)

POLICY HISTORY

Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

<u>/s/ Rusty Waterfield</u>	<u>January 4, 2023</u>
Responsible Officer	Date

Policy Review Committee (PRC) Approval to Proceed:

<u>/s/ Donna W. Meeks</u>	<u>August 18, 2022</u>
Chair, Policy Review Committee (PRC)	Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

<u>/s/ Chad A. Reed</u>	<u>January 27, 2023</u>
Responsible Oversight Executive	Date

University Counsel Approval to Proceed:

<u>/s/ Allen T. Wilson</u>	<u>January 31, 2023</u>
University Counsel	Date

Presidential Approval:

<u>/s/ Brian O. Hemphill, Ph.D.</u>	<u>February 2, 2023</u>
President	Date

Policy Revision Dates: October 1, 2007; April 9, 2010; April 26, 2011; March 15, 2017;
February 2, 2023

Scheduled Review Date: February 2, 2028