OLD DOMINION UNIVERSITY

Information Security Program

Contents

Introduction

The purpose of this document is to provide an overview of the information security program at Old Dominion University, including the policies and standards that form the foundation of the program (http://www.odu.edu/about/policiesandprocedures/computing). Policies and standards inform the practices taken to protect electronic resources that fall under federal and state laws and regulations such as the Family Education Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry, Data Security Standard (PCI-DSS).

The intent of the program is to provide effective security that aligns with and enables open and collaborative computing environments and business administration in support of instruction, research, and other scholarly activities that fulfill the mission of Old Dominion University. The program is intended to assess and manage risks to the University's electronic assets and to reduce risks in alignment with other enterprise risks that are being managed by the University. The program is intended to protect the confidentiality, integrity, and availability of electronic resources and is not intended to prevent, prohibit, or inhibit the sanctioned use of information technology resources as required to meet Old Dominion University's mission and academic and administrative goals. The program establishes principles for initiating, implementing, maintaining, and improving information security for Old Dominion University.

It is the collective responsibility of all users to ensure:

- Confidentiality of information which ODU must protect from unauthorized access
- Integrity and availability of information stored on or processed by ODU information systems
- Compliance with applicable laws, regulations and ODU policies governing information security and privacy protection

Consistent with Old Dominion University's Memorandum of Understanding granting Level II delegated authority from the Commonwealth under the Virginia Restructured Higher Education Financial and Administrative Operations Act of 2005 and in keeping with ODU Policy 3505 – Information Technology Security Policy, ODU exercises independent authority for establishing and executing its information security program.

Scope

The program applies to all users, electronic information assets, facilities hosting those assets, applications, systems, and network resources. Affiliated organizations, or any entity, including third parties, using Old Dominion University information technology resources must operate those assets in conformity with the Old Dominion Information Security Program, unless otherwise formally exempted by the President or his designee.

Information Security Policy

Policy is developed and executed, and expectations are set for protecting University information assets. These are supported by related standards and guidelines to facilitate development of procedures across the campus that promote information security and compliance:

- Industry Cyber Security Frameworks or Standards provide best practices, often based on collaboration between industry, academia and government, to identify voluntary practices to manage cyber security risks. The National Institue for Standards and Technology (NIST) Cyber Security Framework (CSF) describes their effort to produce "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."
- ODU Policies are high-level statements of principle that establish authority to operate and that provide technology direction to the campus community.
- ITS Standards establish more specific criteria and minimum baseline requirements or levels that must be met to comply with policy. They provide a basis for verifying compliance through audits and assessments.
- Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists.
- Procedures are maintained by operational units to describe and document established activity for specific operations. Procedures should be consistent with ITS Standards.

Policy development and maintenance is described in ODU Policy 1001 – Development, Approval and Maintenance of University Policy. Information Technology policy is driven by Board of Visitors and ODU policies and directives, legislation and regulations, audit findings, risk assessment and University strategic planning and initiatives. Key campus stakeholders are consulted early and research is conducted to find potential models from other similar universities.

As the designated senior Information Technology official at ODU, the Chief Information Officer (CIO) formally proposes University-wide policies, standards and guidelines. Under the broad authority provided by the University Policies, the CIO establishes specific requirements for all members of the university community. The formulation and distribution of information technology policies, standards, and guidelines connect the university's expectations to individual conduct, institutionalize expectations, support compliance with laws and regulation, mitigate institutional risk, and enhance productivity and efficiency in the university's operations.

Information Technology related policies are in place as follows:

- Policy 3500 – Policy on the Use of Computing Resources
- Policy 3501 – Information Technology Access Control Policy
- Policy 3502 – Information Technology Infrastructure, Architecture, and Ongoing Operations

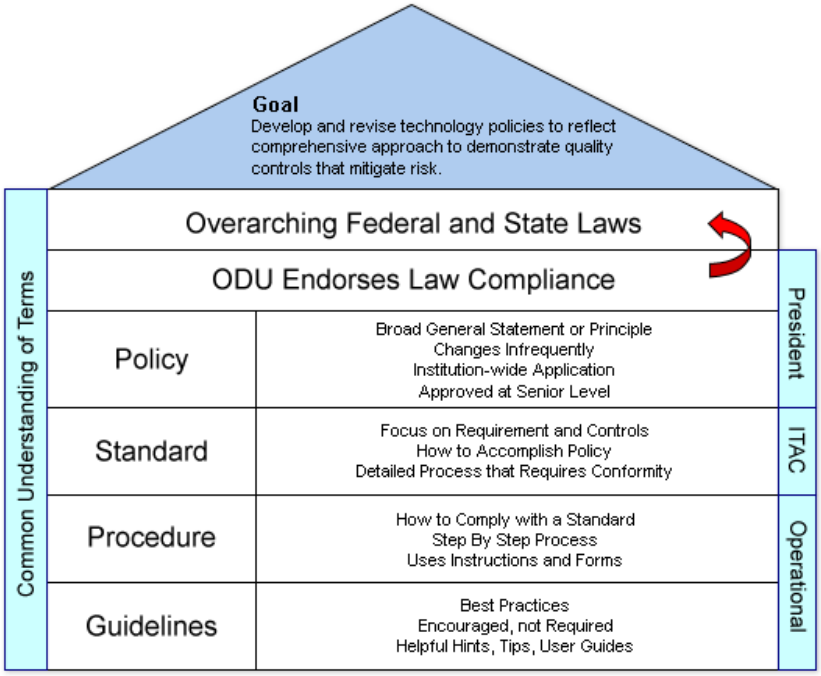
- Policy 3504 – Data Classification Policy
- Policy 3505 – Information Technology Security Policy
- Policy 3506 - Electronic Messaging Policy for Official UniversityCommunication
- Policy 3507 - Information Technology Accessibility Policy
- Policy 3508 - Information Technology Project ManagementPolicy
- Policy 3509 - Software Decision Analysis Policy

Security Policy Management

In collaboration with appropriate University representatives, the Information Security Officer (ISO) leads efforts to develop, approve, and publish a suite of information security policies and standards, based upon the industry's best practices in information security. These policies, standards, and guidelines formally establish the University's Information Security Program and set forth employee responsibility for protection of ODU electronic assets.

The information security policy also incorporates information security requirements of applicable regulations including, but not limit to FERPA, PCI-DSS, and HIPAA. Professional organizations, such as the national EDUCAUSE Association, Internet-2, and the Virginia Alliance for Secure Computing and Networking (VASCAN), serve as resources for enhancing information security practices.

The graphic below illustrates the governance of the policy development and approval structure.



A complete list of information security polices, standards and guidelines can be found on the Information Technology Services website. ITS Standards development and maintenance is described in ITS Standard 01.1.0 Technology Policy Development and Maintenance Standard.

Information Security Organization and Governance

Information security cannot be treated solely as a technology issue. Based on the institution's growing dependence on information technology and information technology-based controls, information security risks increasingly contribute to institutional legal, financial, and reputational risks. Information security is an intrinsic part of governance and consists of the leadership, organizational structures, and processes that safeguard Old Dominion University's information, its operations, its market position, and its reputation.

Board Authority

The Code of Virginia Section 23.1-1301, as amended, grants authority to the Old Dominion University Board of Visitors to establish rules and regulations for the institution. Section 6.01(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. Virginia Code Section 23-38.88, as amended, allows public institutions of higher education the opportunity for specific structured financial and administrative operational authority, including the management and use of computing and telecommunications resources and services.

CIO Authority

The University President gives the CIO responsibility for university policies and procedures for acquisition, implementation, documentation and use of information technology resources and for meeting its compliance obligations. Information Technology Services (ITS) also provides and manages a variety of computing facilities and services for the university. The CIO reports to the Vice President of Administration and Finance. The President delegates specific responsibilities to the Information Technology Advisory Committee (ITAC), a body appointed by the University to represent various campus constituencies. Information Security audits are the responsibility of Old Dominion University's Internal Audit Department and the Commonwealth of Virginia's Auditor of Public Accounts.

Information Security Officer

Information security responsibilities for the University are assigned to the President of Old Dominion University as Agency head. The President designates the Information Security Officer (ISO) responsibility to develop and manage Old Dominion University's IT security program and to coordinate and provide information security updates to the CIO. The ISO oversees an annual review of the information security program and communicates the review outcomes to the CIO and to appropriate stakeholders. The ISO reports to the President on the current state of campus information security relative to protecting university information assets as needed.

Roles and Responsibilities

Information security roles are defined in Standard 1.2.0, Information Technology Roles and Responsibilities. As Agency Head, the President is designated as the responsible individual for the security of Old Dominion's IT systems and data. The President designates the ISO to develop, implement, and maintain a program of information security safeguards.

The responsibilities of the ISO and other positions with security duties are described in Standard 1.2.0, Information Technology Roles and Responsibilities. Personnel identified perform their assigned responsibilities in support of the Information Security Program.

Technical support staff and individual users are expected to follow established standards and practices and to report potential security risks or violations. Administrators across the university are responsible for ensuring information security policies, standards and practices are followed by employees in their respective areas.

Privacy of Personal Information

All users of information technology resources are advised of the open nature of information disseminated electronically, and must not assume privacy or restricted access to information they create or store on campus systems. Old Dominion University is a public university and information stored on campus information systems may be subject to disclosure under state law. The University will disclose information about individuals to comply with applicable laws or regulations, to comply with or enforce applicable policy, to ensure the confidentiality, integrity, or availability of campus information, and to respond to valid legal requests or demands for access to campus information. Information collected by the University and the ways the University use the information are described in ITS Standard 02.1.0 Internet Privacy Standard.

Security Awareness and Training

The focus of security awareness at Old Dominion University is to create an attitude and culture toward good security practices and facilitating a climate that sees information security practices as beneficial to the protection of the University and our students and staff. Awareness program guidelines are published within ITS Standard 03.1.0 Security Awareness Program Guidelines. Users must formally acknowledge their responsibilities through the acceptance of a statement on the terms of use of information technology resources. These Terms of Use are outlined in ITS Standard 09.1.0 Acceptable Use Standard. Training is required on an annual basis.

In addition to annual training, security awareness information is provided to new employees and new students at the time of orientation. Online resources are provided to educate users on best computing practices and the importance of reporting security incidents. Security tools are provided at no charge. News of email scams, phishing attempts and other malicious actions are posted to inform users of possible threats.

Identity Management

Old Dominion University maintains a diverse technical environment with many services which require unique identifying credentials in order to gain access and authorization. These credentials are managed as

much as possible though central identity management systems. As part of a long-range goal to streamline access to computing resources at Old Dominion University, ITS developed MIDAS (**M**onarch **ID**entification and **A**uthorization **S**ystem).

MIDAS allows users to have one account ID and password for accessing multiple computing resources at the University. For many systems, this allows access to computing resources that are authorized on the basis of roles (faculty, staff, or student). This system continues to be developed with fundamental security principles in mind. The MIDAS system and account administration are guided by ITS Standards 04.1.0 MIDAS Identity Management Standard and 04.2.0 Account Management Standard.

User access to IT systems is based on the principle of least privilege. Proper authorization and approval are required for access. The Standard 4.2.0, Account Management identifies practices used in requesting, granting, administering and terminating account access.

Incident Management

Old Dominion University's Data and System Breach Response Framework is documented in Annex B, Incident Annex 5 of the University Crisis and Emergency Management Plan. The Data and System Breach Response Framework involves preparation for incidents and management response when there is suspected loss of University data or critical systems. The process for responding to security incident is designated in Standard 5.1.0, IT Security Incident Handling. Security incidents are managed by the Information Security Team who ensures that security incidents are promptly investigated, documented, reported appropriately, resolved in a manner that restores operation quickly and, if required, maintains evidence for further disciplinary, legal, or law enforcement actions. The incident response program is reviewed annually and modified as needed to comply with applicable laws and university policies and standards.

Preparation for potential incidents includes conducting System Inventories and Risk Assessments for sensitive systems, system security planning, management practices for desktops, servers, networks and projects, system hardening and data protection measures. Detection, analysis, containment, recovery and review include several mechanisms such as malware protection, intrusion detection, monitoring, logging and incident handling protocols. Standards and procedures are in place to support these efforts.

Operational Security

To ensure the secure operation of information technology facilities and resources, system activities must be managed consistently and under a set of principles and controls.

Physical Security

Physical areas where information assets contain protected data are protected from unauthorized physical access. Many IT assets are located in public and non-public access areas and must be physically secured to prevent theft, tampering, or damage. ITS Standard 6.1.0, Information Technology Facilities Security establishes requirements for safeguarding the facilities that house equipment, systems, services and personnel. Controls also include environmental essentials, monitoring and auditing, and periodic reviews. Management conducts reviews and documents physical access rights to campus limited-access areas on a routine basis.

Access Control

Access to information technology resources is controlled on the basis of business need and security requirements. Network access control lists enforce specific security and business requirements. Access management, user registration and termination, and privilege management govern the allocation of rights. Sets of controls are in place that restricts access through technical structures and authentication methods. Passwords are managed through a formal process and secure log-on procedures.

Sensitive systems are explicitly identified and receive special handling. Network access and routing controls are applied for users and equipment. Appropriate authentication controls are used for external connections and remote users. Physical and logical access to diagnostic and configuration portals and utility programs are controlled. Duties are separated to protect systems and data. Access rights are audited at regular intervals.

Systems Security

System Security is maintained over the lifetime of systems through a series of standards intended to protect Old Dominion University resources from project initiation through implementation and maintenance of the system, and upon retirement and disposal of the system. Project management standards specify risk-based project classification. System planning includes a Risk Assessment standard to be followed prior to placing a system into production status. Pre-implementation practices are specified in system scanning standards. Implementation practices are specified by a change management standard which outlines planning, communicating, testing, planning a back-out strategy, gaining approval and executing the change in a controlled manner.

System Configuration Management is outlined via several system management standards including, Standard 06.5.0, Server Management, Standard 06.12.0, Network Management and Standard 06.13.0, Desktop Management. Overall system security during the production lifetime is maintained via operational

security standards including malicious code protection, access controls standards, data protection standards, facility security standards, personnel security standards and IT System Security standards. Data disposal is specified in an IT Asset Control standard.

Personnel Security

In addition to defining security roles and responsibilities, personnel security is addressed through pre-employment screenings, adequate position descriptions, terms of employment, and security education and training. The Standards of Conduct and Code of Ethics express responsibilities regarding confidentiality, data protection, ethics, and appropriate use of facilities, materials and equipment. Third party users are made aware of their responsibility to comply with relevant laws, regulations and University expectations. Contractual arrangements further reflect the University's security policies.

Contingency Planning

Contingency planning is conducted to minimize the impact and loss of information assets in the event of a disaster. Business continuity plans are developed in accordance with Standard 07.1.0, Business Impact Analysis to understand risks and to identify and prioritize critical business processes.

Based on the results of the analysis, a risk assessment is performed to evaluate the probability and impact and to consider the consequences to information security. An overall strategy is developed for crisis management, recovery and restoration. Plans are formalized with agreements as to the required levels of operation, the time frames, and the implementation strategy. Continuity plans are tested regularly to ensure that they are up to date and effective.

Security Assessments and Reviews

Risk Management

Identifying and prioritizing risks form the basis for determining appropriate actions to take. Risk assessment involves evaluating risks and their likelihood along with selecting and implementing controls to reduce risks to an acceptable level. Each risk assessment documents major findings and risk mitigation recommendations. No set of controls can achieve complete security so assessments are completed as needed to evaluate the effectiveness of the controls but not less than every three years.

Regular assessments are performed using multiple layers of assessments. System Owners and Data Owners conduct Risk Management reviews in accordance with Standard 8.1.0, Risk Management. Security configurations are reviewed annually and reapplied when systems undergo material modifications.

Management's approach to information security is reviewed on a regular schedule and as necessary to ensure continuing appropriateness, adequacy and effectiveness. By Standard 8.2.0, Security Program Review, the IT Security Program is reviewed and evaluated by the ISO and the security team regularly to

discuss specific incidents and to identify areas of concern. Additionally, the team meets at planned intervals or if significant changes occur to assess opportunities for improvement or to manage security threats or other conditions. Standard 8.1.0, Risk Assessment Standard ensures a review of controls and how controls provide adequate mitigation to identified risks. Security plans are completed by the System Owner. The plans are reviewed by the ISO or designee for approval. The institutional oversight committee, Information Technology Advisory Committee (ITAC) , reviews new standards or notable changes to standards and provides input to the security plan in this way.

Board of Visitors Policy 1610, Charter of the Internal Audit Department summarizes the department's objectives to evaluate and improve the effectiveness of risk management, control and governance processes. One of the key objectives of Internal Audit is "evaluating the accuracy, security, effectiveness and efficiency of the University's information technology and processing systems." The Internal Audit Director meets quarterly in executive session with the Audit Committee of the Board of Visitors to report audit findings. In addition, the Auditor of Public Accounts for the Commonwealth of Virginia and other external auditors that have business with the University perform external reviews.

Annual Security Plan

The Information Security Officer submits a comprehensive review of the Security Program annually to the CIO in compliance with the Standard 08.2.0, Security Program Review. This review includes a summary of reviews and assessments during the previous year along with recommendations for addressing identified vulnerabilities.

Compliance

Old Dominion University's information security practices must comply with a variety of federal and state laws, and institutional policies designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information, personal financial information, medical information, and confidential student information.

There are many individual laws, regulations, and policies that establish our information security requirements. Some of the most notable include:

- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health insurance Privacy and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Privacy Act of 1974
- Sarbanes-Oxley Act of 2002
- Virginia Computer Crime Act

Additional laws and regulations specify the disclosure of employee and student information and require the University to take specific actions in the event the institution suspects protected information may have been disclosed either accidentally or maliciously to unauthorized parties. The process of identifying the triggering factors and the resulting notification responses are outlines in Standard 05.2.0 Data Breach Notification.

Policy Enforcement

The Information Security Officer or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate University officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Allegations against employees that are sustained may result in disciplinary action. Such actions will be handled as noted in Standard 10.1.0 Disciplinary Action. Student infractions will be coordinated with the Office of Student Conduct and Academic Integrity using established policies and practices. Third party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to the University. Non-compliance may result in personal, criminal, civil, or other administrative liability.

Old Dominion University reserves the right to temporarily or permanently suspend, block, or restrict access to campus information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of ODU information assets; to protect ODU from liability; or to enforce this policy and its related standards and practices.