OLD DOMINION UNIVERSITY
University Policy

Policy #3504
DATA CLASSIFICATION POLICY

Responsible Oversight Executive: Vice President for Administration and Finance
Date of Current Revision or Creation: April 26, 2011

A. PURPOSE

The purpose of this policy is to establish a uniform data classification framework to assist data owners in determining the level of data security that must be implemented to secure the information for which they are responsible.

B. AUTHORITY

Virginia Code Section 23-9.2:3, as amended, grants authority to the 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.

Restructured Higher Education Financial and Administrative Operations Act, Virginia Code Section § 23-38.88, as amended

C. DEFINITIONS

Data Classification - In the context of information security, it is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization**.**

Data Owners **- I**ndividuals responsible for decisions about the usage of University data.

Data Users - Individuals who access University data in order to perform their assigned duties or to fulfill their role in the University community.

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 Resources – Include, but are not limited to, computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services.

Security Administrators **- I**ndividuals who ensure that appropriate controls, mechanisms, and processes are in place to meet the security requirements necessary to protect an information technology resource.

University Data - All data or information owned, used, created or maintained by the University whether individually controlled or shared, stand-alone or networked.

D. SCOPE

This policy applies to all users of Old Dominion University information technology resources and governs all information technology resources either owned by or operated for University business through contractual arrangements. Users may include employees, students, volunteers, employees of affiliated organizations, and visitors to the institution. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University. Students include all persons attending classes whether enrolled or not enrolled. Affiliated organizations are separate entities that exist for the benefit of the University and include the Foundations, the Community Development Corporation, and the Alumni Association. Visitors include vendors and their employees, parents of students, volunteers, guests, uninvited guests and all other persons located on property owned, leased, or otherwise controlled by the University.

This policy refers to all data owned, used, created or maintained by the University whether individually controlled or shared, stand-alone or networked. It applies to all data sources found on equipment owned, leased, operated or contracted.

E. POLICY STATEMENT

The security of University information and the infrastructure upon which it is processed, transmitted or stored is patterned after accepted standards for management of information security, such as ISO/IEC 17799, Information Technology - Code of Practice for Information Security Management, and industry best practices.

Classifications and associated protective controls for information take into account academic and business needs for sharing or restricting information and the impacts associated with such needs. Data classification impacts other security decisions on system security plans, risk assessments, locations regarding data storage, authorization and access requirements, and continuity of operations and disaster recovery planning.

The Office of Computing and Communications Services (OCCS) provides guidance to enable users to understand their particular custodial roles and responsibilities with respect to information. OCCS implements the technical infrastructure that allows University employees to effectively exercise these custodial roles.

Every user has a responsibility toward the protection of University data; some offices and individuals have very specific responsibilities. Data owners, in particular, determine the level of data security and classification that must be implemented. As described below, data owners, data users and security administrators have distinct roles and associated responsibilities under this policy.

1. Data Custodial Roles and Responsibilities

   a. Data owners are responsible for:
      - knowing and understanding the data for which they are responsible;
      - evaluating and ensuring the data have been appropriately classified based on State and Federal law, regulatory agency requirements and/or any contractual obligations, and University policies;
      - establishing access and utilization criteria;
      - exercising due care in setting standards for protection of data;
      - monitoring compliance and enforcing policy; and
      - implementing practices to assure data accuracy.

   b. Data users are responsible for:
      - protecting their access privileges;
      - proper use of the University data they access;
      - following policy and information access procedures established by data owners;
      - accessing only the information for which they are authorized;
      - reporting suspected or actual violations of policies; and
      - exercising due care in the use of data.

   c. Security administrators are responsible for:
      - executing access authorizations or data transfers authorized by the data owner;
      - using best practices to maintain the confidentiality, integrity, and availability of information;
      - providing a mechanism for monitoring compliance and enforcing policy; and
      - exercising due care in the administration of systems hosting the data.

   The examples provided in this policy are illustrative only. Nothing in this policy is intended to identify a restriction on the right of data owners to require policies and/or procedures in addition to the ones identified in this document.

2. Data Classification Levels

   The data classification levels are listed in order from the most secure to the least secure:

   a. Highly Confidential

      Highly confidential information requires special precautions to ensure the integrity and confidentiality of the information in its storage, usage, and transmittal. This information must be protected from unauthorized modification or retrieval and is not generally disclosed. Highly confidential information may be used with third parties when safeguards and countermeasures are in place to protect that information. Unauthorized disclosure of highly confidential information can adversely and/or seriously affect the University as a whole or in part.

      Examples of highly confidential data include, but are not limited to,
      - Student records
      - Legally protected data
      - President's working papers or correspondence
      - Privileged attorney-client data
      - Access control data

b. Protected

Protected data includes both confidential information for use only by select individuals or systems within the University and private data used by the University that is specific to an individual. Confidential data are distributed on a need-to-know basis between members of the University staff, its systems, and specific third parties where appropriate, and unauthorized disclosure can adversely affect the University as a whole or in part. Private data may only be disclosed to a third party with the permission of affected individuals. Unauthorized disclosure of private information can adversely affect individuals associated with the University, but may not necessarily affect the University as an entity.

Examples of confidential data may include, but are not limited to,

- Non-public contracts
- Donor information
- Information exempt from disclosure under the Virginia Freedom of Information Act

Examples of private data include, but are not limited to:

- Appointment schedules
- Performance reviews

c. Public

Public information is, by its very nature, designed to be used by anonymous persons or systems that may have an interest with the University. Public information is routinely disclosed and made freely available. Further, the University also depends on data exchange with certain outside third party organizations, and the University must make sure that information is exchanged according to this policy based on the information classification level.

Examples of public data include, but are not limited to,

- Press releases
- Directory information classified as such by the University under FERPA
- Schedule of classes

Violations of this policy should be reported to the University's Information Security Officer (ISO). The ISO role is assigned to the Assistant Director for Information Security and Operations in the Office of Computing and Communications Services. Any faculty, staff or student found to have violated this policy may be subject to the appropriate disciplinary action.

F. PROCEDURES

For security purposes, some procedures related to data classification are maintained internally. Procedures are available upon request to relevant parties, notably data owners responsible for major systems, such as the Registrar, the Controller, and Institutional Research and Assessment, as authorized by the Office of Computing and Communications Services.

Other data owners are directed to the Data Classification Procedure for further assistance.

Data owners and users are provided additional guidance in Best Practices in Protecting University Data.

G. RESPONSIBLE OFFICER

Assistant Vice President for Computing and Communications Services

H. RELATED INFORMATION

Board of Visitors Policy 1424, Policy on Intellectual Property
University Policy 3500 - Use of Computing Resources
University Policy 3501 - IT Access Control Policy
University Policy 3505 - Information Technology Security Policy
University Policy 4100 – Student Record Policy
OCCS Standard 02.2.2 - IT Security Roles and Responsibilities
OCCS Standard 08.2.2 - Access Determination and Control
OCCS Standard 09.2.2 - Threat Detection
OCCS Standard 09.3.2 - Security Monitoring and Logging
OCCS Standard 09.4.2 - IT Security Incident Handling
OCCS Standard 09.5.2 - Data Breach Notification
OCCS Standard 10.2.1 - IT Asset Control
Data Classification Procedure
Guideline: Best Practices in Protecting University Data
OCCS System Inventory Index
Office of Research Volunteer or Visiting Scholar Agreement

POLICY HISTORY
****

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

/s/ Rusty Waterfield — February 7, 2011
Responsible Officer Signature — Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna W. Meeks — December 14, 2010
Policy Review Committee (PRC), Chair Signature — Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Robert L. Fenning — April 19, 2011
Responsible Oversight Executive Signature — Date

University Counsel Approval to Proceed:

/s/ Patrick B. Kelly — April 22, 2011
University Counsel — Date

Presidential Approval:

/s/ John R. Broderick — April 26, 2011
President — Date

Policy Revision Dates: October 1, 2007; April 26, 2011

Scheduled Review Date: April 25, 2016