

**Old Dominion University  
Technology Policies, Standards, Procedures and Guidelines**

**Data Classification Policy**

**Title:** Data Classification Standard  
**Reference Number:** Policy 3504

**Purpose**

The purpose of this compliance standard is to provide the University community with a clear understanding of the ethical and proper use of data contained within University systems. This policy outlines the proper use and classification of information assets on University systems.

**Data Classification**

Data classification is assigned to protect data. Any user or automated system interacting with a University operated or sponsored computer resource must comply with the defined data classification levels. A data classification level is assigned to all information that is maintained, stored, or produced by University systems.

Data Owners will perform an annual assessment of the information contained in their systems and will classify that information according to the classification levels defined in this policy.

Security Administrators will take appropriate steps on the information system to safeguard the information according to its classification level.

The Information Classification levels are (from highest to lowest):

- Trade Secret
- Sensitive
- Private
- Confidential
- Public

**Trade Secret**

A trade secret represents the highest level of Intellectual Property (IP) that the University maintains. If trade secret information is disclosed, it may harm the competitive edge of the University, or may otherwise significantly hamper the University's ability to function.

**Sensitive**

Sensitive 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. Sensitive information may be used with third parties when safeguards and countermeasures are in place to protect that information. Unauthorized disclosure of Sensitive information can adversely and/or seriously affect the University as a whole or in part.

**Private**

Private information is information that is specific to a person that is used by the University. Unauthorized disclosure of private information can adversely affect persons associated with the University, although it may not necessarily affect the University as an entity. Permission must be obtained from the person in order to disclose private information to a third party.

**Confidential**

Confidential information is for use only to select persons or systems within the University, and is distributed on a need to know basis between members of the University staff, its systems, and

## Old Dominion University Technology Policies, Standards, Procedures and Guidelines

specific third parties where appropriate. Confidential information, by its very nature, is except from disclosure under the Freedom of Information Act. Unauthorized disclosure of confidential information can adversely affect the University as a whole or in part.

### Public

Public information is, by its very nature, designed to be used by anonymous persons or systems which 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.

Violations of this policy should be reported to the OCCS Security Group.

### Definitions

**Data Owner** is the individual responsible for the practice decisions of data. Data Owner is also referred to as Data Steward, Business Owner or Executive Sponsor.

An **Information Asset** represents individual data elements, data lists, addresses, documents, measurement samples, programs, program source code, recorded ideas, aggregations of data, and other intellectual property produced by members of the University.

**Information Technology Resources** are defined as computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services.

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

**User** includes anyone who accesses and uses the Old Dominion University information technology resources.

### Policy References

ODU faculty, staff and students are bound by all applicable laws, policies, standards and procedures and guidelines. For reference, some frequently referenced documents are noted. This is a non-inclusive list and not intended to limit applicability of any other law or policy.

|                                     |  |
|-------------------------------------|--|
| <p>Ⓢ Policy Foundation:</p>         | <p>Federal and State Law, including but not limited to,</p> <ul style="list-style-type: none"> <li>▪ Freedom of Information Act.</li> <li>▪ Computer Crimes Act.</li> <li>▪ Federal rules of evidence, Sec 802 and Sec 1120</li> <li>▪ Grahm-Leach-Bailey</li> <li>▪ HIPPA</li> <li>▪ FERPA</li> </ul> |
| <p>📖 Related Standards:</p>         | <p>Policy 3500 Use of Computing Resources<br/>Policy 3501 Access to Computing Resources<br/>Policy 3510 Compliance</p>   |
| <p>📄 Related Procedures, Forms:</p> | <p>Data Classification Procedures</p>  |

**Old Dominion University**  
**Technology Policies, Standards, Procedures and Guidelines**

|                             |   |
|-----------------------------|---|
| ① Related Guidelines:       | ISO Reference 70.02.10<br>Commonwealth Security Policy  |
| ✂ Maintenance:              | Office of Computing and Communications Services   |
| ✓ Effective Date:           | Reviewed on an annual basis   |
| ✓ Approved by:              | Rusty Waterfield<br>Acting Assistant Vice President, Office of Computing and<br>Communications Services |
| ✓ Approved: January, 2006   | University Advisory Council on Technology<br><input checked="" type="checkbox"/> Required for Standard  |
| ✓ Approved: October 1, 2007 | Rosanne Runte, President<br><input checked="" type="checkbox"/> Required for Policy                     |