Office of Computing and Communications Services

The purpose of an Information Technology Standard is to specify requirements for compliance with Old Dominion University Information Technology policies, other University policies, as well as applicable laws and regulations. Standards may include business principles, best practices, technical standards, migration and implementation strategies, that direct the design, deployment and management of information technology.

Information Technology Standard: Acceptable Use Standard
Reference Number: 09.1.0
Date of Current Revision or Creation: December 2012

A. PURPOSE

The purpose of a compliance standard is to provide the University community with a clear understanding of the terms and conditions under which access to any Old Dominion University information technology resource is granted.

B. DEFINITIONS

Account holders are users who have been granted computer account permissions to access and use Old Dominion University information technology resources.

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.

C. STANDARDS STATEMENT

Acceptable Usage Statement
The Acceptable Use Statement is included in the application that account holders complete prior to receiving rights to an account.

Account holders are granted access to computing, networks, telecommunications and electronically stored information contingent upon their prudent and responsible use. Access is granted to the individual only. Individuals are not authorized to transfer or share access with another. This Acceptable Use Statement applies to all current and future accounts and access to University IT resources. The acceptance of the Acceptable Use Statement is logged.
**Terms of Use**
Account holders acknowledge understanding of the terms of use and consent to the following:

In any investigation of misuse, the University may inspect, without prior notice, the contents of files, voice mail, logs, and any related computer-generated or stored material, such as document output.

Computer files may be inspected occasionally by systems personnel when assuring system integrity or performing related resource management duties.

Users will comply with the institution’s policies and procedures regarding information technology and telecommunication resources.

ODU reserves the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on ODU systems.

**Account Holder Responsibilities**
Account holders are responsible for the following in the use and security of all accounts.

An account is to be used only by the designated user. The designated user is solely responsible for all work done in that account.

Each account may be used only for the expressed purpose of supporting the University’s mission.

Users are responsible for protecting their passwords. Users must take precautions and practice secure password management.

Any user feeling pressured to reveal a password or suspect that their account has been compromised should contact the IT Security Team. Non-reported cases of unauthorized access may be classified as intentional and subject to enforcement procedures.

Users are responsible for locking or logging out of any device. The account holder may be responsible if someone uses that account to make an unauthorized act.

**Unacceptable Behavior**
The following actions are considered unacceptable behavior.

Account holders may not use information or resources for any illegal or unauthorized purpose or act to violate Federal, State or local laws or University policies.

Account holders may not participate in any malicious behavior that harms or interfere with others’ use of resources.
Account holders may not use resources or information for commercial purposes without prior authorization.

Account holders may not disrupt network services or tamper with software protections or restrictions.

Account holders may not use copyrighted and licensed materials on ODU systems unless the ODU owns the materials or ODU has otherwise complied with intellectual property laws governing the materials.

Account holders may not transmit unencrypted sensitive data over the Internet.

**Enforcement**

Misuse of computing, networking, and information resources may result in severe consequences, including the loss of access to information technology resources.

**Account Termination**

IT management has the responsibility to maintain accurate access privileges to information technology resources.

Access privileges will be terminated for employees transferring departments or leaving University employment.

Student accounts are deactivated in accordance with student enrollment status.

**D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION**

Federal and State Law
Policy 3500 - Use of Computing Resources
Policy 3501 - IT Access Control Policy
IT Standard 4.2.0 - Account Management Standard
IT Standard 10.1.0 - Disciplinary Action
Security Awareness Training

**E. HISTORY**

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2008</td>
<td>ITAC/CIO</td>
<td>Created</td>
</tr>
<tr>
<td>October 2009</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2010</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2011</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2012</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>December 2012</td>
<td>IT Policy Office</td>
<td>Minor rewording for clarity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Numbering revision</td>
</tr>
</tbody>
</table>