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.

<table>
<thead>
<tr>
<th>Information Technology Standard:</th>
<th>Mobile Device Management Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Number:</td>
<td>02.8.0</td>
</tr>
<tr>
<td>Date of Current Revision or Creation:</td>
<td>April 2013</td>
</tr>
</tbody>
</table>

A. PURPOSE

The purpose of this compliance standard is to establish the rules for the secure, reliable and accountable use of all mobile computing devices.

B. 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.

Highly Confidential data 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. 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.

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** – IT 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.

**Jailbreak** is to gain the ability to modify protected system files. It is also referred to as rooting or unlocking.

**Mobile Computing and Storage Devices** are defined as portable devices intended primarily for the access to or processing of data and/or to provide persistent storage. New products with these characteristics appear on the market frequently. Examples include, but are not limited to, the following types of products: laptop, notebook, tablet, smartphones, PDAs, etc. magnetic storage drives, optical storage drives, compact discs, digital versatile discs, wireless network cards, memory cards, USB drives, cell phones, music players, smart watches, etc.

**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. Examples of confidential data may include, but are not limited to, Non-public contracts, donor information, and 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.

**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.

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

**C. STANDARDS STATEMENT**

Old Dominion University allows the use of mobile computing devices and storage devices, including University-owned devices, University-owned but personally managed devices, and personally-owned devices, to access IT resources as long as the devices are compliant to IT security standards and guidelines.

Accesses to all IT resources, including those available for use by mobile devices, are granted through an Account Management process. Authorized users formally consent to the terms and conditions of use through the acknowledgment of the University’s **Acceptable Use Standard**.
Device Security

User Requirements:
Users must label devices with contact information to make the device easy to return if lost.

Users must configure a PIN or passcode to gain access to the device.

Users must set an idle timeout that will automatically lock the phone after a period of time.

Users must keep all software, including the operating system and applications, up to date.

Users should enroll the device in “Find My iPhone” or similar service to help locate the device if misplaced if capable.

Users must not “jailbreak” or “root” the device.

Users must be responsible for the secure and appropriate back up of software and data on the device.

Data Security and Storage

User Requirements:
Users must accept and protect University data under their control.

Users must take appropriate steps to secure any University data they create, possess, or access.

Users must carefully review the files stored on the device to ensure that no restricted information is stored.

Users must, regardless of the device’s ownership, access or store University Data through devices that do not meet University IT requirements.

Incident Reporting

User Requirements:
Users must participation in required security awareness training programs provided by the University.

Users must immediately report lost or stolen devices to the Technical Support Center or by submission of the online Computer Incident Reporting Form.

University Data
User Requirements:
Users with access to data classified as Highly Confidential or Protected data as outlined in University Policy 3504 are required to adhere to additional standards in the use, management, and storage of University data. Public data does not have restrictions.

Highly Confidential or Protected data stored on mobile devices must be encrypted using approved encryption techniques, the University’s Virtual Private Network connection, and/or wireless transmission protocols.

Users must carefully review the files stored on the device to ensure that there is no restricted information and delete the protected information as soon as it is no longer needed.

Users must accept and understand that University reserves the right to wipe some or all data from a mobile device in the event of employment separation or termination and/or the lost or replacement of a mobile device.

Users must accept and understand that mobile devices are subject to open records requests or audit processes. In such cases, the user must provide full access to a mobile device.

Users must accept, understand and surrender a mobile device to the University if used in a data preservation or other legal matter.

Technical Support
The University does not assume any liability or responsibility for technical support for a user’s personally-owned computing device.

Due to the quantity, complexity and diversity of computer hardware and software combinations, limited assistance is available for personally-owned devices. The IT department will provide recommendations, guidance and advice as time permits. Priority support will be provided to University-owned devices.

Enforcement
Users who do not comply with this Standard may be denied access to University IT resources and may be subject to 10.1.0 Disciplinary Action Standard.

Noncompliant devices may be disconnected from the IT infrastructure until the device is brought into compliance.

Effective Date
All users currently using mobile computing and storage devices must bring the device in compliance with this policy effective Month, Day, Year.

Exceptions
The Information Security Officer or designee may approve exceptions to this policy.
D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

Federal and State Law
University Policy 6202 Telework Policy
University Policy 3310 Allowance for Usage of Personal Mobile Devices and Wireless Service for University Business
University IT Policies
09.1.0 Acceptable Use Standard
02.3.0 Data Classification Standard
05.1.0 IT Security Incident Handling Standard
05.4.0 Virus & Malicious Code Protection Standard
10.1.0 Disciplinary Action Standard

E. HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2013</td>
<td>IT Policy Office</td>
<td>Created; replacement/merge of Portable Computer Management Standard and Remote Access Standard</td>
</tr>
</tbody>
</table>

SharePoint Library, Standard #
Last updated: 8/14/2013