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>Business Continuity and Disaster Recovery Plan Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Number:</td>
<td>7.2.0</td>
</tr>
<tr>
<td>Date of Current Revision or Creation:</td>
<td>December 18, 2012</td>
</tr>
</tbody>
</table>

A. PURPOSE

The purpose of this standard is to outline the Business Continuity and Disaster Recovery Planning requirements for IT systems and data.

B. DEFINITIONS

**Business Continuity Plan (BCP/COOP)** is Old Dominion’s documented plan and set of procedures created to assure that the capability exists to continue essential University functions across a wide range of potential emergencies.

**IT Disaster Recovery Plan (DRP)** is a documented process and set of procedures used to safeguard and recover IT resources in the event of a disaster.

**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.

**Virginia Department of Emergency Management (VDEM)** is the State agency that works with local government, state and federal agencies and voluntary organizations to provide resources and expertise in emergency management.
C. STANDARDS STATEMENT

IT Systems and Data Requirements for Business Continuity
Commonwealth of Virginia Continuity of Operations Planning requirements are defined by Virginia Department of Emergency Management (VDEM.) The Continuity of Operations Planning Manual published by VDEM will be consulted for IT related requirements. IT requirements will be included as a part of the University’s Business Continuity of Operations Plan (COOP.)

COOP & DR Liaison Designee
The University has designated the Information Security Officer (ISO) as the employee assigned to collaborate with the agency Continuity of Operations Plan (COOP) coordinator on the IT aspects of COOP and related Disaster Recovery planning activities.

Business Impact Analysis
Based on Business Impact Analysis (BIA) and Risk Assessment (RA) results, ODU will develop COOP IT-related documentation which identifies:

1. Essential business functions that require restoration and the Recovery Time Objective (RTO) for each;
2. Recovery requirements for IT systems and data needed to support the essential business functions; and
3. Personnel contact information and incident notification procedures.

Disaster Recovery Plan (DRP)
The documentation on the continuity of IT business operations is provided in the IT Disaster Recovery Plan (DRP). The DRP is to be protected as sensitive data and stored at a secure off-site location.

The DRP will be maintained, reviewed and updated with each review and change documented, minimally at 12 month intervals.

The DRP will include manual process procedures for designated ITS staff to reference as part of restoration of essential university services. Departments are responsible for the manual processes and procedures used to accomplish their primary business.

The DRP will, where possible, address the sequence of essential function restoration. The plan recognizes that many services are dependent upon Banner Administrative System restoration yields and related access. Essential functions that must be restored will be factored into the entire restoration sequence and documented accordingly. Such technical instruction and restoration procedures are included in the DRP for reference.

The DRP will document the identified support teams, their specific responsibilities and names and contact information of team members and alternate team members. Contact information will be maintained in the DRP but marked as restricted.
The DRP will address the utilization of equipment residing in a remote location used to house computer storage and tape media.

The DRP will include information regarding the creation, use and control of backups, such as frequency and related server names. IT is responsible for the execution and maintenance of backups to essential servers and databases.

The Disaster Recovery Plan works in conjunction with the University Business Continuity Plan (BCP/COOP). Changes made to the DRP will be coordinated to ensure that the changes are in agreement with the University BCP/COOP. Issues which appear to be in conflict are to be directed to IT management for resolution.

**Disaster Recovery Testing**

IT will conduct an annual exercise (or more often as necessary) to assess the adequacy and effectiveness of the remote backup site and the selected essential IT services. Testing will include the work groups designated to support the restoration of essential services. Effective preplanning is expected and proper notification is to be given to the campus regarding the test schedule and possible disruption of services.

Results from any Disaster Recovery Test will be reviewed by IT management. Participants will meet post-test to discuss actions, activities and obstacles experienced during the test. Discussions should address ways of accomplishing goals with pre-stage solutions and amending the test objectives as needed.

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

Federal and State Law  
Policy 3505 Security Policy  
7.1.0 Business Impact Analysis Standard  
8.1.0 Risk Assessment Standard

**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>Rerwording for clarity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Numbering revision</td>
</tr>
</tbody>
</table>