

# Frostburg State University

## Data Use Standards

---

### Purpose

Frostburg State University has developed Data Use Standards as part of its Data Classification Policy. These standards outline requirements for handling and protecting all the University's institutional data, whether it be Public, Internal Use Only, or Confidential.

### Scope

All members of the Frostburg State University community (staff, faculty, students, contractors, consultants, visitors, etc.) must safeguard Frostburg State University data. Accordingly all members should be able to readily identify the data classification of the information resources they encounter, and are responsible for ensuring the minimum standards of treatment are met.

### Policy

The following table defines required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

<b>Security Control Category</b>	<b>Data Classification</b>		
	<b>Public</b>	<b>Internal Use Only</b>	<b>Confidential</b>
<i>Access Controls</i>	<ul style="list-style-type: none"> <li>No restriction for viewing</li> </ul>	<ul style="list-style-type: none"> <li>Viewing and modification restricted to authorized individuals as needed for business-related roles</li> <li>Authentication and authorization required for access</li> </ul>	<ul style="list-style-type: none"> <li>Viewing and modification restricted to authorized individuals as needed for business-related roles</li> <li>Authentication and authorization required for access</li> <li>Confidentiality agreement required</li> </ul>
<i>Copying/Printing (applies to both paper and electronic forms)</i>	<ul style="list-style-type: none"> <li>No restrictions</li> </ul>	<ul style="list-style-type: none"> <li>Data should only be printed when there is a legitimate need</li> <li>Copies must be limited to individuals with a need to know</li> <li>Data should not be left unattended on a</li> </ul>	<ul style="list-style-type: none"> <li>Data should only be printed when there is a legitimate need</li> <li>Copies must be limited to individuals authorized to access the data and have signed a confidentiality</li> </ul>

		printer	<p>agreement</p> <ul style="list-style-type: none"> <li>Data should not be left unattended on a printer</li> </ul>
<i>Network Security</i>	<ul style="list-style-type: none"> <li>Protection with a network firewall recommended</li> <li>IDS/IPS protection recommended</li> </ul>	<ul style="list-style-type: none"> <li>Protection with a network firewall required</li> <li>IDS/IPS protection required</li> <li>Servers hosting the data should not be visible to entire Internet</li> </ul>	<ul style="list-style-type: none"> <li>Protection with a network firewall with only minimal access permitted</li> <li>IDS/IPS protection required</li> <li>Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets such as the guest wireless network</li> <li>The firewall ruleset should be reviewed periodically</li> </ul>
<i>Virtual Environments</i>	<ul style="list-style-type: none"> <li>May be hosted in a virtual server environment</li> <li>All other security controls apply to both the host and the guest virtual machines</li> </ul>	<ul style="list-style-type: none"> <li>May be hosted in a virtual server environment</li> <li>All other security controls apply to both the host and the guest virtual machines</li> </ul>	<ul style="list-style-type: none"> <li>May be hosted in a virtual server environment</li> <li>All other security controls apply to both the host and the guest virtual machines</li> </ul>
<i>Physical Security</i>	<ul style="list-style-type: none"> <li>System must be locked or logged out when unattended</li> </ul>	<ul style="list-style-type: none"> <li>System must be locked or logged out when unattended</li> <li>Hosted in a secure location required; a Secure Data Center is recommended</li> </ul>	<ul style="list-style-type: none"> <li>System must be locked or logged out when unattended</li> <li>Hosted in a Secure Data Center required</li> </ul>
<i>Remote Access to systems hosting the data</i>	<ul style="list-style-type: none"> <li>Access restricted to local network or FSU Virtual Private Network (VPN) service</li> </ul>	<ul style="list-style-type: none"> <li>Access restricted to local network or FSU Virtual Private Network (VPN) service</li> <li>Remote access by third party for technical support</li> </ul>	<ul style="list-style-type: none"> <li>Restricted to local network or secure VPN group</li> <li>Unsupervised remote access by third party for technical support</li> </ul>

		limited to authenticated, temporary access via FSU Virtual Private Network (VPN) service	not allowed
<i>Data Storage</i>	<ul style="list-style-type: none"> <li>Storage on a secure server recommended</li> <li>Storage in a secure Data Center recommended</li> </ul>	<ul style="list-style-type: none"> <li>Storage on a secure server recommended</li> <li>Storage in a secure Data Center recommended</li> <li>Should not store on an individual's workstation or a mobile device. This includes personal and/or contractor-owned equipment.</li> </ul>	<ul style="list-style-type: none"> <li>Storage on a secure server required</li> <li>Storage in Secure Data Center required</li> <li>Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use encryption. This includes personal and/or contractor-owned equipment.</li> <li>Portable media (e.g., portable hard drives, flash drives, magnetic tapes, and CDs) must be stored in a secure location</li> <li>Paper/other hard copy: do not leave unattended where others may see it; store in a secure location</li> </ul>
<i>Transmission</i>	<ul style="list-style-type: none"> <li>No restrictions</li> </ul>	<ul style="list-style-type: none"> <li>No requirements</li> <li>Encryption recommended (for example, via SSL or secure file transfer protocols)</li> </ul>	<ul style="list-style-type: none"> <li>Encryption required (for example, via SSL or secure file transfer protocols)</li> <li>Cannot transmit via e-mail unless encrypted and secured with a digital signature</li> </ul>
<i>Backup/Disaster Recovery</i>	<ul style="list-style-type: none"> <li>Backups required; daily backups</li> </ul>	<ul style="list-style-type: none"> <li>Daily backups</li> </ul>	<ul style="list-style-type: none"> <li>Daily backups</li> </ul>

	recommended	required	required
		<ul style="list-style-type: none"> <li>Off-site storage recommended</li> </ul>	<ul style="list-style-type: none"> <li>Off-site storage in a secure location required</li> </ul>
<i>Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, etc.)</i>	<ul style="list-style-type: none"> <li>See "Frostburg State University Media Disposal Procedures"</li> </ul>	<ul style="list-style-type: none"> <li>See "Frostburg State University Media Disposal Procedures"</li> </ul>	<ul style="list-style-type: none"> <li>See "Frostburg State University Media Disposal Procedures"</li> </ul>
<i>Training</i>	<ul style="list-style-type: none"> <li>General security awareness training recommended</li> <li>System engineer or admin recommended</li> </ul>	<ul style="list-style-type: none"> <li>General security awareness training required</li> <li>System engineer or admin recommended</li> </ul>	<ul style="list-style-type: none"> <li>General security awareness training required</li> <li>System engineer or admin required</li> <li>Applicable policy and regulation training required</li> </ul>

**Revision History**

<b>Version Number</b>	<b>Date</b>	<b>Author</b>	<b>Description</b>
1.0	March 2015	Lori Bennett	Initial Document
1.1	July 2015	Lori Bennett	Added portable media specifications
1.2	September 2015	Lori Bennett	Approved 9/2/2015