### Guidance on Data Storage and Sharing

<table>
<thead>
<tr>
<th>Data Classification Level</th>
<th>Examples</th>
<th>Secure Storage &amp; Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidential Data</strong></td>
<td>Unauthorized disclosure and/or loss of control of confidential data may reasonably result in significant financial losses, unacceptable risks, or impair the efficient conduct of the University mission.</td>
<td>Approved Storage - Banner, Fortis, uStor</td>
</tr>
</tbody>
</table>
| **High Security**                                             | • Personal Identifiers: Birthdate, SSN, Driver’s license number, and Mother’s Maiden Name  
  • Financial Data: Credit Card Numbers, Bank Account Numbers  
  • Authentication Data: Biometric Information, Passwords, Digital Signatures  
  • Protected Health Information | Secure Exchange - Filelocker                                    |
| **Sensitive Data**                                            | Sensitive data is private data that must be protected, but has a lesser degree of impact associated with unauthorized disclosure and/or loss of control versus confidential data.                                                                                                                                  | Approved Storage - Banner, Fortis, uStor                     |
| **Medium Security**                                           | • Personally identifiable information including home address, and marital status  
  • Personnel Data including beneficiary and dependent information | Secure Exchange - Filelocker                                  |
| **Internal Data**                                             | Proprietary data or information produced only for use by University members with a legitimate purpose to access such data.                                                                                                                                                                                                           | Internal Data should only be stored and shared via University owned, maintained, or purchased devices, solutions, and services.                                                                 |}

| **Public Data**                                               | Institutional information that has few restrictions and/or is intended for public use.                                                                                                                                                                                                                                                  | There are no security restrictions or guidance needed for Public Data.                               |
| **Minimum Security**                                          | • Directory information  
  • Presentations  
  • Press releases                                                                                                                                                                                                                                                                                                                  |--------------------------------------------------------------|

9/2015 [http://security.appstate.edu/resources/policies_and_standards/data_class_guideline](http://security.appstate.edu/resources/policies_and_standards/data_class_guideline) for more information. Questions? Email security@appstate.edu