I. BACKGROUND

The University of Arizona takes seriously its commitment to respect and protect the privacy of its students, alumni, faculty and staff, as well as to protect the confidentiality of information important to the University's academic and research mission. For that reason, UA has classified its information assets into the categories Regulated, Confidential, Public, and Internal for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access.

II. DATA CLASSIFICATIONS

Use these criteria to determine which data classification is appropriate for a particular information asset.
<table>
<thead>
<tr>
<th><strong>INTERNAL</strong></th>
<th><strong>PUBLIC</strong></th>
<th><strong>CONFIDENTIAL</strong></th>
<th><strong>REGULATED</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Data not intended for public use or exposure. Internal data generally should not be disclosed outside of the University without the permission of the person or group that created the data. Any data not specifically classified as Regulated, Confidential, or Public should be considered Internal.</td>
<td>Data that may be disclosed to any person, regardless of affiliation with the University. Some level of control is required to protect the integrity and availability of Public data (e.g., protecting original (source) documents from unauthorized modification).</td>
<td>Data controlled by federal, state, local, and/or industry regulations. These data are affected by data breach notification laws and contractual provisions in government research grants, which impose legal and technical restrictions on the appropriate use of institutional information.</td>
</tr>
</tbody>
</table>

| **Examples** | • Proprietary University information, produced for use only by UA community members  
• Internal operating procedures and operational manuals  
• Internal memoranda, emails, reports and other documents  
• Contact lists that contain information that is not publicly available  
• Technical documents, such as system configurations | • Public-facing web pages  
• Directory data (e.g., contact information)  
• Press releases  
• Course information  
• Dates of attendance  
• Application and request forms  
• Maps, newsletters, newspapers and magazines | • Applicant, alumni, donor, potential donor and parent data  
• FERPA and GLBA data  
• Human Subject Research data  
• Restricted or unpublished research data  
• Data protected by confidentiality agreements  
• Law enforcement or court records and confidential investigation records  
• Citizen or immigrations status  
• Detailed information about certain University buildings, activities or events, including facility security system details  
• Social Security Numbers  
• Credit Card Numbers  
• Financial/ Banking Account Numbers  
• Driver’s License Numbers  
• Health Insurance Policy ID Numbers  
• Data as defined under FISMA, ITAR/EAR, HIPAA |

Policy title: Data Classification and Handling Standard  
Policy number: IS-S302, Version #3  
Last updated: 10/9/2017
<table>
<thead>
<tr>
<th>Access</th>
<th>Access limited to members of the UA community.</th>
<th>Open access to public information. However, care should always be taken to use all University information appropriately and to respect all applicable laws. Information that is subject to copyright must only be distributed with the permission of the copyright holder.</th>
<th>Access limited to those with a need to know, at the discretion of the data owner or custodian.</th>
<th>Access limited to those permitted under law, regulation and UA policies, and with a need to know.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission-Encryption</td>
<td>No encryption is required for the transmission of Internal Data.</td>
<td>No encryption is required for the transmission of Public Data.</td>
<td>Encryption is strongly recommended when transmitting information through a network. Third-party email services are discouraged for transmitting Confidential Data.</td>
<td>NIST-approved encryption is required when transmitting information through a network. Regulated numbers may be redacted instead of encrypted.</td>
</tr>
<tr>
<td>Transmission-Wireless Network</td>
<td>Wireless transmission of Internal Data permissible.</td>
<td>Wireless transmission of Public Data permissible.</td>
<td>Encryption is strongly recommended when transmitting information through a wireless network. Third-party email services are discouraged for transmitting Confidential Data.</td>
<td>Wireless transmission of data must be approved by appropriate compliance officers and/or Information Security Officer. If approved, NIST-approved encryption is required. Regulated numbers may be redacted instead of encrypted.</td>
</tr>
<tr>
<td>Transmission-Email</td>
<td>Email of Internal Data permissible.</td>
<td>Email of Public Data permissible.</td>
<td>Encryption is strongly recommended when emailing Confidential Data. Third-party email services are discouraged for transmitting Confidential Data.</td>
<td>NIST-approved encryption is required for all Regulated Data. Third-party email services are not appropriate for transmitting Regulated Data. Regulated numbers may be redacted instead of encrypted.</td>
</tr>
<tr>
<td>Storage</td>
<td>No encryption is required for the storage of Internal Data. Care should still be taken to protect the integrity of Internal Data.</td>
<td>No encryption is required for the storage of Public Data. Care should still be taken to protect the integrity of Public Data.</td>
<td>Encryption is strongly recommended. If appropriate level of protection is not known, check with the data steward and/or the Information Security Office before storing Confidential Data unencrypted. Third-party processing or storage services may receive or store Confidential data if UA has a valid contract with the vendor that specifies appropriate storage or Confidential Data.</td>
<td>Encryption is required for storage of Regulated Data. Regulated numbers may be redacted instead of encrypted.</td>
</tr>
</tbody>
</table>

Please see Data Classification and Handling Standard [File Share Quick Reference Guide](#) to determine which data classification is appropriate for storage and sharing in particular assets.

### III. REVISION HISTORY

A. Revision 1: 11/15/08  
   • Effective 7/1/09  
B. Revision 2: 5/1/15  
   • Effective 5/1/15  
C. Revision 3: 10/9/17  
   • Effective 10/9/17