POLICY COVER SHEET

(See Faculty Staff Handbook 1460 for instructions at UI policy website: www.webs.uidaho.edu/uipolicy)

[3/09]

Faculty/Staff Handbook [FSH] ☐ Addition ☐ Revision* ☐ Deletion* ☐ Emergency

Minor Amendment ☐

Chapter & Title: ________________________________________________________________

Administrative Procedures Manual [APM] XX Addition ☐ Revision* ☐ Deletion* ☐ Emergency

Minor Amendment ☐

Chapter & Title: APM 30.### UI Data Classification and Standards Policy (New policy)

All policies must be reviewed, approved and returned by a policy sponsor, with a cover sheet attached to apm@uidaho.edu or fsh@uidaho.edu respectively.

*Note: If revision/deletion request original document from apm@uidaho.edu or fsh@uidaho.edu, all changes must be made using "track changes."

Originator(s):
(Please see FSH 1460 C)

Name: Mary George, Mitch Parks
Date: 5/19/16

Telephone & Email:
maryg@uidaho.edu, mitch@uidaho.edu
5-5222, 5-2522

Policy Sponsor: (If different than originator.)

Name: Dan Ewart
Date: 5/19/16

Telephone & Email: dewart@uidaho.edu, 5-2271

Reviewed by General Counsel ☐ Yes ☐ No Name & Date: ________________________________

I. Policy/Procedure Statement: Briefly explain the purpose/reason of proposed addition, revision, and/or deletion to the Faculty/Staff Handbook or the Administrative Procedures Manual.

This policy establishes the responsibility of university data users to protect the data they have access to and the levels of protection required based upon the type of data being accessed.

II. Fiscal Impact: What fiscal impact, if any, will this addition, revision, or deletion have?

This policy should reduce the risk and exposure to the university by unsecured or unprotected data. Reduction in risk correlates to reduction in costs due to fines, administrative costs, and litigated costs in the event of a data security breach.

III. Related Policies/Procedures: Describe other policies or procedures existing that are related or similar to this proposed change.

APM 30.13 – Network device standards addresses system and physical device security from which data security is inferred. This new policy addresses the security needed for the data, which is the ultimate goal, from which will infer the security needed on physical devices depending on the types of data that they access. APM 30.13 should stay in place until it can be revised or deleted after all topics in it have been reviewed and addressed elsewhere.
### IV. Effective Date:
This policy shall be effective on July 1, or January 1, whichever arrives first after final approval (see FSH 1460 D) unless otherwise specified in the policy.

If not a minor amendment forward to: ____________________________

<table>
<thead>
<tr>
<th>Policy Coordinator</th>
<th>FSH</th>
<th>Track # __________</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appr. &amp; Date:</td>
<td>Appr. __________</td>
<td>__________</td>
</tr>
<tr>
<td>[Office Use Only]</td>
<td>FC</td>
<td>Date Rec.: __________</td>
</tr>
<tr>
<td></td>
<td>GFM</td>
<td>Posted: t-sheet __________</td>
</tr>
<tr>
<td></td>
<td>Pres./Prov. __________</td>
<td>h/c __________</td>
</tr>
<tr>
<td>[Office Use Only]</td>
<td></td>
<td>web __________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APM</th>
<th>Register: __________</th>
</tr>
</thead>
<tbody>
<tr>
<td>F&amp;A Appr.: __________</td>
<td>[Office Use Only]</td>
</tr>
<tr>
<td></td>
<td>(Office Use Only)</td>
</tr>
</tbody>
</table>