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: ____________________________________________

Minor Amendment □
Chapter & Title: APM 30.12 – UI Computer Use 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 Date
Mary George 1/30/17
Telephone & Email: maryg@uidaho.edu 885-5222

Policy Sponsor: (If different than originator.) Name Date
Dan Ewart
Telephone & Email: dewart@uidaho.edu 885-2271

Reviewed by General Counsel __X__Yes ____No Name & Date: Casey Inge & Kent Nelson – May 2016-Jan 2017

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.

The current computer use policy is very old and outdated. Much of the policy is specific to certain technologies (email, directories, etc.) or needs to be placed in an area that can be updated easily (with proper structure) when technologies, phone numbers, procedures, etc. change. The new policy should be succinct, but broad enough to cover all of the existing issues (and more) without being specific to the types of systems or technology resources, which is what this new policy is intended to accomplish. ITS will maintain publicly-available, published information on technology standards and will have a published process for ensuring that any changes made to the standards are suitably vetted.

The current computer use policy addresses the following topics:
1. State law, university policy
2. Commercial/political/personal benefit use
3. Accessing directories, files, and emails
4. Electronic files as public records
5. Unauthorized machine access, decryption, unauthorized privileges
6. Removal/transferring software
7. Sharing accounts
8. Password protection
9. Leaving a computer
10. Sensitive personal information storage
11. Disturbing others, food in computer labs, inferring w/ system operation
12. Sending offensive messages
13. Consuming unreasonable amount of resources
14. Playing games on computers

The new policy updates the language to cover the responsibilities of users and systems: (Below are the topics covered in the rewritten policy. Numbers indicate existing policy topics that are covered in the new policy rewrite)

- Federal & state laws (1)
- Personal conduct (11)
- Privacy - new
- UI policies & procedures (1, 2)
- Security and privacy of devices and data (3, 5)
- Reporting violations - new
- Unauthorized & attempts to access unauthorized resources (3, 5, 6, 7)
- Intercepting/hindering traffic
- Access, destroy, modify data/systems (5, 6)
- Commercial/political/personal benefit/use (2, 14)
- Unlawful, obscene, defamatory (12)
- Personal safety, security
- Copyright, copying files (6, new)
- References to various codes and legislation (1)

Notes:
Topic 4 – Is not specifically covered in this new policy. Our FSH 6520/APM 65.03 & 65.06 – also does not specifically cover this information item, but is somewhat close. It would seem that the records management section in the APM (65.##) may be a more suitable spot to discuss that any type of records (paper or electronic) are university property—if we want to add this to our university policies?
8, 9, 13 – Will be covered in ITS standards documents and subsequent other IT policy revisions in progress.
10 – Covered in the new data classification policy – APM 30.11.
11 – This will be covered in ITS computer lab-specific info

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

This should reduce UI’s risk exposure by having a policy that clearly states the obligation of all persons and systems that access UI technology resources and allows flexible access to create technology-specific updates as needed in related standards documents. Reducing risk should reduce costs associated with technology security breaches or issues which can amount to millions of dollars in costs.

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

We have reviewed all of the “IT-related” policies within the UI and the State ITA office. We did reviews of other universities IT policies and compared the topics covered in their acceptable use policies with ours. We came up with a prioritized list of topics that should be covered by this policy, while ensuring that we are covering all of the existing topics somewhere. We have a number of worksheets that show all of the related “IT” topics and the current policies that are related or similar to this change. We can send those files, if needed, please ask. They are quite huge and may require some additional explanation.

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></td>
<td>Date Rec.: ______________</td>
</tr>
<tr>
<td></td>
<td>Appr. __________</td>
<td>Posted: t-sheet __________</td>
</tr>
<tr>
<td>[Office Use Only]</td>
<td>FC</td>
<td>h/c __________</td>
</tr>
<tr>
<td></td>
<td>GFM</td>
<td>web __________</td>
</tr>
<tr>
<td></td>
<td>Pres./Prov. ______</td>
<td>Register: ______________</td>
</tr>
<tr>
<td>[Office Use Only]</td>
<td></td>
<td>(Office Use Only)</td>
</tr>
</tbody>
</table>

**APM**

<table>
<thead>
<tr>
<th>F&amp;A Appr.: __________</th>
<th>[Office Use Only]</th>
</tr>
</thead>
</table>