IT Operational Oversight Committee

Review IT Acceptable Use Policy

October 31, 2011

Project Title – Review IT Resource Acceptable Use Policy.

Project Team –

- Jolene A. King, Business Office - Physical Facilities, Fiscal Director Physical Facilities
- Markus A. Lill, Medicinal Chemistry/Molecular Pharmacology in College of Pharmacy
- David R. McKinnis, Technical Assistance Program, Director Technical Assistance Program/Assoc. Vice Provost
- Terry W. Schroeder, Administrative Computing, Executive Director Administrative Computing
- Joanna Grama, ITaP Networks and Security, Information Security Policy and Compliance Director

Executive Summary –

This team reviewed proposed revisions to the IT Resources Acceptable Use Policy and suggested additional revisions to the policy consistent with University objectives, other IT policies, and best practices from other institutions. The result of this team’s work is a newly revised IT Resources Acceptable Use Policy that can be submitted to the University Policy Office for consideration. A copy of the current IT Resources Acceptable Use Policy and proposed revised policy is attached to this report.

Report and Recommendation(s) –

An acceptable use policy is the cornerstone of any organization’s information security program. These types of policies tell employees how to properly use the organization’s information technology resources. Because organizations cannot always enforce through technology how its users actually use information technology resources, these types of policies are primarily created in order to influence user behavior. An acceptable use policy is essentially a code of conduct. It states permitted and prohibited uses of an organization’s information technology resources and can be used to address a range of personnel, legal, and information security issues.

The IT Resource Acceptable Use Policy (V.4.1) was originally issued in July 2004. The current document can be found at: http://www.purdue.edu/policies/pages/information_technology/v_4_1.html. It has not been revised since it was created, despite numerous attempts to do so. Since Purdue has formalized its system-wide policy creation and revision process, there now exists a clear way in which to revise this policy. In January 2011, the University Policy Office formally asked IT Networks and Security to review the IT Resource Acceptable Use Policy (IT AUP) as part of a regular five-year review. The University Policy Office also asked IT Networks and Security to revise the IT AUP into the new policy format specified by the Policy Office.
IT Operational Oversight Committee

Review IT Acceptable Use Policy

October 31, 2011

As part of this review, Gerry McCartney, Vice President of Information Technology, asked an Operational Oversight Committee working team to spearhead this task to ensure a comprehensive review of the document.

A copy of the revised IT AUP, as proposed by IT Networks and Security and reviewed by the Operational Oversight working team, is attached to this report. The revised document was prepared after a review of substantive edits that have been proposed from 2006-2011 by IT Networks and Security, the University’s Security Officers Working Group, and the University’s Data Stewards Organization. The revised document also includes revisions proposed by this team after reviewing similar acceptable use policies from Purdue’s strategic partner and peer institutions.

Key stakeholders for any information security policy include the Office of the Vice President for Information Technology, IT Networks and Security (ITNS), the University’s Security Officers Working Group, and the University’s Data Stewards Organization. The information security policy process is described at: http://www.purdue.edu/securepurdue/bestPractices/endUserSecurityGuidelines.cfm

After a policy is proposed and an initial draft created according to the above process, the policy is submitted to the University Policy Office and will follow the formal policy creation and review process described at: http://www.purdue.edu/policies/pages/about_policies/about_pol.html

In addition to policy review, this Operational Oversight Committee working team proposes the following recommendations for IT Networks and Security (or other Office of the Vice President for Information Technology operational areas as needed):

- Consider developing a list of specific security recommendations for departments to follow. For instance, having a checklist of physical security actions might be helpful for both departments and end users. (ITNS has already begun work on this task in response to this suggestion.)

- Consider the long-term ramifications of personal-use devices that access/use IT Resources. How can we make this use more secure? How can we better ensure that users understand that their use of Purdue IT Resources on their personal device brings them under the rubric of Purdue’s IT security (and other) policies?

- Consider a list of FAQs for the IT AUP that describe common issues that the University/ITaP encounters, and how those issues are resolved under the IT AUP. (ITNS has already begun work on this task in response to this suggestion.)

- Consider whether Purdue needs to re-think how it allows users to use personal devices to access restricted data. Should we even allow this? If yes, what parameters should be put in place to ensure good security?

- Consider "working from home" guidelines document/article to help users understand their responsibilities for working from home. (ITNS has already begun work on this task in response to this suggestion.)

- Consider the method of dissemination of this policy, for example should it be in freshman orientation, new employee orientation, or should we receive notices when violating (such as
excessive use), etc. Our thinking is that nearly no one may read and know this policy, thus dissemination should be reviewed/addressed.

Timeline –
Below is the complete timeline for revisions to the IT AUP since its original promulgation. Once the proposed revisions to the IT AUP are provided to the University Policy Office, time to policy approval and promulgation is estimated to be six months.

- July 30, 2004: Original issuance of the IT AUP.
- February 3, 2006: University Security Officers group asked for comments about current IT AUP. (No comments received.)
- October 11, 2006: Request from the Office of the Vice President for Research (Pete Dunn) to eliminate a conflict in the IT AUP with language in the Email Use Policy regarding modest personal use. Meeting with Peter Dunn (VPR), Gerry McCartney (VPIT), Peg Fish (Internal Audit), and Joanna Grama (ITNS) regarding policy conflicts relative to personal use of IT Resources and outside activities use of University IT Resources.
- November 22, 2006: Initial proposed revisions to the IT AUP forwarded to the IT Executive Steering Committee (ITESC) for discussion (the determination was made not to forward the changes through the Security officers group since the initial revisions were only to resolve a conflict with an existing policy).
- November 28, 2006: ITESC Meeting; ITESC asks for additional review of the revised IT AUP to address outside activities use of IT Resources. (Note that the ITESC met two times per year, as agenda items dictate.)
- December 21, 2006: Meeting with Peter Dunn, Gerry McCartney, Peg Fish, Scott Ksander (ITNS), Connie Lapinskas (Provost's office), and Joanna Grama regarding IT AUP policy revisions for outside activities.
  - Joanna Grama and Pete Dunn charged with creating an “Outside Activities Warning Letter” that could be used during the Form 32A approval process to alert faculty to the dangers in using Purdue IT Resources for outside activities such as consulting or expert witness work.
- February 13, 2007: Revisions to the IT AUP and the “Outside Activities warning letter” forwarded to Peter Dunn, Gerry McCartney, Peg Fish, Scott Ksander, and Connie Lapinskas for consideration.
- April 17, 2007: Following receipt of comments from the February 13, 2007 working committee, revisions to the IT AUP forwarded to Scott Ksander for transmittal to the ITESC for final consideration.
- April 17, 2007: ITNS forwards revised IT AUP to Purdue Marketing and Communications (PMC) for editorial review (to be completed contemporaneously with the ITESC review).
- April 24, 2007: ITNS forwards revised IT AUP to Legal Counsel for review.
- April 24, 2007: ITESC Meeting; Review and approval of the revised IT AUP
- May 4, 2007: Legal Counsel completes review of policy with no additional comments or concerns.
IT Operational Oversight Committee

Review IT Acceptable Use Policy

October 31, 2011

- May 4, 2007: Approved (ITESC, PMC, and Legal) revised IT AUP transmitted to Gerry McCartney for forward to EVPT and Provost for review, and for subsequent Presidential signature.
- August 14, 2007: Morgan Olsen (then EVPT) requests additional revisions to IT AUP to the new outside activities language. Pete Dunn and Gerry McCartney agree to follow-up.
- September 20, 2007: ITESC Meeting; IT AUP revisions under advisement.
- March 4, 2008: ITNS receives revised IT AUP from Pete Dunn. (Note that prior to 2011, this was the last date with proposed revisions to the IT AUP.)
- July 8, 2008: ITESC Meeting; IT AUP revisions taken under advisement.
- November 20, 2008: ITESC Meeting; IT AUP revisions still under advisement. ITESC discussed strategies for getting proposed revisions in front of University Senate for review and comment prior to promulgation. (It is unknown whether the IT AUP was presented to the University Senate. Minutes of the University Senate during the 2008-2010 period do not reflect review of the IT AUP by the full senate.)
- April 8, 2009: ITESC Meeting; IT AUP not discussed due to lack of status update.
- October 30, 2009: University policy on “Formulation and Issuance of Purdue University System-Wide Policies (III.1.1)” promulgated. ITNS decides to pursue revisions to IT AUP through new, formal University process.
  - Further revisions to the policy were held at this time pending the ability to engage the ITESC in ensuring adequate stakeholder review of the revised IT AUP.
- August 2010: ITESC disbanded as IT Governance structure moves toward that described in the Campus Information Technology Plan (CITP). Policy issues will be dealt with via the governance vehicles described in the CITP as situations dictate.
- January 13, 2011: University Policy Office requests review of IT AUP as part of its regular 5-year review process.
- February-April 2011: ITNS (Joanna Grama) edits last-known revised IT AUP version (dated March 4, 2008) into the University’s new policy template; makes edits to the IT AUP as needed for clarity and to conform to new policy format.
- April 2011: Gerry McCartney agrees to form a working group through the IT Governance Operational Oversight Committee to review the IT AUP in anticipation of revisions to the policy.
- May 17, 2011: Joanna Grama meets with University Policy Office Coordinator, Jessica Teets, to determine process for policy approval at this point and to convey information to Operational Oversight Committee.
- May 20, 2011: Operational Oversight working committee formed to review current IT AUP, proposed IT AUP (in new policy format), and research to date to ensure that appropriate revisions are made to the IT AUP.
- June-October, 2011: Operational Oversight working committee reviews, discusses, and makes edits to IT AUP.
- October 10, 2011: Final Operational Oversight working committee edits complete.
IT Operational Oversight Committee

Review IT Acceptable Use Policy

October 31, 2011

- October 10, 2011: Proposed revisions to IT AUP are shared with Office of the Vice President for Information Technology Leadership Team, and a select group of data stewards and security officers for early feedback and review.
- October 21, 2011: Feedback received and incorporated from stakeholders.
- October 31, 2011: This final report prepared and presented to the Operational Oversight Committee in anticipation of presentation to IT Strategic Governance Committee.

Resource Requirements –

There are no new costs required to implement and sustain the IT Resource Acceptable Use Policy or any of the recommendations proposed by this working team. It is this team’s understanding that IT Network and Security addresses operational issues regarding information security policies within the “Information Security Policy and Compliance Director” position.

Attachments-

1. Bibliography of peer institution acceptable use policy sites.
Attachment #1

Bibliography of peer institution acceptable use policy sites (Last updated: 5/17/2011)

University of Illinois
- [http://www.cam.illinois.edu/viii/VIII-1.1.htm](http://www.cam.illinois.edu/viii/VIII-1.1.htm)

Indiana University
- [http://informationpolicy.iu.edu/policies/IT01.shtml](http://informationpolicy.iu.edu/policies/IT01.shtml)

University of Iowa
- [http://www.uiowa.edu/~our/opmanual/ii/19.htm](http://www.uiowa.edu/~our/opmanual/ii/19.htm)

University of Michigan
- [http://spg.umich.edu/pdf/601.07-0.pdf](http://spg.umich.edu/pdf/601.07-0.pdf)
- [http://www.itd.umich.edu/itcsdocs/r1103/](http://www.itd.umich.edu/itcsdocs/r1103/)

Michigan State University
- [http://lct.msu.edu/guidelines-policies/aup/](http://lct.msu.edu/guidelines-policies/aup/)

University of Minnesota
- [http://policy.umn.edu/Policies/it/Use/ITRESOURCES.html](http://policy.umn.edu/Policies/it/Use/ITRESOURCES.html)

Northwestern University
- [http://www.it.northwestern.edu/policies/csn-use.html](http://www.it.northwestern.edu/policies/csn-use.html)
- [http://www.it.northwestern.edu/policies/responsibilities.html](http://www.it.northwestern.edu/policies/responsibilities.html)

Ohio State University
- [http://cio.osu.edu/policies/responsible_use.html](http://cio.osu.edu/policies/responsible_use.html)

Pennsylvania State University
- [http://guru.psu.edu/policies/AD20.html](http://guru.psu.edu/policies/AD20.html)

University of Wisconsin
- [http://www.cio.wisc.edu/policies/appropriateuse.aspx](http://www.cio.wisc.edu/policies/appropriateuse.aspx) (Consider reviewing this one online, their web-interface does not print well)

University of Chicago
- [http://itservices.uchicago.edu/policies/eaup/](http://itservices.uchicago.edu/policies/eaup/)
IT Operational Oversight Committee

Review IT Acceptable Use Policy

October 31, 2011

Cornell University
- http://www.dfa.cornell.edu/dfa/cms/ treasurer/policyoffice/policies/volumes/informationtech/upload/vol5_1.html

Georgia Institute of Technology

University of Arizona
- http://security.arizona.edu/aup

University of California, Berkeley
- http://technology.berkeley.edu/policy/usepolicy.html?view=print

University of California, Davis

University of Texas, Austin
- http://www.utexas.edu/cio/policies/pdfs/AUP.pdf
IT Operational Oversight Committee

Review IT Acceptable Use Policy

October 31, 2011

Attachment #2

Current in-force IT Resource Acceptable Use Policy (V.4.1):

http://www.purdue.edu/policies/pages/information_technology/v_4_1.html
Reason for this Policy

This policy outlines the responsible use of all Purdue University computing and network resources (IT Resources). IT Resources are provided by the University to support its ongoing mission of learning, discovery, and engagement.

Statement of Policy

This policy covers students, faculty, staff, and any and all individuals granted IT Resource privileges at Purdue University and all uses of such IT Resources. Any individual who uses any IT Resources of Purdue University consents to all of the provisions of the following policy and agrees to comply with all of the terms and conditions set forth herein, all other applicable University policies, regulations, procedures, and rules, and with applicable local, state, and federal laws and regulations.
Violations of this policy or any other University policy or regulation may be subject to revocation or limitation of computer and network privileges as well as other disciplinary actions or may be referred to appropriate external authorities.

Common sense and mutual respect for other users underlie all of the rights, privileges, and responsibilities of IT Resource users. Users of Purdue University IT Resources are expected to abide by the following guidelines;

- Comply with all applicable local, state, and federal laws.
- Comply with all Purdue University policies, regulations, procedures, and rules.
- Respect the intellectual property rights of others. Making unauthorized copies of licensed software or copyrighted material is prohibited.
- Refrain from sharing passwords or accounts with anyone, including trusted friends or family members. Users will be held responsible for any actions performed using their accounts. Purdue University information technology staff will never ask users for their passwords.
- Practice the same level of etiquette in all communication using Purdue University IT Resources as expected in non-electronic communication. Respect others when using Purdue IT Resources.
- Only access files or data if they belong to you, are publicly available, or the owner of the data has given you permission to access them.

Prohibited

Prohibited uses of Purdue IT Resources include the following:

- Circumvention of any security measure of Purdue University or another entity.
- Intentional use, distribution, or creation of viruses, worms, or other malicious software.
- Operating a business, usurping business opportunities, organized political activity, or conducting activity for personal gain.
- Excessive use of IT Resources, including, without limitation, resources such as bandwidth, lab computers, and paper.
- Implying that the user is representing, giving opinions, or otherwise making statements on behalf of the University without prior authorization or using Purdue University tradenames, logos, or trademarks without prior written authorization.

Disclaimer

The University makes no warranties of any kind, whether expressed or implied, with respect to the University IT Resources it provides. The University will not be responsible for damages resulting from the use of University IT Resources, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a University employee, or by any user’s error or omissions. The University specifically denies any responsibility for the
accuracy or quality of information obtained through University IT Resources, except material represented as an official University record.

Definitions

IT Resource  A computing asset provided by the University to further its mission of discovery, learning, and engagement. Examples of such assets include, but are not limited to, network bandwidth, computers, mobile devices, printers, and paper.

Who Should Know This Policy

- President
- Provost
- Executive Vice President and Treasurer
- Chancellors
- Vice Presidents
- Deans
- Directors/Department Heads/Chairs
- Principal Investigators
- Business Office Staff
- Administrative and Professional Staff
- Clerical and Service Staff
- All Employees
- Undergraduate Students
- Graduate Students
- Faculty

Related Documents

- Delegation of Administrative Authority and Responsibility For Information Assurance, Security and Awareness (V.1.1)
  http://www.purdue.edu/oop/policies/pages/information_technology/v_1_1.html
- Residence Hall Network Computing AUP

Contacts

Subject  Questions about this policy, or to report a suspected policy violation
Contact  IT Security & Privacy
Telephone  494-4000
E-mail  itap-securityhelp@purdue.edu
IT Operational Oversight Committee

Review IT Acceptable Use Policy

October 31, 2011

Attachment #3

Proposed revised IT Resource Acceptable Use Policy
STATEMENT OF POLICY

This policy applies to all use of University IT Resources. Any individual or entity using IT Resources consents and agrees to comply with all of the terms and conditions set forth in this policy, all other applicable University policies and regulations, and applicable local, state, and federal laws and regulations concerning the use of IT Resources.

The following uses of IT Resources are prohibited:

- Circumvention of any security measure of Purdue University or another entity.
- Intentional use, distribution, or creation of viruses, worms, or other malicious software.
- Creating copies or unauthorized distribution of licensed software or copyrighted material.
• Accessing data that is not publicly available, does not belong to the user, or for which the user does not have explicit permission to access.

• Use of IT Resources for organized political activity that is inconsistent with the University’s tax-exempt status.

• Use of IT Resources that disables other IT Resources, consumes disproportionate IT Resources such that other users are denied reasonable access to those resources, or materially increases the costs of IT Resources.

• Use of IT Resources that violates any other University policy or regulation, including without limitation, Purdue policies on Anti-Harassment (III.C.1) and Equal Opportunity, Equal Access and Affirmative Action (III.C.2).

In most instances, non-Purdue sources of E-mail, Internet access, or other information technology services must be used for activities that are unrelated to the University’s mission. Modest incidental and non-recurring personal uses of IT Resources are tolerated as part of the daily learning and work of all members of the University community, provided that use does not violate any other applicable University policy or regulation.

Use of IT Resources for any purpose unrelated to the University’s missions, or for any purpose that could lead directly or indirectly to Financial Conflicts of Interest, is prohibited unless it has been approved in advance in accordance with Purdue policies on Individual Financial Conflicts of Interest (III.B.2) and Conflicts of Commitment and Reportable Outside Activities (III.B.1). Any such use of IT Resources is with the understanding that the approved use of IT Resources is at the sole discretion of the University and must:

• Comply with all University software licenses.
• Comply with all University policies and practices,
• Comply with federal and state laws and regulations,
• Not generate additional costs to the University, and
• Not interfere with University work or use of IT Resources,

All users of IT Resources will be held responsible for any actions performed using their IT Resource accounts. Violations of this policy or any other University policy or regulation may be subject to revocation or limitation of IT Resource privileges as well as other disciplinary actions or may be referred to appropriate external authorities.

The University makes no warranties of any kind, whether expressed or implied, with respect to the IT Resources it provides. The University will not be responsible for damages resulting from the use of IT Resources, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a University employee, or by any user’s error or omission. The University specifically denies any responsibility for the accuracy or quality of information obtained through IT Resources, except material that is presented as an official University record.

REASON FOR POLICY
This policy outlines the responsible use of all University IT Resources. The University provides IT Resources to support its ongoing missions of discovery, delivery, and engagement.

INDIVIDUALS AND ENTITIES AFFECTED BY THIS POLICY

This policy covers students, faculty, staff, and all individuals or entities using any IT Resource and all uses of such IT Resources.

WHO SHOULD KNOW THIS POLICY

Any individual or entity using IT Resources.

EXCLUSIONS

This policy does not cover personally-owned technology devices that are not connected to or otherwise using University IT Resources.

This policy does not apply to cyber security research activities that, by their very nature, violate the scope of this policy. Such research must be carried out in a manner that employs sufficient and appropriate safeguards to contain the research to pre-defined and intended University IT Resources. Such research must be safeguarded from conception to termination of the research. In addition, such research must not interfere with or compromise the operation or security of other University IT Resources. Faculty, staff, and students conducting such research are strongly encouraged to consult with IT Networks and Security or departmental IT staff to ensure that appropriate safeguards are in place.

Purdue University information security policies institute controls that are used to protect Purdue University data and IT Resources. While every exception to a policy or standard weakens protection for IT Resources and underlying data, occasionally exceptions will exist. The Security Policy Exception Procedure must be used when requesting an exception to Purdue University information security policies. The Chief Information Security Officer, or his or her designee, will approve or deny any request for an exception.

WEBSITE ADDRESS FOR THIS POLICY

http://www.purdue.edu/policies/pages/information_technology/v_4_1.html

CONTACTS

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>E-mail/Web Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Clarification</td>
<td>ITaP Networks and Security</td>
<td></td>
<td><a href="mailto:Itap-securityhelp@purdue.edu">Itap-securityhelp@purdue.edu</a></td>
</tr>
</tbody>
</table>

DEFINITIONS

Financial Conflicts of Interest
This term is used as defined in the University’s policy on Individual Financial Conflicts of Interest (III.B.2).

**IT Incident**
This term is used as defined in the University’s policy on Incident Response (VII.B.3).

**IT Resource**
All computing, network, and information technology assets provided by or for the University to further its missions. Examples of IT Resources include:
- Hardware
- Software
- Wireless access (such as PAL use)
- Network bandwidth (such as Internet connectivity or ResNet use)
- Mobile devices (such as cellular phones, smart phones, pagers, and laptop computers)
- Electronic information resources and the data contained in those resources
- E-mail facilities
- Peripherals (such as printers, copiers, and fax machines)

This definition reflects examples of University IT Resources, but is not all-inclusive.

**Purdue, University, and Purdue University**
Any campus, unit, program, association or entity of Purdue University, including but not limited to Indiana University-Purdue University Fort Wayne, Purdue University Calumet, Purdue University North Central, Purdue University West Lafayette, Purdue Cooperative Extension Service and Purdue University College of Technology Statewide.

**RESPONSIBILITIES**

**ITaP Networks and Security**
Facilitate the establishment and maintenance of standards and technical reference materials to support this policy and post such information online.

**Centralized and Departmental IT Units and IT Resource Owners (and designees)**
Implement and monitor compliance with this policy and related standards on IT Resources within their areas of responsibility.

Ensure that reasonable measures have been taken to secure IT Resources within their areas of responsibility. Physically secure IT Resources within their areas of responsibility. IT Resources may require differing levels of physical security depending on the classification of the data that they process, the systems they access, and their cost.

**Users of IT Resources**
Use IT Resources in compliance with all applicable laws and University policies, including without limitation, the University’s policy on Data Classification and Governance (VII.B.6).
Be familiar with and consult online security standards and technical reference materials as applicable to their use of IT Resources. Physically secure and safeguard IT Resources within the user's possession and control depending on the classification of the data that they process, the systems they access, and their cost. Report violations of this policy and/or suspected IT Incidents immediately and in accordance with the University’s policy on Incident Response (VII.B.3).

PROCEDURES

ITaP Networks and Security will facilitate the establishment and maintenance of standards and technical reference materials to support this policy and post such information online.

Centralized and Departmental IT Units and IT Resource owners and their and designees must follow standards issued by ITaP Networks and Security in support of this policy. These areas may also issue additional guidelines, procedures, or other requirements regarding the use and security of IT Resources within their areas of responsibility. Specific reference materials may vary from campus to campus or department to department. In the event that a unit does not believe it can fulfill the requirements of this policy or its related standards and guidelines, the unit must request a policy exception using the Security Policy Exception Procedure.

RELATED DOCUMENTS, FORMS AND TOOLS

Individual Policies

- Conflicts of Commitment and Reportable Outside Activities (III.B.1): http://www.purdue.edu/policies/ethics/iibi1.html
- Data Classification and Governance (VII.B.6): http://www.purdue.edu/policies/information-technology/viib6.html

University IT Policies: http://www.purdue.edu/policies/information-technology.html

Standards supporting the implementation of this and other university IT policies: www.purdue.edu/securepurdue/bestPractices/


HISTORY AND UPDATES

Comment [JLG5]: Note to UPO: Language added 11/18/2011 in response to request from legal counsel that, as they are revised, language be added to all IT policies to reflect that users have an obligation to immediately report suspected IT policy violations and incidents. This is in response to growing body of laws that require consumer notification in response to an IT or security breach.
XXX X, 2011: Significant revisions have been made to update this policy from its original version, issued July 30, 2004. It also has been formatted in the current policy template.

**APPENDIX (OPTIONAL)**

There are no appendices to this policy.