Remote Access to IT Resources (V.1.6)

POLICY V.1.6
Volume V, Information Services
Chapter 1, Data Security
Responsible Officer: VCIS
Responsible Office: VCIS
Originally Issued: May 24, 2005
Revised: September 25, 2007
Calumet Revision: December 9, 2010

Table of Contents

- Statement of Policy
- Reason for Policy
- Individuals and Entities Affected by This Policy
- Who Should Know This Policy
- Exclusions
- Web Site Address for This Policy
- Contacts
- Definitions
- Responsibilities
- Related Documents, Forms, and Tools
- Appendices

Statement of Policy

Remote access to Purdue University Calumet IT Resources must be accomplished in a manner that enables business, academic, and research activity, while preventing unauthorized access and protecting University IT Resources.

Remote access to IT Resources, unless otherwise specifically denied, is permitted under this policy. Nothing in this policy prevents university IT Resource owners, central and departmental IT units, or other designated individuals from implementing policies, standards, or guidelines related to Remote Access to university IT Resources or computing device use within their areas of responsibility.

Reason for Policy
Controlled access to IT Resources is essential for Purdue University Calumet to continue its mission of learning, discovery, and engagement. This policy describes the appropriate measures necessary for accessing Purdue University Calumet IT Resources from Remote Hosts.

This policy is guided by the following objectives:

1. Preserve Purdue University Calumet’s ability to operate and maintain its IT Resources;
2. Protect the security and functionality of university IT Resources and the data stored on those resources;
3. Safeguard the privacy, property, rights, and data of users of university IT Resources;
4. Preserve the integrity and reputation of the University;
5. Comply with applicable federal, state, and local laws; and
6. Comply with applicable university policies, standards, guidelines, and procedures.

INDIVIDUALS AND ENTITIES AFFECTED BY THIS POLICY

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

Who Should Know This Policy

Chancellors
Vice Chancellors
Deans
Directors
Department Heads and Chairs
Principal Investigators
Faculty and Staff
Students
Non-employee users of Remote Access to university IT Resources

EXCLUSIONS

Purdue University Calumet information security policies institute controls that are used to protect Purdue University Calumet 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 Calumet information security policies. The Vice Chancellor Information Services, or his or her designee, will approve or deny any request for an exception.

WEB SITE ADDRESS FOR THIS POLICY


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>Vice Chancellor Information Services</td>
<td></td>
<td><a href="mailto:vcis@purduecal.edu">vcis@purduecal.edu</a></td>
</tr>
</tbody>
</table>

DEFINITIONS

IT Resource
All tangible and intangible computing and network assets provided by or for the University to further its mission. Examples of such assets include, but are not limited to, hardware, software, wireless access, network bandwidth, mobile devices, electronic information resources, printers, and paper.

Protected Health Information
Health information in any form that can be connected to a patient, including the individual's past, present, or future physical or mental health or condition, the provision of healthcare to the individual, or the past, present, or future payment for the provision of healthcare to the individual.

Remote Access
Access to Purdue University Calumet IT Resources from an electronic or other device not directly connected to the Purdue University Calumet wired or wireless networks, but not including accesses to such IT Resources where Remote Access is considered a primary function and normative use. For example, use of a Web browser to remotely access a Purdue University Calumet Web page is not covered by this policy.

Remote Host
An electronic or other device used for Remote Access.

Remote User
Any user of IT Resources from a Remote Host.
RESPONSIBILITIES

Remote Users
Ensure that reasonable measures have been taken to secure the Remote Host used to access Purdue University Calumet IT Resources.

Prior to accessing IT Resources, follow this policy and any related standards and security requirements for any Remote Host. Remote Users must also follow any guidelines, procedures, or other requirements for Remote Access issued by their departmental IT units and/or owners of the IT Resource(s) to be remotely accessed.

Follow applicable university policies pertaining to data security and use, including but not limited to, the University’s Data Handling Requirements and any guidelines issued by the HIPAA Privacy Compliance Office for Remote Access to Protected Health Information.

Centralized and Departmental IT Units and IT Resource Owners (and designees)

Ensure that reasonable measures have been taken to secure university IT Resources within their areas of responsibility that are to be remotely accessed.

Implement and monitor compliance with this policy and related standards on university IT Resources within their areas of responsibility.

PROCEDURES

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

Departmental IT units must follow standards issued by Information Services in support of this policy. Departmental IT units may also issue additional guidelines, procedures, or other requirements as necessary to secure departmental IT Resources which are to be remotely accessed. Specific reference materials for implementing security measures may vary from campus to campus or department to department.

In the event that an IT 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.

Violations of this policy may result in disciplinary action or sanctions in accordance with university policy and procedures and applicable state and federal laws.
RELATED DOCUMENTS, FORMS, AND TOOLS

University IT policies:
www.calumet.purdue.edu/security/

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

Security Policy Exception Procedure:

HIPAA Privacy Compliance Office:
www.purdue.edu/hipaa/

HISTORY AND UPDATES

March 1, 2010: Significant revisions have been made to update this policy from its original interim version (issued May 24, 2005). It also has been formatted in the current policy template.

APPENDICES

There are no appendices to this policy.