PURDUE
UNIVERSITY

REMOTE ACCESS STANDARDS
Developed to support the implementation of the Remote Access to IT Resources policy (VII.B.4)

Issued March 1, 2010 from Purdue University Security Officer's Group and IT Networks and Security. Questions about this standard can be addressed to itap-securityhelp@purdue.edu.

I. Introduction:

It is the responsibility of Remote Users to ensure that reasonable measures have been taken to secure the Remote Host used to access Purdue University IT Resources. This standard applies to all Remote Users of Purdue University IT Resources including faculty, staff, students, outside contractors, vendors, and other agents.

II. Remote Access Security Standards

All Remote Users must follow the security requirements set forth in this standard for any Remote Host accessing IT Resources prior to such access, as well as any guidelines, procedures, or other requirements issued by their departmental IT units and/or the owners of the IT Resource which are to be remotely accessed.

Remote User responsibilities are described below:

Remote User Requirements:

- Remote Users must ensure that their Remote Hosts used to access University IT Resources meet all security expectations specified in the End User Security Guidelines prior to accessing any University IT Resource.
- It is the responsibility of Remote Users to take reasonable precautions to ensure their remote access connections are secured from interception, eavesdropping, or misuse.

All Remote Users are responsible for following applicable University policy, including the University's Data Handling Requirements, when handling any Purdue University data remotely accessed within the course of the Remote User's job function at Purdue University. Policies to follow and actions to perform include, but are not limited to:

- All Remote Users are expected to only remotely access data in accordance with Purdue University IT policies.
- Do not save or store University sensitive or restricted data on the Remote Host used to access University IT Resources.
- Where applicable, all Remote Users are also responsible for following any guidelines issued by the HIPAA Privacy Compliance Office for remote access to Protected Health Information accessed within the course of the Remote User's job function at Purdue University.

PURDUE UNIVERSITY

III. Related References

- Remote Access to IT Resources policy (VII.B.4), available at: http://www.purdue.edu/policies/information-technology/viib4.html
- University IT Policies are available at: http://www.purdue.edu/policies/information-technology.html
- Standards supporting the implementation of University IT Policies are available at: http://www.purdue.edu/securepurdue/bestPractices/
- End User Security Guidelines, available at: http://www.purdue.edu/securepurdue/bestPractices/endUserSecurityGuidelines.cfm
- HIPAA Privacy Compliance Office: http://www.purdue.edu/hipaa/
- Purdue University Data Classification and Handling Requirements, available at: www.purdue.edu/securepurdue/bestPractices/dataClass.cfm
- Purdue Virtual Private Network (VPN) information, available at: http://www.itap.purdue.edu/connections/vpn/

Revised November 21, 2011 to update URLs.