College of Agricultural Sciences --- Remote Access Policy: ITP-004

1.0 Purpose

The purpose of this policy is to define standards for connecting devices to the College of Agricultural Sciences' network.

2.0 Scope

This policy applies to all College of Agricultural Sciences employees, contractors, consultants, temporary personnel, and other workers or students with a College of Agricultural Sciences-owned or personally-owned computer or workstation used to connect to the College of Agricultural Sciences network. This policy applies to remote access connections used to do work on behalf of the College of Agricultural Sciences, including reading or sending email (via email client or Web browser), remote access to college documents or internal services, and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, Remote Desktop, PC Anywhere, and cable modems.

3.0 Policy

Remote access policy standards are designed to minimize the potential exposure to the College from damages which may result from unauthorized use, or insecure access of College resources. Damages include the loss of sensitive or confidential institutional data, intellectual property, damage to public image, and damage to critical College of Agricultural Sciences' internal systems.

3.1 General

1. It is the responsibility of the College of Agricultural Sciences employees, contractors, vendors and agents with remote access privileges to the College of Agricultural Sciences' network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the College of Agricultural Sciences. Access and control will be enforced via the Penn State University or College of Agricultural Sciences' VPN gateway.

3.2 Requirements

1. Any devices connecting to the College of Agricultural Sciences network must do so via an approved VPN service.
2. All devices that are connected to the College of Agricultural Sciences internal networks via remote access technologies must use the most up-to-date antivirus software.
3. Personal equipment that is used to connect to the College of Agricultural Sciences' networks must meet all the requirements of College of Agricultural Sciences-owned equipment for remote access.
4. Organizations or individuals who wish to implement non-standard Remote Access solutions to the College of Agricultural Sciences production network must obtain prior approval from the College of Agricultural Sciences' security team.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, by their Administrative unit, the College, or the University.

5.0 Supporting Documents

NA

6.0 Revision History

Last updated: 12/14/2009