College of Agricultural Sciences --- PII Scanning Policy: ITP-009

1.0 Purpose

The purpose of this policy is to define the scanning requirements of college computers for the presence of Personally Identifiable Information (PII). This policy further provides the authority for members of the College's security team and the University's Security Office to audit remediation efforts for college computers to ensure compliance with relevant university and college policies.

2.0 Scope

This policy applies to all university-owned computers, any computer connected to a non-student segment of the university/college network, any computer storing university data, or the data itself. University-owned computers is defined as any computer acquired using university general funds or grant funds administered through the university. Non-student college network segments include all university networks not dedicated to student-only use, university wireless networks, and county extension office networks. University-owned computers which may be located at non-campus, commercial, or residential locations are subject to the provisions of this policy. PII is defined as social security numbers, credit card numbers, driver's license numbers and bank account information.

3.0 Policy

The storing of PII on a university sytem is prohibited by university policy unless a special exception has been granted by the university's Chief Privacy Officer. The elimination of PII from university systems protects the university's students, stakeholders, alumni, and employees. Eliminiation of PII greatly reduces the financial and negative publicity liabilities associated with PII breaches. All university-owned computers and computers defined in the Scope section must be scanned for the presence of PII on a regular basis using a university-approved scanning application. Scans should be performed every 2 weeks and at least every 30 days. Scanning results must be remediated during that same time period by one of the following:

1. Deletion of files that contain PII data.
2. Purging of the PII data from the files.
3. Marking the findings as "false positives".

It is the responsibility of the employee to which a computer is assigned or the individual responsible for the data (in the case of shared drives or folders) to ensure that the scans and remediation efforts are performed during the timeframe described above. Members of the College or University security team are authorized to monitor scanning logs in accordance with college IT policy ITP-003 Audit Policy. The security team **may** notify users or unit leaders of instances of non-compliance but are not required to.

4.0 Enforcement

Costs associated with PII notifications will be the responsibility of the unit to which the user of the compromised system reports. Anyone found violating this policy may be subject to disciplinary action by his or her Administrative unit, the College, or the University. College or University Security Office personnel may block network access to any system that has not performed a scan or remediated results within the above time periods.

5.0 Supporting Documents

College policy ITP-001 Acceptable Computer Use
College policy ITP-003 Audit
University policy FN07 Credit Card Sales
University policy AD11 University Policy on Confidentiality of Student Records
University policy AD19 User of Penn State Identifier and Social Security Number
University policy AD20 Computer and Network Security
University policy AD22 Health Insurance Portability and Accountability Act (HIPAA)
University policy AD23 Use of Institutional Data
University policy AD35 University Archives and Records Management
University policy AD53 Privacy Statement

6.0 Revision History

Last updated: 11/9/2010