



Information Privacy and Security (IPAS) Phase I Project Activity

1. Work with ATW to make eCommerce site and Bursar's compliant with PCI DSS. Due to deadline of December 31st for Bursar to be compliant.
2. Develop Reference Architecture Documents with ATW to be used as the base "template" or list of requirements for departments using eCommerce. Will be based on nature of interface, operating system, etc. and implementation will be mandatory.
3. Privacy and Security Project awareness training for Budget Executives. To include a request for assignment of Administrative, Technical, and Financial Officer contacts for each merchant to be responsible for PCI DSS compliance effort.
4. PCI DSS awareness training for all credit card merchants at Penn State. (Administrative, Technical, and Financial Officer contacts will require training as dictated by ATW recommendations.)
5. PCI DSS technical training and instructions for technical contacts.
6. Asset Inventory Documentation for each Merchant to include:
 - a. Contact list (Administrative, Technical, Financial Officer)
 - b. Technical information on machines that process credit
 - c. Network diagram to include flow of credit card transactions.
 - d. Additional inventory details as determined by PCI DSS ATW
7. Security Testing and Assessment
 - a. Vulnerability scans by SOS and ATW
 - b. Web application scans, if applicable
 - c. Additional testing as recommended by ATW
8. Gap Analysis with PCI DSS list of requirements (includes review of technical and physical controls, etc.)
9. Policy and Procedure Review at Penn State and departmental level
10. Risk Analysis with results from security testing and PCI Gap Analysis
11. Remediation Plan options. Remediation Plans will be at departmental level, but will also include Penn State-wide suggested solutions that may include:

- a. Broader security strategies that may improve overall security posture (network infrastructure changes, etc.) that would provide technical economies of scale.
- b. Analysis of central security services versus distributed (especially for IDS/IPS, logging, firewall service, etc.)
- c. Central credit card processing versus distributed, etc.

12. Final Prioritized Remediation Plan for each department and Penn State overall

13. Initiation of Remediation Plan and on-going Progress Reporting