**Treasury Operations**

Contact

* Robert Carter, Director, Business Operations 202-885-2715

The Department of Treasury Operations within the Office of Finance and Treasurer provides cash management services to the university community by overseeing the university's liquidity, which includes initiating electronic payments for university obligations. The department assists with debt management, and the administration of credit card acceptance for goods and services, including assigning merchant ID numbers. Treasury Operations also administers the university's endowment and works with its broker to manage donor stock gifts. The department serves as the primary liaison between banks, financial institutions, credit card processors, and the university.

**Office of Information Technology Information Security Team**

Call the help desk to schedule a security consultation 202-885-3998

Call us using our direct lines:

* Cathy Hubbs, Chief Information Security Officer 202-885-3998
* Eric Weakland, Director, Information Security 202-885-2241

**Information Security Team**

OIT's information security team supports AU's executive leadership and community by evaluating digital information assets for sources of risk throughout the IT planning, implementation, management, and ongoing operation phases. The group translates discovered risks into business terms to help stakeholders determine whether to accept, deter, fix, or transfer those risks.

The team works to accomplish this through:

* Ensuring compliance with applicable policies, laws, and regulations
* Enforcing university policies and standards
* Implementing technologies that increase the visibility of potential risks to our data
* Developing repeatable processes that validate security in IT systems and services
* Contributing to awareness, training, and education programs
* Initiating partnerships with departments to evaluate and improve their computer security practices
* Working with its IT partners to safeguard new technologies and services
* Applying the principles of in-depth defense when employing solutions investigating and responding to security incidents

**The Payment Card Industry Data Security Standard (PCI DDS) is…**

a contractual obligation, an industry standard, and a set of international requirements for protecting customer credit card data. The standard is refreshed every three years. Compliance with PCI DSS version 3 will begin January 2015.

**American University's Cardholder Data Security Policy (**www.american.ed/policies)

“This policy applies to all American University faculty, staff, students, and organizations that handle electronic or paper documents associated with credit or debit card receipt transactions who accept payments in the form of credit or debit cards. The scope includes any credit or debit card activities conducted at all American University campuses and locations….The Assistant Vice President of Treasury may terminate credit and debit card collection privileges for any department in compliance with this policy.”

**What Does Treasury Operations Do to Assist with PCI Compliance?**

* Acts as the primary point of contact for campus questions relating to credit card processing and securing cardholder data
* Reviews requests for and assigns merchant IDs
* Ensures campus merchants review the Cardholder Data Security Policy and sign the confidentiality agreement
* Provides ongoing training for cardholder data security
* Manages relationship with AU's processor ACI/Official Payments
* Assists with purchase, installation, maintenance, and replacement of POS hardware devices used for card data processing
* Coordinates collection of answers for self-assessment questionnaire (SAQ)
* Contacts AU's quality security assessor (QSA) for assistance with translations of PCI DSS and its specific applications to American University's environment, including contractual language required for third-party service providers

**What Does OIT Information Security Do to Assist with PCI Compliance?**

* Partners with Treasury Operations to support understanding of technology requirements
* Assists campus partners and their technology vendors to determine compliance requirements to protect PCI-covered data
* Partners in the creation and delivery of security awareness materials and events as needed
* Contacts AU's QSA for assistance with translations of PCI DSS and its specific applications to AU's environment
* Monitors and test technology controls meant to safeguard PCI-covered data on the AU network
* Translates technology sections when completing annual SAQ
* Prepares quarterly system scan reports
* Coordinates annual penetration testing

**Resources**

* [EDUCAUSE Higher Education Information Council's Credit Card Data Wiki](https://wiki.internet2.edu/confluence/display/2014infosecurityguide/Credit%2BCard%2BData)
* [Official Source of PCI SSC Data Security Standards](https://www.pcisecuritystandards.org/security_standards/)
* [List of Validated Payment Applications](https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php)