UH PCI Technical Guidelines

Foundational Principles:

- UH network is an **UNTRUSTED** and public network – both wired and wireless IP connections.
    - **UH Network IS NOT PCI COMPLIANT.**
- Isolate devices used for PCI transactions from the UH network to minimize scope of PCI compliance
    - Use network segmentation – implement a firewall or router to separate devices used for PCI transactions from the rest of the Merchant's department/campus network
- Devices used for PCI transactions should not be used for any other purposes (do not use devices for email, web browsing, or any other department uses)
- Minimize scope:
    - Minimize the number of devices used to process PCI transactions
    - Minimize the number of people handling PCI transactions

Requirement #1: Install and Maintain a firewall configuration to protect cardholder data

- Implement firewall rules or router ACLs to prevent lateral movement between segments
- Document & vet firewall rule changes
- Maintain a current network diagram
- Maintain a current data flow diagram for PCI-related transactions
- Use private IP addresses if possible (maintain NAT logs)

Requirement #2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Change ALL default passwords **before** connecting PCI devices/computers to any network
- Remove/disable unnecessary default accounts **before** connecting to any network
- Secure default settings and configurations **before** connecting to any network
- Implement system hardening standards (e.g. NIST, CIS, ISO, etc.)
- Ensure that PCI data is encrypted at rest and in transit
- Maintain inventory of system components that are in scope for PCI-DSS

Requirement #3: Protect stored cardholder data

- If at all possible, do not retain cardholder data (even if encrypted)
- If you do need to retain cardholder data, you must:
    - Encrypt the data
    - Have a specific retention requirement
    - Have a data retention policy & schedule that includes a quarterly process for identifying and destroying data beyond the retention period
    - Securely destroy data at the end of the retention period (both paper and electronic)

- Check that cardholder data is NOT included in log, history files, database contents/schemas, etc.
- Implement key management procedures to protect encryption keys

Requirement #4: Encrypt transmission of cardholder data across open, public networks (note: UH wired & wireless networks are open, public networks)

- UH guidance: Do not use UH-developed web applications to collect cardholder data - use PCI approved services & devices for credit card collection and processing
- All UH web pages collecting any information should use trusted keys or certificates (HTTPS)
  - Certificate information for UH departments: http://www.hawaii.edu/sitelic/incommon/

Requirement #5: Protect all systems against malware and regularly update anti-virus software or programs

- ITS provides anti-virus for free: http://www.hawaii.edu/askus/1254
- Enable automatic updates and automatic scanning; retain audit logs are required to be maintained
- Regularly check that anti-virus software is running and cannot be disabled

Requirement #6: Develop and maintain secure systems and applications

- Ensure that automatic updates are enabled for both operating system and applications
- Scan systems for vulnerabilities monthly
- Ensure that only required applications are installed and running on the systems that are used for PCI transactions
- If using home-grown/custom software or web applications to process PCI transactions, you must have a written software development life cycle process based on industry standards that includes implementation of information security processes and vetting, change management, separate test/development environment from production, verifying that live PAN data is NOT used for testing, vetting that application is not vulnerable to common exploits, etc.
- Merchant's must only use PCI DSS validated third-party service providers. The University has implemented a PCI DSS compliant, hosted eCommerce management system. Merchant departments shall use this designated third party system or apply for exception by completing Appendix B, Item G

Requirement #7: Restrict access to cardholder data by business need to know

- "Need to know" is when access rights are granted to only the least amount of data and privileges need to perform a job
- Minimize the number of people handling PCI transactions

- If possible, establish separate user accounts for each person handling PCI transactions to provide accountability and an audit trail
- Never share accounts
- Separate system administrator accounts from user accounts

Requirement #8: Identify and authenticate access to system components

- Each person must be assigned a unique account for accountability and audit purposes
- Establish & document onboarding, offboarding, and access controls procedures for any personnel handling PCI transactions including mandatory training, and revocation of accounts/access for both inactivity or separation from service
- Monitor accounts for unauthorized access and access attempts
- Establish & document secure account management procedures following industry best standards (e.g. strong passwords/MFA, auto lockout/logoff for idle sessions, etc.)

Requirement #9: Restrict physical access to cardholder data

- Secure physical areas or physical devices where PCI transactions are conducted & limit access to only authorized personnel
- Prevent unauthorized connections to PCI network environment
- Prevent unauthorized use of devices used to process PCI transactions
- Implement & document procedures for “visitors”
- Physically inventory & secure all media involved in processing PCI transactions; maintain current inventory list
- Use secure destruction methods when decommissioning devices/equipment used to process PCI transactions
- Provide annual training for all personnel involved in processing PCI transactions

Requirement #10: Track and monitor all access to network resources and cardholder data

- Maintain and review audit trails regularly (e.g. firewall/router logs, system event logs, user logs, web logs, etc.)
- Retain logs for a minimum of 3 months
- Ensure that time stamps are accurate (enable NTP if possible)
- Limit access to logs to authorized individuals
- Ensure logs are backed up and test backups

Requirement #11: Regularly test security systems and processes

- If possible, DO NOT USE wireless networks
- If you must use wireless networks:
    - **DO NOT USE the UH wireless network!!!**
    - Ensure that access to the wireless network is only available to devices used to process PCI transactions (e.g. hidden, non-default SSID, only allow authorized MAC addresses to connect to AP, etc.)

    - Maintain and review access point logs
    - Maintain an inventory of authorized wireless access points, connected devices AND a documented business purpose
- For all networks used for PCI transactions:
    - Regularly scan network for devices and vulnerabilities
    - Implement a methodology for penetration testing (pen testing) based on industry standards (e.g. NIST SP800-11)
    - Perform external & internal pen testing at least annually or after significant changes were made to the PCI environment; validate that segmentation is operational and effective

Requirement #12: Maintain a policy that addresses information security for all personnel

- Review the appropriate SAQ and ensure that all processes and procedures are documented
- Develop and maintain an appropriately sized information security policy