

COMPLIANCE TIMELINE FOR SAQ D (PARTIAL)

1st Quarter

- Employee Training (12.6.1/12.9.4) [A]
 - Acknowledgement of Campus Merchant Bank Cards Acceptance Agreement (FRS Policy 8.14) [A]
 - Employee Acknowledgement of Security Policy (12.6.2) [A]
 - Risk Assessment [A] (12.1.2)
 - Firewall and Router Rule Review (1.1.6) [S]
 - Vulnerability Scan (11.2) [Q]
 - Wireless Access Point Test (11.1) [Q]
 - Removal/Disabling of Inactive User Accounts (8.5.5) [Q]
 - Stored Cardholder Data Review (3.1) [Q]
 - User Password Change [Q] (8.5.9)
-

2nd Quarter

- Electronic Cardholder Data Search [A] (Optional)
 - Back-Up Media Inventory and Security Review of Off-Site Storage Facility (9.5/9.9.1) [A]
 - Web Application Security Scan (6.6) [A]
 - Vulnerability Scan (11.2) [Q]
 - Wireless Access Point Test (11.1) [Q]
 - Removal/Disabling of Inactive User Accounts (8.5.5) [Q]
 - Stored Cardholder Data Review (3.1) [Q]
 - User Password Change [Q] (8.5.9)
-

3rd Quarter

- Incident Response Plan Test (12.9.2) [A]
 - Penetration Test (11.3) [A]
 - Firewall and Router Rule Review (1.1.6) [S]
 - Vulnerability Scan (11.2) [Q]
 - Wireless Access Point Test (11.1) [Q]
 - Removal/Disabling of Inactive User Accounts (8.5.5) [Q]
 - Stored Cardholder Data Review (3.1) [Q]
 - User Password Change [Q] (8.5.9)
-

4th Quarter

- Assessment Preparation [A]
- Security Policy Review (12.1.3) [A]
- Vulnerability Scan (11.2) [Q]
- Wireless Access Point Test (11.1) [Q]
- Removal/Disabling of Inactive User Accounts (8.5.5) [Q]
- Stored Cardholder Data Review (3.1) [Q]
- User Password Change [Q] (8.5.9)
- Assessment [A]

Ongoing

- Network Diagramming (11.2)
- Antivirus Software Use (5.2)
- Critical Security Patch Installation (6.1)
- Revocation of Access for Terminated Users (8.5.4)
- Disabling of Vendor Accounts for Remote Maintenance (8.5.6)
- Destruction of Media With Unneeded Cardholder Data (9.10)
- Updating Intrusion Detection/Prevention Engines (11.4)