PCI Best Practices

General (Servers & desktops)

- Establish policies and procedures to limit the storage and retention time of PCI data.
- Provide for the physical security of systems & associated peripherals and ensure there is no unauthorized physical access to them including a requirement to lock workstation screens when leaving the work area.
- Restrict data transfers to/from PCI systems.
- Regularly backup critical systems and data and ensure integrity and usability of backups.
- Implement detailed system and security logging of important events for all system components.
- Ensure that all users have and use unique accounts for logging onto computer systems. Group, shared or generic accounts and passwords are prohibited.
- Regularly review system security and audit logs.
- Prohibit non-encrypted transmission of sensitive cardholder data.
- Assign an individual to be responsible for information security management responsibilities.
- Ensure anti-virus, anti-spyware and anti-malware software is installed on all systems, that it is operational, and is regularly updated.
- Ensure timely installation of updates and patches to operating system and application software.
- Implement regular management reviews to insure compliance with relevant policies and standards.
- Enable Network Time Services (NTP) or similar technology on all systems to provide synchronized clocks across all systems for consistent event logging and tracking. (this should be the default for system utilizing Cougarnet/Active Directory).
- Ensure proper disposal of equipment.
- Destroy media containing cardholder information when it is no longer needed for business or legal reasons.

Servers

- Provide separate environments for development/test and production.

- Establish change control processes for application software updates and system changes; Evaluate security impact of proposed system, application and network changes. Ensure recovery process in the event changes are unsuccessful or unsatisfactory.

- Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users. Ensure logging is in place to audit all actions taken by those with elevated access as well as users who connect to databases directly rather than by means of applications.

- Use accepted security standards in development of PCI application software.

- Remove all unnecessary functionality (services and protocols not directly needed to perform the devices' specified functions), such as scripts, drivers, features, subsystems, file systems, and unnecessary and insecure services and protocols.

- Store back-up media in a secure location. Off-site copies of backup media should be sent to a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.