PCI Requirements for Nelnet Users

Current PCI compliance requirements that will allow you to continue using SAQ-A under normal circumstances (Note that PCI compliance can change frequently and the information provided become outdated):

Server Related

- All UMD websites must be hosted on a DIT managed server or a PCI compliant service provider. Implement one primary function per server to avoid functions requiring different security levels co-existing on the same server.
- If a UMD website is hosted externally, the server must be in a monitored secure location.
- Operating system and application software versions must be supported by the vendor.
- The hosting provider must be a validated hosting provider within the last year.
- Security patches installed within one month of release.
- 2-factor authentication to the web server for administrative and developer access (including 90 day password changes, no reuse of old passwords allowed).
- Vendor access to the server should only be allowed for maintenance and support.
- File integrity monitoring (FIM) of the operating system, web server and application (i.e. all static files).
- You may not process a credit card on behalf of a customer using a Virtual Terminal

Website Related

- Use HTTPS per Google certificate recommendations
  - 2048 bit
  - SHA-2
- Use TLS 1.2 or higher, no RC4 or fallback.
- Limit parameter information passed to Nelnet (i.e., Order Number, Order Type, Order Description, Amount Due, Redirect URL & parameters, Retries Allowed, Time Stamp and hash).

- **Other requirements:**

  Obtain AOC from web hosting provider annual

  Complete a SAQ-A

  Provide the website the URL’s are hosted on
Please remember that being the merchant you are responsible for all 12 Requirements of the PCI-DSS standard even if you currently qualify for the shorter SAQ A.