

TO: Sandy Lindsey

 University of Tennessee System Administration Information Security Office

FROM: <Marchant Point of Contact>

 <Marchant Name>

 <MID>

DATE: <date>

**SUBJECT: Risk Mitigation and Migration Plan for Payment Card Industry Data Security Standard (PCI DSS) V3.1 Requirements**

Please accept this document as the Risk Mitigation and Migration Plan for PCI DSS v3.1 for <*insert merchant name here>*. This plan covers PCI DSS Requirements 2.3 (e), 2.3 (f), 4.1 (f), and 4.1 (g).

A description of where and how we are currently using SSL and/or early versions of TLS, how we intend to mitigate the risks with these technologies, and our migration plan are listed below.

1. Where and how are SSL/early TLS currently used in your environment?

*<Insert description usage, including: what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment.>*

1. How are you mitigating risks with SSL/early TLS?

*<Insert description(s) of the level of risk with SSL/early TLS in your environment and the additional security controls you have put in place to mitigate these risks.>*

1. How are you monitoring for new vulnerabilities associated with SSL/early TLS?

*<Insert description(s) of the processes you are employing to monitor for new vulnerabilities associated with SSL/early TLS.>*

1. How are you ensuring that SSL/early TLS are not implemented into your cardholder data environment? (Meaning, how can you verify that new or upgraded systems connected to your cardholder data environment don’t contain SSL/early TLS?)

*<Insert description(s) of changes you are making in your processes to make sure that SSL/early TLS are not being implemented into any new environments.>*

1. When will your migration plan from SSL/early TLS be completed?

*<Insert the date when you expect to complete your migration from the SSL and/or early version TLS protocols.>*