globalpayments

DATA SECURITY UPDATE

Version 3.2.1 of the Payment Card Industry Data Security Standard (PCI DSS) is Here!

"Version 3.2 of the Data Security Standard will be retired as of 1st January 2019"

Version 3.2.1 (V3.2.1) of the PCI DSS was released in May 2018 and contains minor changes compared to V3.2. These mostly relate to dates in previous versions that have now passed together with details regarding the TLS/SSL (Transport Layer Security/Secure Socket Layer) Migration.

You can view the full version of the standard by visiting the Document Library of the PCI Security Standards Council (PCI SSC) website or by clicking **here**. However, you (and any third parties you use to accept card payments) must validate themselves against this new version. Over the page, you'll find a table that details the changes that you need to familarise yourself with.

As with previous versions of the PCI DSS, there'll be a transitional period to allow you sufficient time to move to the new version, as well as to complete any assessments that are already in progress. Until 31st December 2018, you'll be able to validate your PCI DSS compliance against either V3.2 or V3.2.1. However, V3.2 will be retired on 1st January 2019 and you'll only be able to validate your compliance using V3.2.1 after this date.

Supporting documents have also been updated and can be found on the PCI SSC's Document Library. These include:

- Self-Assessment Questionnaires (SAQ) and guidelines,
- Report on Compliance (ROC),
- Prioritised Approach Tool.

If you have any queries regarding the revised standard, please contact your Relationship Manager or call us on 0345 702 3344*, selecting the option for 'all other enquiries'.

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. To help us continually improve our service, and in the interests of security, we may monitor and/or record your telephone calls with us. Any recording remains our sole property. We also provide a Textphone service on 0345 602 4818.

Service. Driven. Commerce

PCI DSS V3.2.1
Summary of Changes

PCI DSS V3.2 Clauses	PCI DSS V3.2.1 Clauses	Change
2.2.3 2.3 4.1	2.2.3 2.3 4.1	Removed note and testing procedure regarding use of Appendix A2 to report SSL/early TLS migration effort as the migration date has passed. Added note to guidance referencing updated applicability of Appendix A2.
3.51. 6.4.6 8.3.1 10.8, 10.8.1 11.3.4.1 12.4.1 12.11, 12.11.1	3.5.1 6.4.6 8.3.1 10.8, 10.8.1 11.3.4.1 12.4.1 12.11, 12.11.1	Removed note from requirements referring to an effective date of February 1, 2018 as this date has passed.
3.6.2	3.6.2	Fixed error in Guidance Column – Reference to Requirement 3.5.1 changed to 3.5.2.
Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS	Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present Point of Sale/Point of Interaction (PoS/PoI) terminal connections	Updated Appendix A2 to reflect that the SSL/early TLS migration date of July 1, 2018 has passed. Requirements A2.1 – A2.3 updated to focus only on the allowance for POS POIs that aren't susceptible to known exploits and their service provider termination points to continue using SSL/early TLS.
Appendix B: Compensating Controls	Appendix B: Compensating Controls	Replaced reference to Navigating Guide with Guidance Column for understanding intent of requirements. Removed Multi-Factor Authentication (MFA) from the compensating control example as MFA is now required for all non-console administrative access. Added use of one time passwords as an alternative potential control for this scenario.