Guidance for Requirements 3 and 4: Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms for definitions of "strong cryptography" and other PCI DSS terms.

Requirement	Guidance
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows. **3.1.1** Implement a data retention and disposal policy that includes: ▪ Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements ▪ Processes for secure deletion of data when no longer needed ▪ Specific retention requirements for cardholder data ▪ A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements	A formal data retention policy identifies what data needs to be retained, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. In order to define appropriate retention requirements, an entity first needs to understand their own business needs as well as any legal or regulatory obligations that apply to their industry, and/or that apply to the type of data being retained. Extended storage of cardholder data that exceeds business need creates an unnecessary risk. The only cardholder data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. Implementing secure deletion methods ensure that the data cannot be retrieved when it is no longer needed. **Remember, if you don't need it, don't store it!**