Sabre Red Apps Security Information

6 February 2018

Red App Security Information

If your *Red App* will handle cardholder or personal information, you are required to include this information when you submit your *Red App* to *Sabre* for certification:

- A comprehensive dataflow diagram for the *Red App* and a detailed description of the flow of sensitive (cardholder or personal) data, including all access points into the *Red App* (for example, can it be accessed outside of the *Red App* Workspace) and any connectivity between the application and other entities (such as other *Red Apps*, *Sabre Red Workspace*, emulator, host, web services, etc.).

- A description of all PCI data that the Red App processes, stores, or transmits:

    - Primary Account Number (PAN)
    - Cardholder Name
    - Service Code
    - Expiration Date
    - Magnetic Stripe Data
    - CVV/CVC Data
    - PINs/PIN Blocks
    - Any Track-1 or Track-2 Data

- A description of all Personal Data that the Red App processes, stores, or transmits (refer to Security Policy ITS105 Data Protection):

    - Social Security Number
    - Driver's License Number
    - Passport Number
    - Date of Birth
    - Address, phone number, country of National Identification, etc.

- A description of how GDPR compliance is managed

- A description of how the PAN is rendered unreadable everywhere it is stored.

- A description of the method of strong cryptography and security protocols (encryption algorithms and key strengths) used wherever cardholder or personal identifying data is stored, transmitted, or received over open, public networks (such as SSH, VPN, IPSEC or SSL/TLS).

- A description of which secure coding guidelines are followed, such as OWASP Top 10.

- A description of the retention period and purging process for any stored cardholder or personal identifying data.