Office of the Secretary of State
Washington State Archives

Records Management Advice
Issued: September 2020
(Originally Issued: December 2014)

Using Records Retention Schedules:
Strategies for Managing Sensitive Payment Cardholder Data

Purpose: Provide guidance to state agencies and local governments on managing sensitive cardholder data obtained during payment card transactions in order to minimize public and agency risk.

State and local government agencies need to destroy Sensitive Cardholder Data as soon as a payment card transaction is complete, in order to comply with the Payment Card Industry (PCI) Security Standards Council's current Data Security Standard (PCI DSS).

Sensitive Cardholder Data consists of the:

1. Sensitive Authentication Data (such as the Card Verification Value (CVV)/Card Validation Code (CVC) found on the front or back of the card and/or encoded in the magnetic strip); and the
2. Entire Primary Account/Credit Card Number.

This destruction of sensitive cardholder data is authorized by the records series **Financial Transactions – Sensitive Cardholder Data (DAN GS 01070 / GS2014-030)** in both the *State Government General Records Retention Schedule* and the *Local Government Common Records Retention Schedule (CORE)*.

Here are some basic strategies that can be used:

Point Forward

1. Keep the sensitive cardholder data separate (or easily separable) from the rest of the transaction record, or do not record it at all (whenever possible); and
2. Document this approach in agency procedures.

Cleaning Up the Backlog

For existing records where sensitive cardholder data is part of the transaction record, strategies include:

1. Database records – deleting sensitive cardholder data (including from backups).
2. Paper records – physically removing or permanently redacting the sensitive cardholder data.
3. Email records – electronically redacting the sensitive cardholder data.