Best Practices

1. Eliminate electronic storage of cardholder data. Never collect, enter, or store cardholder information. Credit card information must not be stored directly on the agency's webpage nor entered onto their website.
2. Implement proper destruction methods.
3. Use Online Payment Card Systems Appropriately. Many departments use third-party payment systems or gateways to outsource online payment card processing. Customers should be directed to complete payments online using these applications.
4. Never email credit card information
5. Always authenticate a Payer before discussing cardholder information.
6. When an item or service is purchased using a credit card, and a refund is necessary, the refund must be credited to the same credit card account from which the purchase was made.
7. Limit and monitor physical access to systems that store, process, or transmit cardholder data.
8. Secure the processing environment. The threat of Point of Sale (POS) terminal tampering is serious, as every day criminals attempt to install skimmers and other devices to capture cardholder data and create fraudulent cards. Ensure all POS devices are secure and periodically inspect devices for tampering and/or substitution. Keep an inventory of all devices (with serial numbers) and train staff to look for abnormalities (broken seals, damage to the device, damage to external cables, etc.). You should also train staff to limit access to POS devices to only authorized individuals. Report any third-party individuals claiming to be repair or maintenance personnel immediately.
9. Keep duties related to processing cardholder information as separate roles (i.e., issuing refunds, processing receipts, etc.)
10. Improve oversight of third-party service providers. You cannot completely outsource your PCI compliance responsibility. It is important that you know and document all third-party service providers involved in payment card processing. It is also critical to ensure the appropriate contractual language is in place dictating which specific PCI DSS requirements are the responsibility of each entity. Assessing these vendors and service providers annually will ensure their compliance efforts are sufficient and protect your institution from any collateral damage should they suffer a data breach.
11. Implement a formal incident response plan.
12. Educate staff with PCI Training.
13. Agency's must report any actual or suspected security incident in which cardholder information may have been compromised to the State Controller's Office (SCO).