SALT LAKE COUNTY
COUNTYWIDE POLICY
ON
INFORMATION TECHNOLOGY SECURITY

Payment Card Industry Data Security Standard Policy

Purpose-

The purpose of this policy is to define the guidelines for accepting, storing, processing, or transmitting credit card information to comply with the Payment Card Industry's Data Security Standard (PCI-DSS). As merchants who handle cardholder data, Salt Lake County agencies are obliged to safeguard that data and adhere to the standards established by the Payment Card Industry Security Standards Council, including setting up controls for handling credit card data, ensuring computer and internet security, and completing an annual self-assessment questionnaire.

Reference-

The policy and standards set forth herein are provided in accordance with Section 3.10 of countywide policy 1400, which directs Salt Lake County Information Services to provide security systems and policies. Also reference the following:

All Countywide Information Technology Security Policies in the 1400 series
Countywide Policy - I062 Management of Public Funds
Countywide Policy - 1210 Refund of Payments Made Through Debit or Credit Cards
Countywide Policy - 2070 GRAMA Records Retention Scheduling Process
Salt Lake County Ordinance - Section 2.81 Security of Personal Identifiers
Salt Lake County Ordinance - Section 2.82 Records Management
Government Records Access and Management Act, §630-2-101 et.seq., Utah Code annotated

1.0 Scope

The scope of this policy includes any County Agency that accepts, stores, processes, or transmits credit card information (electronically or on paper), its employees, volunteers, or anyone else who has access to the Salt Lake County cardholder data environment, including contractors, consultants and others with a business association with Salt Lake County.

2.0 Definitions

Information Technology Resource(s) and/or System(s) (IT resource(s) and/or system(s))
Computers, hardware, software, data, storage media, electronic communications (including, but not limited to, e-mail, fax, phones, phone systems and voice mail), networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access, beyond ordinary public access to, the County's shared computing and network infrastructure.

County Agency Management
With respect to their own individual offices or departments, any of the following, or their designees: County Mayor, County Executive Branch Department Directors, County Elected Officials, or the County Council as a whole.

Payment Card Industry Data Security Standard (PCI-DSS)
A comprehensive set of security standards and best practices for securing cardholder data.

Self-Assessment Questionnaire (SAQ)
A validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard.

Attestation of Compliance *(AOC)*
A form completed by merchants at all levels declaring their compliance status with the Payment Card Industry Data Security Standard.

External Vulnerability Scan
A scan performed by an approved scan vendor (ASV) from outside the cardholder data environment looking for flaws or weaknesses which, if exploited, may result in an intentional or unintentional compromise of a system.

Service Provider
A business entity that is not a payment brand, who processes, stores, or transmits cardholder data on behalf of a County agency. This also includes companies that provide services that control or could impact the security of cardholder data.

Card Holder Data
At a minimum, the full Primary Account Number (PAN), plus any of the following:

- Cardholder name
- Expiration date
- Service code (3 or 4-digit value on magnetic-stripe that contains expiration date of the payment card)
- Magnetic-stripe (Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions)
- Card validation code (A security code visible on the back of the card)
- PIN ("personal identification number")
- PIN blocks (A block of data used to encapsulate a PIN during processing)

3.0 Policy Statement

Any County agency that accepts, processes, transmits or stores cardholder data using any County IT Resource or system shall comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. No activity may be conducted, nor any technology employed that might obstruct compliance with any portion of the PCI-DSS. County agencies that accept, process, transmit or store cardholder data shall develop internal practices and procedure to ensure compliance with the PCI-DSS.

3.1 PCI-DSS Compliance

PCI-DSS compliance requires among other things that County agencies that accept, process, transmit or store cardholder data shall:

3.1.1 Complete the appropriate annual SAQ and AOC for their merchant category.

3.1.2 Complete an annual external vulnerability scan performed by an approved scan vendor (ASV) if required by their merchant category. This scan can also be performed by Salt Lake County Information Services upon request.

3.1.3 Keep the current SAQ and AOC on file.

3.1.4 Be prepared to provide a copy of the SAQ and AOC to their payment processor upon request as verification of compliance.

3.1.5 Provide annual security awareness training to all agency employees. This training is available through County Information Services.

3.1.6 Maintain County records relating to PCI-DSS compliance and supporting documentation pursuant to GRAMA, County Ordinance 2.82 (2001), and approved county records retention schedules.

3.2 Service Providers

If a County agency utilizes a service provider to process payment card transactions, the County agency shall:

3.2.1 Maintain a list of service providers.

3.2.2 Maintain a written agreement between the County agency and the Service Provider that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.

3.2.3 Have an established process for engaging service providers, including proper due diligence prior to engagement.

3.2.4 Verify and monitor the PCI-DSS compliance status of all service providers.

4.0 Exceptions

4.1 Any exceptions to this policy must be explicitly approved in writing by County Information Services and shall be approved in conformance with Countywide Policy 1001.

5.0 Enforcement

County agencies that accept, process, transmit or store cardholder data will demonstrate their compliance with the Payment Card Industry Data Security Standard (PCI-DSS) annually to the County Auditor by September 30th of each year. Agencies found to be non-compliant will have a 6-month grace period to become compliant. County agencies that are deemed non-compliant after the 6-month grace period shall cease accepting, processing, transmitting, or storing cardholder data until such time that they are deemed compliant by the County Auditor.

5.1 Anyone found to have knowingly violated this policy shall be subject to disciplinary action, including but not limited to temporary loss of network connectivity, loss of

Internet access, or complete and permanent termination of access to any Salt Lake County Network and can lead to other disciplinary action, up to and including termination from County employment.

6.0 Education

County agencies are responsible to educate staff that work with cardholder data about this Policy.

APPROVED and ADOPTED this 26 day of June 2018.

SALT LAKE COUNTY COUNCIL

Aimee Winder Newton

Aimee Winder Newton, Chair

ATTEST:

Sherrie Swensen

Sherrie Swensen, County Clerk

APPROVED AS TO FORM:

Deputy District Attorney Date 6/12/18