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 payment card information to comply with the Payment Card Industry's Data Security Standard (PCI-DSS). Salt Lake County agencies that collect payment card revenue on behalf of the County and others who are in scope of this policy 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 Technology Division to provide security systems and policies. Also reference the following:

All Countywide Information Technology Security Policies in the 1400 series.
Countywide Policy - 1062 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, §63G-2-101 et.seq., Utah Code annotated.

1.0 Scope

The scope of this policy includes County agencies and other entities listed below that accept, store, process, or transmit cardholder data (electronically or on paper), their employees, volunteers, and 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.

1.1 County agencies that collect payment card revenue on behalf of the County

1.2 Outsourced contractors (see definition)

1.3 On-site contractors (see definition)

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 voicemail), 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.

Cardholder Data Environment (CDE)
The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.

Sensitive Authentication Data
Security-related information used to authenticate cardholders and/or authorize payment card transactions.

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 reporting tool used to document self-assessment results from an entity's PCI-DSS assessment.

Attestation of Compliance (AOC)
A form for merchants and service providers to attest to the results of a PCI-DSS assessment as documented in the SAQ.

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, that 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.

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

- Cardholder name
- Expiration date
- Service code
- Magnetic stripe (Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions)
- Card verification code
- PIN ("personal identification number")
- PIN blocks (A block of data used to encapsulate a PIN during processing)

Service Code
Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data.

Card Verification Code
For Discover, JCB, MasterCard, and Visa payment cards, the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the

code is a four-digit unembossed number printed above the PAN on the face of the payment card.

Outsourced Contractors
Non-County entities that accept, store, process, or transmit cardholder data (electronically or on paper) on behalf of the County, using either the County's IT systems or resources or an independent IT system.

Onsite Contractors
Non-County entities conducting business on County property that use an independent IT system to process non-county payment card transactions.

3.0 Policy Statement

County agencies that collect payment card revenue on behalf of the County shall comply with the 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 collect payment card revenue on behalf of the County shall also develop internal practices and procedures to ensure compliance with the PCI-DSS.

3.1 PCI-DSS Compliance

PCI-DSS compliance requires among other things that County agencies that collect payment card revenue on behalf of the County will:

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 the County's Information Technology Division 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 the County's Information Technology Division.

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 that accepts payment card revenue on behalf of the County establishes a contract with an outsourced or onsite contractor 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 provider is 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. Due diligence may vary based on needs of the agency. At a minimum, due diligence should include how the service provider validates their PCI-DSS compliance, what evidence

of compliance the service provider will make available, information on which PCI-DSS requirements are the responsibility of each party, and service provider breach notification practices. Agencies shall maintain evidence of due diligence performed

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

3.2.5 Maintain information about which PCI-DSS requirements are managed by each service provider, and which are managed by the entity.

3.3 Outsourced Contractors and Onsite Contractors

3.3.1 County agencies that establish agreements with outsourced contractors will ensure that written agreements include requirements for compliance with this policy and with PCI-DSS standards.

3.3.2 County agencies that establish agreements with onsite contractors will ensure that written agreements include requirements for PCI-DSS compliance.

4.0 Exceptions

4.1 Any exceptions to this policy must be explicitly approved in writing by the County's Information Technology Division and shall be approved in conformance with Countywide Policy 0002 "Policy Enactment, Maintenance, and Implementation."

5.0 Enforcement

County agencies that collect payment card revenue on behalf of the County will demonstrate their compliance with PCI-DSS annually to the County Auditor by September 30th. County agencies found to be non-compliant will have a 6-month grace period to become compliant.

5.1 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.

5.2 Any County employee 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 that collect payment card revenue on behalf of the County are responsible for educating staff that work with cardholder data about this Policy.

APPROVED and ADOPTED this _____day of _____,2020.

SALT LAKE COUNTY COUNCIL:

By _____
Chairperson

ATTEST:

_____

Sherrie Swensen, County Clerk

APPROVED AS TO FORM
Salt Lake County
District Attorney's Office
Dianne Orcutt
Digitally signed by Dianne Orcutt
Date: 2020.07.27 09:59:18 -06'00'