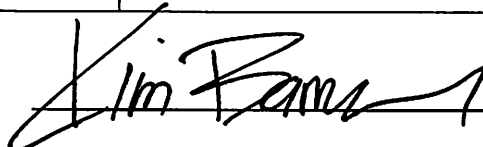


Mayor's Office: Council Agenda Item Request Form
*This form and supporting documents (if applicable) are due the Wednesday
before the COW meeting by noon.*

Date Received (office use)	3 February 2017
--------------------------------------	------------------------

Date of Request	1/24/2016
Requesting Staff Member	Mark Evans
Requested Council Date	28 February 2017
Topic/Discussion Title	Update of Countywide Policy 1400-7
Description	Salt Lake County established a Countywide policy (1400-7) that requires any County agency that accepts payments by credit or debit card to be in compliance with the Payment Card Industry Data Security Standard (PCI-DSS.) This is also a requirement of the agreement they complete with the merchant bank that processes their payment transactions. I am proposing the addition of a new enforcement section that describes what happens in the event an agency does not remain compliant with the PCI-DSS. I am also asking the County Auditor to handle the verification of compliance on an annual basis going forward.
Requested Action¹	Approval of policy update.
Presenter(s)	Mark Evans
Time Needed²	10 minutes
Time Sensitive³	No
Specific Time(s)⁴	No
Contact Name & Phone	Mark Evans – X80666
	See attached approved as to form policy and a letter from the County Auditor indicating his support for this update in the policy.

Mayor or Designee approval:



¹ What you will ask the Council to do (e.g., discussion only, appropriate money, adopt policy/ordinance) – in specific terms.

² Assumed to be 10 minutes unless otherwise specified.

³ Urgency that the topic to scheduled on the requested date.

⁴ If important to schedule at a specific time, list a few preferred times.



SCOTT TINGLEY

CIA, CGAP

Salt Lake County Auditor

STingley@slco.org

CHERYLANN JOHNSON

MBA, CIA, CFE

Chief Deputy Auditor

CAJohnson@slco.org

2001 S State Street, N3-300

PO Box 144575

Salt Lake City, UT 84114-4575

(385) 468-7200; TTY 711

(385) 468-7201 / fax



MEMORANDUM

TO: The Honorable Sim Gill, Salt Lake County District Attorney

CC: Ralph Chamness, Chief Deputy District Attorney
Kelly Wright, Unit Chief, Deputy District Attorney
Beth Overhuls, Chief Information Officer
Mark Evans, VP/Information Security Officer
Anita Kasal, Audit Manager

FROM: Scott Tingley, Salt Lake County Auditor *St*

DATE: Friday, January 6, 2017

SUBJECT: County Auditor's approval of recommended updates to County Wide Policy 1400-7, Payment Card Industry Data Security Standard Policy

The County Auditor's Audit Services Division has been engaged in a special project in collaboration with the Information Services Division ("IS"), facilitating the annual Payment Card Industry's ("PCI") Data Security Standard ("the Standard") Self-Assessment Questionnaire ("SAQ") process throughout the County. All County agencies that process credit or debit card transactions are required to comply with the Standard, and the first step towards compliance is completing an annual SAQ and an Attestation of Compliance ("AOC"). The requirements of the Standard help to ensure that cardholder data processed or stored on County IT systems and databases is protected and secure.

Our work was based on a Memorandum of Understanding ("the MOU"), between the County Mayor and the County Auditor, dated July 15, 2015. One of the Auditor's main roles and responsibilities in the MOU, was to assist County agencies that accept payment cards to complete their SAQ and AOC on a yearly basis. The Auditor is an independent and objective third-party, who can verify County compliance with the Standard, and provide proper segregation of duties in the SAQ and AOC process.

I am happy to report that we had great success with the project. However, through our work, we found that County Wide Policy 1400-7, as it is currently written, lacks a mechanism for holding County agencies accountable for the SAQ and AOC process, and even the Policy itself.

Specifically, one of the County agencies that processes payment card transactions, refused to complete an SAQ and AOC in 2016, despite a year-long effort by the Auditor and IS to get them to do so. Division management, and the Department Director were notified several times about the issue, but in the end, the agency still has not completed an SAQ or AOC for 2016, as required by both the Standard and County Wide Policy 1400-7.

In situations like this, and when either the Auditor or IS determine that a County agency is not in compliance with the Standard, placing cardholder data at risk, County Wide Policy

1400-7, does not afford either the Auditor or IS a mechanism to enforce the Policy, or to allow County agencies due process for correcting the issues identified and become compliant. We recommend that County Wide Policy 1400-7, be updated to provide a mechanism to hold County agencies that process payment card transactions accountable, when they refuse to comply with the requirements of the Standard, or County Wide Policy 1400-7.

Mark Evans, from County IS, has drafted proposed updates to County Wide Policy 1400-7, and has forwarded them on to your office to be approved as to form:

5.0 Enforcement

5.1 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.

The purpose of this memo is to express my full support for the proposed changes to County Wide Policy 1400-7, and to acknowledge the County Auditor's role as outlined in the added language above. I believe that the next steps are to have the proposed changes approved as to form by your office, and then Mark was planning on presenting them to the County Steering Committee at the next scheduled meeting on January 23, 2017. If approved by the Steering Committee, the updates will then go before the County Council for their consideration.

Thank you for your time and attention to this matter. Please do not hesitate to contact me with any questions or concerns that you may have. By phone: (385) 468-7185, or by email: stingley@slco.org.

**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 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 – 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 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
- 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 employees that have access to cardholder data. 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 card holder data is shared with a service provider County agencies 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

- 5.1 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
- 5.2 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 dismissal from County employment

6.0 Education

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

APPROVED AS TO FORM
District Attorney's Office
By: *Dianne K. Orcutt*
Deputy District Attorney
DIANNE K. ORCUTT
Print Name
Date: *01/11/2017*