City of Imperial

Department of Information Technology

PCI Compliance Services

PCI DSS Policies and Procedures

Last update 04/17/2019

PCI DSS Policy

Department of Information Technology | PCI - COMPLIANCE SERVICES

The Payment Card Industry Data Security Standard (PCI DSS) is a required set of standards for optimizing the security of payment card transactions. A payment card is any credit, debit or prepaid card used in a financial transaction. The PCI DSS was developed by the PCI Security Standards Council, an organization founded by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. The standard applies to all organizations that process cardholder information. As such an organization, the City of Imperial's compliance with PCI DSS is mandatory.

By Payment Card Industry Data Security Standards (PCI DSS) requirements, the City of Imperial, Department of Information Technology (DoIT) "PCI Compliance Services" has established a formal set of policies and supporting procedures.

1. Firewall Requirements Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures for having a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the firewall configuration standards adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.
- The network diagrams for the associated cardholder data environment (CDE) are to be consistent with the firewall configuration standards, which requires an illustrative drawing on the diagrams of the logical and/or physical positioning of the firewalls within the network topology.
- Authorized personnel is to regularly review network configuration documentation for the purposes of verifying that firewalls are in place at each Internet connection and between any DMZ and the internal network zone.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

2. Firewall and Router Configurations Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures regarding firewall and router configurations. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that firewall and router rules set reviews to adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
- Appropriately configure, examine, and confirm all firewalls and router settings for all inbound and outbound traffic necessary for the cardholder data environment.
- Appropriately configure, examine and confirm all firewalls and router settings for ensuring that all inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.
- Appropriately configure, examine and confirm all firewalls and router settings for ensuring that all other inbound and outbound traffic is specifically denied by using various configuration settings (i.e., deny all).
- Secure and synchronize router configuration files.
- Appropriately configure, examine, and confirm that router configuration files are secured from unauthorized access.
- Appropriately configure, examine, and confirm that router configurations are synchronized, for example, the running (or active) configuration matches the start-up configuration.
- Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
- Appropriately configure, examine and confirm firewall and router configurations for ensuring that there are perimeter firewalls installed between all wireless networks and the cardholder data environment.
- Appropriately configured, examine and confirm that firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

3. DMZ Configuration and Internet Access to the Cardholder Data Environment Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning DMZ configuration and Internet access to the cardholder data environment. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the DMZ configuration and Internet access to the cardholder data environment policy adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Prohibit direct public access between the Internet and any system component in the cardholder data environment. (Req. 1.3).
- Appropriately configure, examine, and confirm firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment, for ensuring that there is no direct access between the Internet and system components in the internal cardholder network segments. (Req. 1.3).
- Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. (Req. 1.3.1).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. (Req. 1.3.1).
- Limit inbound Internet traffic to IP addresses within the DMZ. (Req. 1.3.2).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that inbound Internet traffic is limited to IP addresses within the DMZ. (Req. 1.3.2).
- Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. (Req. 1.3.3).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment. (Req. 1.3.3).
- Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (Req. 1.3.4).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that anti-spoofing measures are implemented, for example, internal addresses cannot pass from the Internet into the DMZ. (Req. 1.3.4).

- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. (Req. 1.3.5).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. (Req. 1.3.5)
- Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.) (Req. 1.3.6).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that the firewall performs stateful inspection (dynamic packet filtering). (Req. 1.3.6).
- Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. (Req. 1.3.7).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. (Req. 1.3.7).
- Do not disclose private IP addresses and routing information to unauthorized parties. (Req. 1.3.8).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. (Req. 1.3.8.a).
- Appropriately configure, examine, and confirm all applicable and necessary documentation to ensure that any disclosure of private IP addresses and routing information to external entities is authorized. (Req. 1.3.8.b).

The exposure of cardholder data environment system components to direct public Internet access poses obvious security risks by allowing untrusted parties to make direct connections to an environment containing privileged information. The prohibition of direct public Internet access to system components within cardholder data environments helps to ensure that sensitive data, as well as the architecture where sensitive data reside, are insulated from external threats seeking to exploit information or resources.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

4. Personal Firewall Software Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures for personal firewall software on any mobile computers. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the personal firewall software on any mobile PCI computers adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Personal firewall software is required for all mobile devices that connect to the Internet (for example, laptops used by employees) when outside the company network, and which are also used to access the company network. (Req. 1.4).
- Specific configuration settings are defined for personal firewall software. (Req. 1.4).
- Personal firewall software is to be configured to actively run on all such devices. (Req. 1.4).
- Personal firewall software is to be configured in that it is not alterable by users of mobile devices. (Req. 1.4).

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

5. Changing of Vendor Supplied Default Settings Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures for the changing of vendor supplied default settings for all system components. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the changing of vendor default settings for all system components and wireless environments adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. Note: This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.). (Req. 2.1).
- All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are to be changed before a system is installed on the network. (Req. 2.1.c).
- Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are to be removed or disabled before a system is installed on the network. (Req. 2.1.c).
- Appropriately configure, examine, and confirm system settings and all necessary configurations to ensure that encryption keys are changed from default at installation. (Req. 2.1.1.a).
- Appropriately configure, examine, and confirm system settings and all necessary configurations to ensure that default SNMP community strings are changed upon installation. (Req. 2.1.1.b).
- Appropriately configure, examine, and confirm system settings and all necessary configurations to ensure that default SNMP community strings are not used. (Req. 2.1.1.c).

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

6. Configuration Standards for All System Components Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures for developing configuration standards for system components that are consistent with industry-accepted hardening standards. This process will be conducted by authorized personnel with the appropriate technical knowledge and skill sets needed to undertake this activity. The term, System Components, is defined as any network component, server or application included in or connected to the cardholder data environment. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will develop configuration standards for system components utilizing industry-accepted hardening standards for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives. The list of industry-leading security standards, benchmarks, and frameworks to utilize includes, but is not limited to, the following (PCI DSS Requirements and Security Assessment Procedures):

- Center for Internet Security (CIS).
- International Organization for Standardization (ISO).
- SysAdmin Audit Network Security (SANS) Institute.
- National Institute of Standards Technology (NIST).Vendor-specific tools and checklists, along with general setup and hardening procedures
- Additionally, when configuring system components within the cardholder environment, the following conditions must apply in order to ensure further compliance with the Payment Card Industry (PCI) Data Security Standards (DSS) Initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.0):
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the system configuration standards are consistent with industry-accepted hardening standards.
- Appropriately develop, implement, and adhere to relevant policies and supporting procedures to ensure those system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1.
- Appropriately develop, implement, and adhere to relevant policies and supporting procedures to ensure that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.
- System configuration standards used for general provisioning, hardening, securing and locking-down of system components are to include the following procedures:
    - Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
    - Implementing only one primary function per server to prevent functions that require

different security levels from co-existing on the same server.

- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system.
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure.
- Configuring system security parameters to prevent misuse.
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

- Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that that only one primary function is implemented per server.
- If virtualization technologies are used, appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that that only one primary function is implemented per virtual system component or device.
- Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only necessary services or protocols are enabled.
- For any enabled insecure services, daemons, or protocols implemented on system components, ensure they are justified per documented configuration standards.
- Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that security features are documented and implemented for all insecure services, daemons, or protocols.
- Configure system security parameters to prevent misuse.
- System administrators and/or security managers are to have relevant knowledge of common security parameter settings for system components.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that common security parameter settings are included.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that they are set appropriately and in accordance with the configuration standards.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that enabled functions are documented and support secure configuration.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only documented functionality is present on the sampled system components.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

7. Non-Console Administrative Access Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures regarding non-console administrative access. This process will be conducted by authorized personnel with the appropriate technical knowledge and skill sets needed to undertake this activity. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will encrypt all non-console administrative access using strong cryptography for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives. Many system components within the cardholder data environment are accessed through a non-console administrative function; thus, they must ensure that strong cryptography is in place at all times. The following is a list of protocol, secure data transmission elements, and tools that are used for accessing various system components:

- Secure Shell (SSH)
- Virtual Private Network (VPN)
- Secure Socket Layer (SSL) | Transport Layer Security (TLS)
- Secure File Transfer Protocol (SFTP)
- Remote Desktop Protocol (RDP)

Additionally, regarding non-console administrative access, the following conditions must apply in order to ensure further compliance with the Payment Card Industry (PCI) Data Security Standards (DSS) Initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that a strong encryption method is invoked before the administrator's password is requested.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that Telnet and other insecure remote-login commands are not available for non-console access.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that administrator access to any web-based management interfaces is encrypted with strong cryptography.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

8. Data Retention and Disposal Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoTI PCI Compliance Services has established a formal policy and supporting procedures concerning data retention and disposal. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoTI PCI Compliance Services' needs and goals.

Policy

DoTI PCI Compliance Services will ensure that the Data Retention and Disposal policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Comprehensive policies, procedures, and processes are to be developed, implemented, and in place regarding the following:
    - All legal, regulatory, and business requirements for data retention. Specifically, limiting data storage amount and retention time to that which is required for the applicable legal, regulatory, and business requirements.
    - Specific requirements for retention of cardholder data, such as why cardholder data needs to be held (i.e., time period) and the reasons why (i.e., business justification).
    - Secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons.
    - Coverage for all storage of cardholder data.
    - A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.
    - Additionally, all locations of stored cardholder data are to be included in the data retention and disposal processes.

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the data stored does not exceed the requirements defined in the data retention policy.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that data is deleted securely.

Description of Data and Scope for Cardholder Environment

Cardholder data, as defined by the Payment Card Industry Security Standards Council (PCI SSC) Glossary of Terms, includes, at a minimum the Primary Account Number (PAN), and may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or the service code. Additionally, cardholder data may also include Sensitive Authentication Data, such as security-related information (card validation codes/values, full magnetic stripe data, PINs and PIN blocks) used to authenticate cardholders, which appears in plain-text or otherwise unprotected form.

This cardholder data may reside in numerous places throughout the cardholder environment.

DESCRIPTION OF KEY TERMS AND PHRASES (Security Standards Council Glossary of Terms from pcisecuritystandards.org)

- **Access Control:** Mechanisms that limit the availability of information or information-processing resources only to authorized persons or applications

- **Cardholder Data:** The Primary Account Number (PAN) may also appear in the form of the full PAN, plus any of the following:

    - Cardholder name
    - Expiration date
    - Service code

- **Card Verification Code or Value:** Data element on a card's magnetic stripe that uses a secure cryptographic process to protect data integrity on the stripe and reveals any alteration or counterfeiting (referred to as CAV, CVC, CVV or CSC, depending on payment card)

    - **CAV** – Card Authentication Value (JCB payment cards)
    - **CVC** – Card Validation Code (MasterCard payment cards)
    - **CVV** – Card Verification Value (Visa and Discover payment cards)
    - **CSC** – Card Security Code (American Express)

- **Data:** Pieces of information from which *intelligible information* is derived. Data are a collection of information or facts usually gathered as a result of experience, observation, experiment or processes within a computer system or premises. Data may consist of numbers, words or images, particularly as measurements or observations of a set of variables. They are often viewed as the lowest level of abstraction from which information and knowledge are derived.

- **Database:** Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.

- **Degaussing:** Also called disk degaussing, it is the process or technique that demagnetizes the disk so that all data stored on the disk are permanently destroyed.

- **Encryption:** Process of converting information into a form only intelligible to holders of a specific cryptographic key. The use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

- **Full Magnetic Stripe Data:** Also referred to as *track data*. Data encoded in the magnetic stripe or chip is used for authorization during payment transactions. It can be the magnetic-stripe image on a chip or the data on the Track 1 and/or Track 2 portion of the magnetic stripe. Entities must not retain full magnetic stripe data after obtaining transaction authorization.

- **Primary Account Number (PAN):** Acronym for a *primary account number* and also referred to as *account number*. Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

- **Removable Electronic Media:** Media that store digitized data and can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives and removable hard drives.

- **Sanitization:** Process for deleting sensitive data from a file, device or system or for rendering data useless if accessed in an attack

- **Secure Wipe:** Also called *secure delete*, this is a program utility used to delete specific files permanently from a computer system.

- **Sensitive Authentication Data:** Security-related information (card validation codes/values, full magnetic stripe data, PINs and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.

- **Service Code:** Three- or four-digit value in a magnetic stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange or identifying usage restrictions.

- **System Components:** Any network component, server or application included in or connected to the cardholder data environment

Types of Data

- **Electronic Media**
- **Hardcopy Media**: Hardcopy Media are physical representations of information. Paper printouts, printers, facsimile ribbons, drums and platens are all examples of hardcopy media.
    - Paper receipts or other supporting hardcopy documents and receipts
    - Credit card printouts from processing machines
    - Invoices
    - Purchase orders
    - Offline hardcopy batch printouts
    - Other hardcopy formats as identified by organizations

Responsibility for Policy Maintenance

DoTI PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

9. Sensitive Authentication Data (SAD) Storage Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures regarding the storage of sensitive authentication data (SAD). This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services'needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the storage of sensitive authentication data (SAD) adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the full contents of any track from the magnetic stripe on the back of the card or equivalent data on a chip are not stored after authorization.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that PINs and encrypted PIN blocks are not stored after authorization.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

10. Primary Account Number (PAN) Policy for Masking & Displaying the PAN Digits

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning the masking & displaying of the Primary Account Number (PAN). This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the masking & displaying of the Primary Account Number (PAN) adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.
- A list of roles that need access to displays of full PAN is appropriately documented, along with a legitimate business need for each role having access to such information.
- All other roles not specifically authorized to see the full PAN must only see the masked PAN.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the full PAN is only displayed for users/roles with a documented business need and that PAN is masked for all other requests.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that PANs are masked when displaying cardholder data and that only those with a legitimate business need are able to see full PAN.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

11. Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) usage policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures for Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) usage policy. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals. This policy only applies Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) with internet connections for payment card processing and transmission.

Policy

DoIT PCI Compliance Services will ensure that Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) usage adhere to and comply with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Only PCI Security Standard Council approved P2PE solutions are eligible for network scope reduction or removal. For implementation and eligibility verification, an advanced approval from UIT Compliance Services team is required.
- If a PIN Transaction Security (PTS) device or a PCI workstation is connected with Wi-Fi, the PTS device or the PCI workstation must be implemented with a PCI SSC approved P2PE solution.
- Wi-Fi connection alone is prohibited for cardholder data transactions and transmission in City environment.
- If a PTS device is connected with analog, it is permitted for cardholder data transactions and transmission in City environment.
- If a PTS device is connected with Global System for Mobile (GSM, also known as Cellular), it is permitted for cardholder data transactions and transmission in City environment.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

12. Unencrypted Primary Account Numbers (PAN) Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning unencrypted Primary Account Numbers (PAN) that are not to be sent via end-user messaging technologies. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that unencrypted Primary Account Numbers (PAN) are not sent via end-user messaging technologies and that they adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Primary Account Numbers (PAN) will not be sent via unencrypted email.
- Primary Account Numbers (PAN) will not be sent via an instant messaging protocol.
- Primary Account Numbers (PAN) will not be sent via a chat protocol or forum sessions.
- If for any reason, Primary Account Numbers (PAN) must be sent via end-user messaging technologies, they are to be sent using strong encryption, rendering the PAN unreadable.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

13. Anti-Virus Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning anti-virus. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Anti-Virus policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
- Licensed anti-virus software must be utilized for all computer and system components (any network component, server or application included in or connected to the cardholder data environment) within the cardholder environment and for all computers not directly associated with the cardholder environment.
- The licensed anti-virus software utilized must be the most current version available.
- All computers and system components within the cardholder environment must have a standard, supported anti-virus software installed.
- The anti-virus software must be active, must be scheduled to perform virus checks at regular intervals and must have its virus definition and all other associated software files kept current.
- The anti-virus software must be enabled for automatic updates and periodic scans.
- All computers not directly associated with the cardholder environment must have a standard, supported anti-virus software installed.
- The anti-virus software for all computers not directly associated with the cardholder environment must also be active, scheduled to perform virus checks at regular intervals and must have its virus definitions and all other associated software files kept current.
- No user shall disable or tamper with the configuration of anti-virus software installed on their respective computer.
- Employees who allow non-company employees to attach workstations (desktops or laptops) to the company network are responsible for ensuring that those workstations are running anti-virus software and that a current virus signature is installed.
- Employees who attach workstations to the company network are responsible for ensuring that those workstations are running anti-virus software and that a current virus signature is installed.
- Never open any emails that are from an unknown or suspicious source.

- Never open any email attachments from an unknown or suspicious source.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

14. Security Patch Management Installation Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning security patch management. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

Security patch management has become a critical security issue due in large part to the exploitation of information technology systems from numerous external and internal sources. Consequently, all system components directly associated with the cardholder data environment must be securely hardened and configured with all necessary and appropriate patches and system updates for preventing the exploitation or disruption of mission-critical services as mandated (PCI DSS Requirements and Security Assessment Procedures).

Similarly, all IT resources not directly associated with the cardholder data environment must also be securely hardened and configured with all necessary and appropriate patches and system updates in order to prevent the exploitation or disruption of mission-critical services.

In accordance with best practices for security patch management, the subsequent three (3) security concerns will be highlighted throughout the Security Patch Management policy. They are as follows (NIST):

- **Vulnerabilities**: Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the system components directly associated with the cardholder data environment or any other IT resources
- **Remediation:** The three (3) primary methods of remediation are (1) installation of a software patch, (2) adjustment of a configuration setting and (3) removal of the affected software.
- **Threats:** Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network. Common examples are scripts, worms, viruses, and Trojan horses.

Failure to keep system components and other IT resources patched securely and on a consistent basis can cause unwanted damage to all environments directly associated with the cardholder environment. This includes but is not limited to the following:

- Network devices and all supporting hardware and protocols.
- Operating systems within the development and production environments.
- Applications within the development and production environments.
- Any other mission-critical resources within the cardholder data environment that require patches and security updates for daily operations

Additionally, a Security Patch Management Program (SPMP) is to be implemented, which consists of the following initiatives:

- A formalized Security Patch Management Program employee, complete with his/her roles and responsibilities.
- A comprehensive inventory of all system components directly associated with the cardholder environment.
- A comprehensive inventory of all other IT resources not directly associated with the cardholder environment.
- Subscribing to industry-leading security sources, additional supporting resources for vulnerability announcements and other security patch management alerts and issues.
- Procedures for establishing a risk ranking regarding security patch management. This will include but is not limited to (1) the significance of the threat, (2) the existence and overall threat of the exploitation and (3) the risks involved in applying security patch management procedures (its effect on other systems, resources available and resource constraints).
- The creation of a database of remediation activities that need to be applied.
- Test procedures for testing patches regarding remediation.
- Procedures for the deployment, distribution, and implementation of patches and other related security-hardening procedures.
- Procedures for verifying successful implementation of patches and other related security-hardening procedures.
- Installation of applicable critical vendor-supplied security patches within one month of release.
- Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

15. Custom Application Code Change Reviews Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning custom application code change reviews. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Custom Application Code Change Reviews policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Code changes are reviewed by individuals other than the originating code author.
- Code changes are reviewed by individuals who are knowledgeable about code review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines, such as the Open Web Security Project Guide (http://www.owasp.org/index.php/Main_Page), as stated in Requirement 6.5, titled Software Development Processes for Secure Coding Guidelines and Techniques, and for any language-specific platforms utilized to develop internal systems and applications.
- Appropriate corrections are implemented prior to the release of code.
- Code review results are reviewed and approved by management prior to release.

Furthermore, these activities relating to code changes may be done manually or automatically by DoIT PCI Compliance Services.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

16. Change Control Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning change control for security patches and software modifications. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

Change control has become a critical issue due in large part to regulatory compliance purposes and the need to fully document the change control process for accountability and tracking changes. As a result, all system components directly associated with the cardholder data environment and other IT resources that undergo changes must be documented accordingly.

DoIT PCI Compliance Services will ensure that Change Control policy and procedures adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Establishment of change control initiation, implementation and authorization directives
- Establishment of a change control lifecycle
- Establishment of minimum reporting criteria for change control documentation
- Separation of duties, roles, and responsibilities exist between the development/test environment(s) and production environment(s), complete with access controls in place.
- Production data with live Primary Account Numbers (PAN) are not to be used for testing or development.
- Test data and all associated accounts are removed before a production system becomes active.
- Documentation of impact is included in the change control documentation.
- Management signoff by appropriate parties, along with approval for all stages of the change control lifecycle, is required for each change.
- Operational functionality testing is performed and must be documented for each change, where applicable so as to verify that the change does not adversely impact the security of the
- custom code changes
- For custom code changes made, all updates and releases are tested for compliance with Requirement 6.5 before being released to production.
- Additionally, change controls policies, procedures, and supporting initiatives are to properly document the following:
    - Documentation of impact is included in the change control documentation for each sampled.
    - Documented approval by authorized parties is present for each sampled change.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

17. Software Development Secure Coding Guidelines and Training Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning software development and secure coding guidelines and training. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the software development and secure coding guidelines and training policy and procedures adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Software developers and all other relevant personnel involved in the development of software for DoIT PCI Compliance Services are required to undergo annual training in secure coding techniques for the software platforms(s) with which they work.
- Software developers and all other relevant personnel involved in the development of software for DoIT PCI Compliance Services are required to submit their Secure Coding Training checklist on an annual basis as evidence that they are knowledgeable in secure coding techniques.
- Software developers involved in the software development process will adhere to professional guidelines, such as the Open Web Application Security Project (OWASP) Code of Ethics and CWE/SANS.
- DoIT PCI Compliance Services' software development lifecycle includes policies, processes, and procedures to ensure that internally-developed applications are not vulnerable to the following threats:
    - Injection Flaws (SQL, OS and LDAP Injection)
    - Buffer Overflows
    - Insecure Cryptographic Storage
    - Insecure Communications
    - Improper Error Handling
    - All high-risk vulnerabilities identified in the vulnerability identification process as found in the Risk Ranking Table within the Security Patch Management Installation Policy and Procedures document.
    - Cross-Site Scripting
    - Improper Access Control
    - Cross-Site Request Forgery
    - Broken Authentication and Session Management
    - All "High" vulnerabilities and threats as identified in the Risk Ranking Table found in the Security Patch Management Installation Policy and Procedures.

Source: **http://www.owasp.org**

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

18. Data Control & Access Control Policies

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning data control and access control. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Data Control & Access Control policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Limit access to system components and cardholder data to only those individuals whose job requires such access.
- Access needs are to be defined for each respective role, specifically:
    - System components and data resources that each role needs to access for their job function.
    - Level of privilege required for accessing resources.
- Access rights for privileged users are restricted to the least privileges necessary to perform job responsibilities.
- Privileges are assigned to individuals based on job classification and function, such as Role-Based Access Control (RBAC).
- An authorization form is required for all access, which must specify required privileges, and must be signed by management.
- Access control systems are in place on all system components.
- Access control systems are configured to enforce privileges assigned to individuals based on job classification and function.
- Access control systems have a default *Deny All* setting.
- Security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

19. Unique ID & Authentication Methods Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning unique ID and authentication methods. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Unique ID and Authentication Methods policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- All users are assigned a unique ID before allowing them to access system components or cardholder data.
- Authorized personnel is to control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- Terminated users are to have their access immediately revoked.
- Inactive user accounts are to be disabled and/or removed every 90 days.
- Authorized personnel is to manage IDs used by vendors to access, support, or maintain system components via remote access as follows:
    - Enable vendor access only during the time period needed and disabled when not in use.
    - Actively monitored when in use by all appropriate means.
- Additionally, the following best practices are to be implemented regarding accepts attempts and system idle time:
    - Limit repeated access attempts by locking out the user ID after not more than six attempts.
    - Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
    - If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
- Additionally, all users are to be assigned a unique ID for access to system components or cardholder data and must also utilize an approved authentication method by the AS PCI Compliance Services Office.
- Passwords/phrases must meet the following conditions in accordance with PCI DSS mandates:
    - A minimum length of at least seven characters.
    - Contain both numeric and alphabetic characters.
    - Comply with the City of Imperial password policy

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

20. Shared, Group, Generic, and Other Authentication Methods Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning other various authentication methods, such as shared, group, generic, and any other specific methods. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Shared, Group, Generic, and Other Authentication Methods Policy adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that Generic user IDs are disabled or removed.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that shared user IDs for system administration activities and other critical functions do not exist.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that shared and generic user IDs are not used to administer any system components.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.
- Ensure that system administrators understand that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that different authentication is used for access to each customer.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that procedures for user authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include authentication mechanisms that are assigned to an individual account and not shared among multiple accounts and that physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that controls are implemented to ensure only the intended account can use that mechanism to gain access.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

21. Database Access & Configuration Settings Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning database access & configuration settings. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Database Access & Configuration settings policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all users are authenticated prior to access.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that user direct access to or queries of databases is restricted to database administrators.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that application IDs can only be used by the applications (and not by individual users or other processes).

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives

22. Media Storage, Distribution and Classification Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning storage, distribution, and classification. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Media Storage, Distribution and Classification Policy adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes) are to be in place for protecting cardholder data.
- Media backups are to be stored in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.
- All media is to be appropriately classified so the sensitivity of the data can be determined.
- All media is to be sent by secured courier or another delivery method so that it can be accurately tracked.
- Management is to approve any and all media that is moved from a secured area (including when media is distributed to individuals).
- Strict control is to be maintained over the storage and accessibility of media.
- Inventory logs of all media are to be maintained, with media inventory procedures undertaken at least annually.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

23. Media Destruction Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning media destruction. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Media Destruction policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Once the maximum retention period has been allotted for cardholder data, it must be removed from all electronic media, and any hardcopy edition must be disposed of accordingly.
- All hardcopy materials are to be cross-shredded, incinerated or pulped; such that there is a reasonable assurance the hardcopy materials cannot be reconstructed.
- Storage containers for shredding hardcopy materials are to be secured at all times, with appropriate physical controls such as locks on the storage bins.
- Storage of cardholder data on electronic media is not permissible per AS PCI Compliance policy.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

24. Media Device Protection Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning media device protection. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Media Device Protection policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Authorized personnel is to conduct the following:
  - Maintain a list of all devices that capture payment card data, for which the list is to include the following:
    - Make, the model of the device
    - Location of the device (for example, the address of the site or facility where the device is located)
    - Device serial number or another method of unique identification.
  - Periodically inspect all devices to ensure that they have not been tampered with nor substituted.
  - Adequately train personnel to be aware of suspicious behavior and to report tampering or substitution of devices.
  - Ensure that the list of devices is updated when devices are added, relocated, decommissioned.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

25. Physical Security Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning physical security around payment card processing. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Physical Security policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

Any physical location that is part of the Cardholder Data Environment (CDE) must have the following security controls:

- Access is controlled with badge readers or other devices including authorized badges and lock and key.
- Surveillance monitoring equipment and/or access control mechanisms must be in place to monitor the entry/exit points to sensitive areas.
- Surveillance monitoring equipment and/or access control mechanisms must be protected from tampering or disabling.
- Surveillance monitoring equipment and/or access control mechanisms must be monitored and data from equipment or other mechanisms must be stored for at least three (3) months.
- Physical and/or logical controls must be in place to restrict access to publicly accessible network jacks.
- Physical access to wireless access points, gateways, handheld devices, networking/communications hardware and telecommunication lines (i.e., "critical infrastructure hardware") must be appropriately restricted.
- Any physical location that is part of the Cardholder Data Environment (CDE) must have the following security for personnel and visitor access:
- Processes and procedures must be in place for assigning badges to onsite personnel (i.e., employees) and visitors, which consist of granting new badges, changing access requirements and revoking access.
- Processes and procedures must be in place for distinguishing between onsite personnel and visitors, with a mechanism to clearly identify visitors.
- Access to the identification process (such as the badge system) must be limited to authorized personnel.
- Appropriate authorization procedures must be followed before authorizing personnel to access the CDE.
- Any terminated employee must have their access authorization removed immediately.

- Visitors must be authorized before they are granted access to and escorted at all times within, areas where cardholder data is processed or maintained.
- A visitor log must be in place to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. The log should record key information:
    - The visitor's name
    - The firm represented
    - The onsite personnel authorizing physical access
- The visitor log must be retained for at least three months.
- Visitor identification (such as badges) must expire.
- Visitors must surrender their badge or other authorization identification upon departure or expiration.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

26. Securing of Audit Trails Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning the securing of audit trails. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the time-synchronization technology policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Only individuals with a job-related need can view audit trail files.
- Current audit trail files are to be protected at all times from unauthorized modifications via access control mechanisms, physical segregation and/or network segregation.
- Audit trail files are to be promptly backed up to a centralized log server or media that is difficult to alter.
- Logs for external-facing technologies are to be written onto a secure, centralized, internal log server or media.
- Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the use of file-integrity monitoring or change-detection software on logs.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

27. Security Logs & Events Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning security logs & events. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that the Security Logs & Events policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Authorized personnel is to review logs and security events on a daily basis for all system components for the purposes of identifying anomalies or suspicious activity.
- As such, the following items are to be also reviewed by authorized personnel:
  - All security events
  - Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
  - Logs of all critical system components.
  - Logs of all servers and system components that perform security functions.
- Additionally, authorized personnel is to perform the following:
  - Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
  - Follow up on any exceptions and anomalies identified during the review process.
- Furthermore, all audit trail history files are to be retained for at least one year, with a minimum of three months immediately available for analysis.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

28. PCI Workstation and Laptop Usage Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures for PCI Workstation and laptop usage policy. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals. This policy only applies to the PCI workstations and laptops with internet connections but does not apply to stand-alone PTS devices and terminals that are provided by Merchant Services from Wells Fargo Bank.

Policy

DoIT PCI Compliance Services will ensure that PCI Workstation and Laptop Usage Policy adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- A City employee or contractor can only use a dedicated PCI workstation or a dedicated PCI laptop to perform payment card transactions for City customers, clients.
- For card-in-present, mail order, fax order and phone order, it is a violation to enter/process customers' card transaction by any devices with internet connection other than the dedicated PCI workstations or laptops.
- The dedicated PCI workstations and laptops are provided and maintained by DoIT, except R&DE Revel dining POS and P&TS parking meters.
- This policy does not apply to the PCI SSC and UIT approved P2PE devices and systems.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

29. Strong Cryptography and Secure Protocols for CHD transmission

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures concerning the use of strong cryptography and secures protocols. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding PCI DSS and DoIT PCI Compliance Services' needs and goals.

Policy

All departments must ensure that the use of strong cryptography and security protocols adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

- Use strong cryptography and security protocols for safeguarding sensitive cardholder data during transmission over open, public networks.
- Comprehensively document all locations where cardholder data is transmitted or received over open, public networks.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all cardholder data is encrypted with strong cryptography during transit.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only trusted keys and/or certificates are accepted.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the proper encryption strength is implemented for the encryption methodology in use.
- Strong cryptography and secured protocols are defined and approved by PCI DSS.

29. 1 For Voice over IP (VoIP) transmission, the following three requirements must be met:

- 29.1.1 All the VoIP data must be encrypted with strong cryptography and transmitted by secured protocols.
- 29.1.2 Network segregation must be implemented for the VoIP to transmit cardholder data.
- 29.1.3 VoIP with cardholder data is prohibited for storage in any of City of Imperial's systems.

29. 2 It is prohibited to transmit CHD via text messages, instant messages, emails or voicemail.

Responsibility for Policy Maintenance

Administrative Systems PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

30. Evaluation Policy for Payment Systems and Service Vendors

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures for payment systems and service vendor's evaluation. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services will ensure that payment systems and service vendors' usage adhere to and comply with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures).
Payment System and Services Vendors include application system and service providers, and any external consulting services that involve PCI DSS compliance.

30.1 Vendor evaluation for the individual merchant department:

For the evaluation and verification of payment card service providers, the following documents must be submitted to pci-compliance@cityofimperial.org.

An Attestation of Compliance (AOC) must be submitted by using the PCI Security Standards Council (SSC) official form.

Please note the following:

- The AOC must be valid within twelve months.
- Every vendor must submit the AOC as a service provider unless an exception is granted by Treasury Office, ISO and UIT Compliance Office.
- If the AOC is not signed by a PCI SSC certified QSA or ISA, the vendor must also submit their current quarter's Approved Scanning Vendor (ASV) report and the current year's penetration test report for the external network.
- In a twelve month period, the PCI Compliance team will only accept a maximum of three versions of an AOC from the same vendor for review.

If needed at a later stage of the evaluation, the PCI Compliance team might request that the vendor provide a demo on payment processing workflow through its services.

30.2 Vendor and consulting services evaluation for Merchant Services:

Prior to Merchant Services starts the discovery process with a vendor, Merchant Services will contact UIT/AS Compliance Services for the following 30.2.1, 30.2.2 and 30.2.3 assessment. No business engagement or formal purchase orders should be involved with any prospect payment system and services vendors before such assessment is completed and satisfied.

30.2.1 Vendors' PCI DSS compliance assessment (please see 30.1 for requirement documents).
30.2.2 Initial assessment for vendors' qualification to meet DoIT PCI Compliance Services Minimum Security Standard.
30.2.3 Assess vendor systems' feasibility for the integration with DoIT PCI Compliance Services' PCI infrastructure, compliance and security requirement for PCI DSS compliance and DoIT PCI Compliance Services Minimum Security.

Subsequentially, for Data Risk Assessment (DRA), the Information Security Office (ISO) and the City Privacy Office (CPO) evaluate projects based on all applicable security and privacy laws and regulations as well as City policy.

Note: Payment card service providers, please note that according to PCI SSC, all of the organizations that process, transmit, and/or store payment card information must be PCI Security Standard Requirements and Security Assessment Procedures (PCI DSS) compliant.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

31. PCI DSS Awareness Training Policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, DoIT PCI Compliance Services has established a formal policy and supporting procedures for PCI DSS awareness training. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding DoIT PCI Compliance Services' needs and goals.

Policy

DoIT PCI Compliance Services has implemented a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

31.1 All personnel, whose responsibility involves payment card processing, transmission or storage, are required by PCI DSS to be enrolled and complete the training on annual basis.

31.2 For newly required personnel in the merchant departments, Merchant Services team shall notify the PCI Compliance team for the initial enrollment.

31.3 Once personnel is enrolled in the PCI DSS Training, the centralized training system will send out notification on annual basis for training certification and subsequent recertification automatically.

31.4 If personnel is no longer required for the PCI DSS Training due to job changes, a notification with the manager's approval or Merchant Service's approval is required to send to the PCI Compliance team for de-enrollment.

Responsibility for Policy Maintenance

DoIT PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.