Overall PCI Security Policies

0.0 Effective Date

This document goes into effect on 08-30-10

1.0 Purpose

This document lays down what is required to achieve and sustain PCI compliance for the below areas.

2.0 Scope

This policy applies to all areas outlined below.

3.0 Policy

3.1 - Restrict the right of maintaining record structures that support confidentiality

- 3.1.1 - Sensitive authentication data must not be stored after authorization. The sensitive authentication data that should not be stored is the full track contents from the magnetic stripe, card-verification code, and the personal identification number (PIN).Verify sensitive authentication is not stored after authorization. Review the processes for deleting this data and verify it cannot be recovered.

3.2 - Restrict the right of maintaining record structures that support confidentiality

- 3.2.1 - Sensitive authentication data must not be stored after authorization. The sensitive authentication data that should not be stored is the full track contents from the magnetic stripe, card-verification code, and the personal identification number (PIN).Verify sensitive authentication is not stored after authorization. Review the processes for deleting this data and verify it cannot be recovered.

3.3 - Restrict the right of maintaining record structures that support confidentiality

- 3.3.1 - Sensitive authentication data must not be stored after authorization. The sensitive authentication data that should not be stored is the full track contents from the magnetic stripe, card-verification code, and the personal identification number (PIN).Verify sensitive authentication is not stored after authorization. Review the processes for deleting this data and verify it cannot be recovered.

3.4 - Restrict the right of maintaining record structures that support confidentiality

- 3.4.1 - Sensitive authentication data must not be stored after authorization. The sensitive authentication data that should not be stored is the full track contents from the magnetic stripe, card-verification code, and the personal identification number (PIN).Verify sensitive authentication is not stored after authorization. Review the processes for deleting this data and verify it cannot be recovered.

3.5 - Display the minimum data necessary

- 3.5.1 - The organization must ensure the primary account number is masked (the first or the last digits of the number may be displayed).Review the organization's policies and examine displays of credit card numbers to verify credit card numbers are masked, except in cases where there is a specific need to see the entire card number.

3.6 - Confidentiality protection of sensitive messages

- 3.6.1 - The organization must ensure messaging technologies, such as e-mail, chat, and text messaging, are never used to send unencrypted primary account numbers.Verify the organization has a policy stating that Primary Account Numbers (PANs) should not be sent by messaging technologies, unless they are encrypted.

3.7 - Maintain control over access rights and user privileges

- 3.7.1 - The organization must ensure access to the cardholder data and system components are restricted to individuals whose job requires access and that access restrictions are based on least privileges and job classification and duties. Privileges must be requested by management in writing. The organization must use an automated access control system to implement the access controls. The organization must ensure all access to cardholder data databases by users, Administrators, and applications are authenticated.Verify the access control policy includes requirements for assigning privileges based on job classification and function and that an automated access control system is installed, management has signed an authorization form for each individual specifying which privileges are assigned to that individual, and access rights are based on least privileges. Examine the database configuration settings to ensure only users, Administrators, and applications that have been authenticated can gain access to the database and that direct SQL database queries are prohibited.
    - 3.7.1.1 - The organization must ensure all users are identified by a unique userID and that each user is authenticated by either a password or two-factor

    authentication method.Review the list of userIDs to verify that each user has a unique userID.
    - 3.7.1.2 - The organization must ensure privileged userIDs are restricted to the least amount of privileges needed to perform their jobs.Verify users with privileged userIDs are assigned access rights based on the least amount of privileges needed to perform their jobs.
        - 3.7.1.2.1 - Ensure that the assignment of privileges is based upon the person's job function.
        - 3.7.1.2.2 - Access limitations must include an authorization form signed by management that specifies required privileges.
    - 3.7.1.3 - The organization will ensure that information systems enforce a predetermined limit of consecutive invalid access attempts by a user during a predetermined period of time.
    - 3.7.1.4 - The organization will ensure that the information system provides a mechanism to protect the authenticity of communications sessions.
    - 3.7.1.5 - The organization must ensure it has developed a password and user authentication management program that requires a user to repenter his/her password if the session has been idle for more than minutes.Review the usage policy to verify inactive modem sessions are automatically disconnected after a predetermined period of time.Examine a sample of components to verify the system configuration settings for system/session idle time out have been set to minutes or less.Interview system security officers to ensure they have set the appropriate parameters.
    - 3.7.1.6 - The organization must ensure it has developed a password and user authentication management program and usage policies that only activates accounts used by vendors for remote maintenance when the maintenance is occurring.Ensure vendor accounts used for remote maintenance are active only when used by the vendor and that they are monitored during use. Examine the usage policies to verify remote access used by vendors are activated only when needed by the vendor and deactivated immediately after use.Interview system security personnel to ensure they have inactivated all vendor accounts and activate them only when necessary.

3.8 - Inventory and physically secure all media that stores confidential information

- 3.8.1 - The organization must ensure all paper and electronic media that contains cardholder data are physically secured.Verify procedures exist for controlling physical access to paper and electronic media, including reports, faxes, CDs, disks, and hard drives.

3.9 - Maintain media controls

- 3.9.1 - Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.

    - 3.9.1.1 - The organization must ensure all paper and electronic media that contains cardholder data are physically secured.Verify procedures exist for controlling physical access to paper and electronic media, including reports, faxes, CDs, disks, and hard drives.
    - 3.9.1.2 - The organization must ensure any media that contains cardholder data is strictly controlled during any distribution, either internally or externally.Verify a policy exists for the distribution of media containing cardholder data and that the policy covers the distribution to individuals in the organization.
        - 3.9.1.2.1 - The organization must ensure procedures are in place to have management approve any transit of sensitive media from a secured area.
        - 3.9.1.2.2 - The organization must maintain control over all media that contains cardholder data.Verify a policy exists for controlling the storage of media containing cardholder data.
        - 3.9.1.2.3 - The organization must ensure all media containing cardholder data is classified as confidential.Ensure all media containing sensitive information is labeled "Confidential."
        - 3.9.1.2.4 - The organization must ensure all media containing cardholder data can be tracked when being sent outside the facility.Ensure all media containing cardholder data that is sent outside the organization is authorized, logged, and tracked during transit.

3.10 - Label media

- 3.10.1 - The organization must ensure all media containing cardholder data is classified as confidential.Ensure all media containing sensitive information is labeled "Confidential."

3.11 - Track while in transit

- 3.11.1 - The organization must ensure all media containing cardholder data can be tracked when being sent outside the facility.Ensure all media containing cardholder data that is sent outside the organization is authorized, logged, and tracked during transit.

3.12 - Obtain management approval for transit

- 3.12.1 - The organization must ensure procedures are in place to have management approve any transit of sensitive media from a secured area.

3.13 - Physical protection while media is in storage

- 3.13.1 - The organization must maintain control over all media that contains cardholder data.Verify a policy exists for controlling the storage of media containing cardholder data.

3.14 - Manage disposition and destruction

- 3.14.1 - The organization must ensure all cardholder data is destroyed when it is no longer needed.Verify the media destruction policy covers all types of media that contains cardholder data.
    - 3.14.1.1 - The organization will ensure that all hardcopy materials and media to be destroyed are done so in accordance with the strictest standards and guidelines.

3.15 - Destruction and disposal of hard copy materials and media

- 3.15.1 - The organization will ensure that all hardcopy materials and media to be destroyed are done so in accordance with the strictest standards and guidelines.

3.16 - Establish a security and internal control framework policy

- 3.16.1 - The organization must develop, publish, maintain, and distribute a security policy and must address all of the PCI DSS requirements.Verify the information security policy addresses all requirements and has been published and disseminated to all relevant users.
    - 3.16.1.1 - The organization must ensure the security policy contains procedures for identifying threats and vulnerabilities through an annual risk assessment.Review the information security policy to ensure it contains a requirement for an annual risk assessment to identify threats and vulnerabilities.
    - 3.16.1.2 - The organization must ensure the security policy is reviewed on an annual basis and whenever the environment changes.Verify the information security policy is reviewed on an annual basis and when a change occurs in the environment and is updated as necessary.
    - 3.16.1.3 - The organization must ensure the security policy contains daily operational security procedures in accordance with the PCI DSS requirements.Verify the existence of daily operational security procedures in the security policy and that they include administrative and technical procedures for each of the requirements.
    - 3.16.1.4 - The organization must develop procedures for identifying newly discovered vulnerabilities, such as subscribing to alert services. The security alerts and information must be distributed to the appropriate personnel.Verify the responsibility for monitoring security alerts and communicating that information to the appropriate personnel has been formally assigned in the information security policies and procedures.Interview security personnel to ensure new vulnerabilities are identified, including from the use of outside sources.
    - 3.16.1.5 - The organization must ensure that security incident response and escalation procedures have been developed, documented, and distributed to the appropriate personnel.Verify the responsibility for creating and distributing

security incident response and escalation procedures has been formally assigned in the information security policies and procedures.
    - 3.16.1.6 - The organization must ensure that additions, deletions, and modifications to user accounts are assigned to an Administrator.Verify the responsibility for administering user account and authentication management has been formally assigned in the information security policies and procedures.
    - 3.16.1.7 - The organization must ensure all access to data is monitored and controlled.Verify the responsibility for monitoring and controlling all access to data has been formally assigned in the information security policies and procedures.
    - 3.16.1.8 - The organization must develop a security awareness program to ensure all employees are aware of the importance of cardholder data. The organization must ensure all employees participate in training at least annually.
        - 3.16.1.8.1 - Ensure that the security awareness plan has an appropriate education methodology.
        - 3.16.1.8.2 - The organization must ensure all employees read and understand the security policy and procedures at least annually by signing a statement acknowledging this fact.Verify all employees have signed a statement acknowledging that they have read and understand the information security policy.

3.17 - The organizational security policy and procedures will be reviewed when the environment changes or at least annually

- 3.17.1 - The organization must ensure the security policy is reviewed on an annual basis and whenever the environment changes.Verify the information security policy is reviewed on an annual basis and when a change occurs in the environment and is updated as necessary.

3.18 - Establish usage and proper behavior policies

- 3.18.1 - The organization must ensure usage policies have been developed for critical employee-facing technologies.
    - 3.18.1.1 - The organization must ensure the usage policies require explicit management approval before technologies are used.Review the usage policy to verify explicit management approval is obtained prior to using devices.
    - 3.18.1.2 - The organization must ensure the usage policies require users to be authenticated before the device can be used.Review the usage policy to verify that all devices are authenticated with a username and password prior to being used.
    - 3.18.1.3 - The organization must ensure the usage policies require a list of all the devices on the system and the personnel who may access the devices.Review the usage policy to verify that it contains a list of all devices and the personnel who are authorized to use the devices.

  - 3.18.1.4 - The organization must ensure the usage policies require all devices to be labeled with the name of the owner, his/her contact information, and the device's purpose.Review the usage policy to verify all devices are required to be labeled with the owner, contact information, and the purpose of the device.
  - 3.18.1.5 - The organization must ensure the usage policies contain all acceptable uses the technology can be used for and what locations the technology can be used from.Review the usage policy to verify it contains a list of all acceptable uses and locations for the technology.
  - 3.18.1.6 - The organization must ensure the usage policies contain a list of company-approved products.Review the usage policy to verify it contains a list of company approved products.

3.19 - Defining operational roles and responsibilities

- 3.19.1 - The organization must ensure the security policy has clearly defined the security responsibilities of all contractors and employees.Verify information security responsibilities are clearly defined for employees and contractors in the information security policy.
  - 3.19.1.1 - The organization must ensure that a Chief Security Officer has been formally assigned.Verify the position of Chief Security Officer has been formally assigned in the information security policies and procedures.

3.20 - Chief information officer

- 3.20.1 - The organization must ensure that a Chief Security Officer has been formally assigned. Verify the position of Chief Security Officer has been formally assigned in the information security policies and procedures.

3.21 - The organizational security framework will contain procedures for timely security incident response and escalation

- 3.21.1 - The organization must ensure that security incident response and escalation procedures have been developed, documented, and distributed to the appropriate personnel.Verify the responsibility for creating and distributing security incident response and escalation procedures has been formally assigned in the information security policies and procedures.

3.22 - Communication of IT security awareness

- 3.22.1 - The organization must develop a security awareness program to ensure all employees are aware of the importance of cardholder data. The organization must ensure all employees participate in training at least annually.

  - 3.22.1.1 - Ensure that the security awareness plan has an appropriate education methodology.
  - 3.22.1.2 - The organization must ensure all employees read and understand the security policy and procedures at least annually by signing a statement acknowledging this fact.Verify all employees have signed a statement acknowledging that they have read and understand the information security policy.

3.23 - Management of third party services

- 3.23.1 - The organization must ensure the service provider policies and procedures includes a list of all service providers, how the organization will monitor the compliance of the service provider with the PCI DSS requirements, and due diligence.Verify all third party service providers have policies and procedures in place requiring a list of all connected entities, performing due diligence prior to connecting the entities, verifying PCI DSS compliance, and for connecting and disconnecting entities.
  - 3.23.1.1 - Maintain a list of service providersThe testing procedures from Appendix A of this document should be performed to ensure the hosting providers are protecting the environment and cardholder data.
  - 3.23.1.2 - Establish processes and procedures for engaging service providers, including proper due diligence prior to engagement.
    - 3.23.1.2.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses.Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.
      - 3.23.1.2.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.
      - 3.23.1.2.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment.Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.
    - 3.23.1.2.2 - Maintain a program to monitor service providers' compliance status.
  - 3.23.1.3 - The organization will maintain a policy, standard, and procedure to select suppliers according to a fair and formal practice to ensure a viable best fit based on requirements.

3.24 - Supplier Interfaces

- 3.24.1 - Maintain a list of service providersThe testing procedures from Appendix A of this document should be performed to ensure the hosting providers are protecting the environment and cardholder data.

3.25 - Acknowledgment of responsibility for data in possession and control

- 3.25.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses.Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.
    - 3.25.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.
    - 3.25.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment.Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.

3.26 - Formalize third party relationships

- 3.26.1 - Establish processes and procedures for engaging service providers, including proper due diligence prior to engagement.
    - 3.26.1.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses.Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.
        - 3.26.1.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.
        - 3.26.1.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment.Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or

execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.

  - 3.26.1.2 - Maintain a program to monitor service providers' compliance status.

3.27 - Audit provisions

- 3.27.1 - Maintain a program to monitor service providers' compliance status.

4.0 Enforcement

Failure to comply with the policies outlined above may result in a failure of the companies PCI compliance and may result in penalties up to termination of the offending employee.

Policies provided by

The Unified Compliance Framework is the first independent initiative to exclusively support IT compliance management by focusing on commonalities across regulations, standards-based development, and simplified architectures. Unified Compliance's strategic approach to IT compliance reduces cost and limits liability. The UCF's strategic approach simplifies compliance and standards, reduces cost, limits liability, and leverages the value of compliance-related technologies through a harmonized set of controls against which all regulatory standards and best practices can be mapped.

The UCF was created by Dorian Cougias and his research partner, Marcelo Halpern of the international law firm Latham and Watkins, which oversees all legal aspects of the UCF.