PCI DSS Section 5: Regularly Monitor & Test Networks

Requirement #10: Track & Monitor All Access To Network Resources & Cardholder Data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Control 10.1

Control Objective: The organization implements audit trails for linking access to system components to individual users.

Standard: Asset custodians and data owners are required to implement auditing of systems and applications that allow access to system components to be linked to individual users. [167]

Supplemental Guidance: It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS Control 10.2

Control Objective: The organization utilizes automated audit trails for system components to reconstruct events.

Standard: Asset custodians and data owners are required to implement automated audit trails for all system components to reconstruct the following events: [168]

(a) All individual user accesses to cardholder data; [169]
(b) All actions taken by any individual with root or administrative privileges; [170]
(c) Access to all audit trails; [171]
(d) Invalid logical access attempts; [172]
(e) Use of and changes to identification and authentication mechanisms, including but not limited to: [173]
    1. creation of new accounts and elevation of privileges; and
    2. all changes, additions, or deletions to accounts with root or administrative privileges;
(f) Initialization, stopping, or pausing of the audit logs; [174] and
(g) Creation and deletion of system-level objects. [175]

Supplemental Guidance: Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities.

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

[167] PCI DSS v3.2 Requirement 10.1
[168] PCI DSS v3.2 Requirement 10.2
[169] PCI DSS v3.2 Requirement 10.2.1
[170] PCI DSS v3.2 Requirement 10.2.2
[171] PCI DSS v3.2 Requirement 10.2.3
[172] PCI DSS v3.2 Requirement 10.2.4
[173] PCI DSS v3.2 Requirement 10.2.5
[174] PCI DSS v3.2 Requirement 10.2.6
[175] PCI DSS v3.2 Requirement 10.2.7

PCI DSS CONTROL 10.3

Control Objective: The organization follows best practices for logging audit trail entries.

Standard: Asset custodians and data owners are required to configure systems to record at least the following audit trail entries for all system components for each event: [176]

(a) User identification; [177]
(b) Type of event; [178]
(c) Date and time; [179]
(d) Success or failure indication; [180]
(e) Origination of event; [181] and
(f) Identity or name of affected data, system component, or resource. [182]

Supplemental Guidance: By recording these details for the auditable events at PCI DSS requirement 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.4

Control Objective: The organization utilizes time-synchronization technology to synchronize all critical system clocks.

Standard: Network Time Protocol (NTP) is City of Waukesha's official method of synchronizing all system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time:[183]

(a) Asset custodians are responsible for configuring City of Waukesha's NTP servers so that they are receiving time from industry-accepted time sources; [184] and
(b) Asset owners must ensure NTP on their systems is configured properly and validate the following:
    1. Systems are configured to synchronize time with City of Waukesha's NTP servers;
    2. Information systems have the correct and consistent time; [185] and
    3. Time data is protected from unauthorized modification. [186]

Supplemental Guidance: Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. NTP is an Internet standard protocol which enables client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.[187] Official NIST or USNO Internet Time Service (ITS) that can to be used for system time synchronization include, but are not limited to:

- time.nist.gov 192.43.244.18 [primary]; and
- time-nw.nist.gov 131.107.13.100 [alternate]

Procedures: All workstations and servers have their time synchronized with a domain controller; all other network devices use time.nist.gov

[176] PCI DSS v3.2 Requirement 10.3
[177] PCI DSS v3.2 Requirement 10.3.1
[178] PCI DSS v3.2 Requirement 10.3.2
[179] PCI DSS v3.2 Requirement 10.3.3
[180] PCI DSS v3.2 Requirement 10.3.4
[181] PCI DSS v3.2 Requirement 10.3.5
[182] PCI DSS v3.2 Requirement 10.3.6
[183] PCI DSS v3.2 Requirement 10.4
[184] PCI DSS v3.2 Requirement 10.4.3
[185] PCI DSS v3.2 Requirement 10.4.1
[186] PCI DSS v3.2 Requirement 10.4.2
[187] http://tycho.usno.navy.mil/ntp.html

PCI DSS CONTROL 10.5

Control Objective: The organization secures audit trails so logs cannot be altered.

Standard: Asset custodians and data owners are required to secure audit trails so the logs cannot be altered. Securing audit trails includes the following: [188]

(a) Limiting viewing of audit trails to those with a job-related need; [189]
(b) Protecting audit trail files from unauthorized modifications; [190]
(c) As close to real-time as possible, backup or transfer audit trail files to a centralized log server or media that is difficult to alter; [191]
(d) Writing logs for external-facing technologies onto a secure, centralized, internal log server or media device; [192] and
(e) Using File Integrity Monitoring (FIM) or change detection software on logs to ensure that existing log data cannot be changed without generating alerts. [193]

Supplemental Guidance: FIM or change detection software should be configured not to alert when new data is being added to logs. Otherwise normal log traffic will generate change alerts on the log files.

Procedures: Only network and system administrators have access to the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.6

Control Objective: The organization implements a process to review logs and security events for all system components to identify anomalies or suspicious activity.

Standard: Asset custodians and data owners are required to develop and implement a process to review logs and security events for all system components to identify anomalies or suspicious activity that includes: [194]

(a) Reviewing the following, at least daily: [195]
    1. All security events;
    2. Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of cardholder data;
    3. Logs of all critical system components; and
    4. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
        i. Firewalls
        ii. Intrusion Detection Systems (IDS)
        iii. Intrusion Prevention Systems (IPS)
        iv. Authentication servers (e.g., Active Directory domain controllers); and
        v. E-commerce redirection servers;
(b) Reviewing logs of all other system components periodically based on City of Waukesha's policies and risk management strategy, as determined by City of Waukesha's annual risk assessment; [196] and
(c) Following up exceptions and anomalies identified during the review process. [197]

Supplemental Guidance: Many breaches occur over days or months before being detected. Checking logs daily minimizes the amount of time and exposure of a potential breach. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment.

The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.

---

[188] PCI DSS v3.2 Requirement 10.5
[189] PCI DSS v3.2 Requirement 10.5.1
[190] PCI DSS v3.2 Requirement 10.5.2
[191] PCI DSS v3.2 Requirement 10.5.3
[192] PCI DSS v3.2 Requirement 10.5.4
[193] PCI DSS v3.2 Requirement 10.5.5
[194] PCI DSS v3.2 Requirement 10.6
[195] PCI DSS v3.2 Requirement 10.6.1
[196] PCI DSS v3.2 Requirement 10.6.2
[197] PCI DSS v3.2 Requirement 10.6.3

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.7

Control Objective: The organization retains audit trail history.

Standard: Asset custodians and data owners are required to retain audit trail history for at least one (1) year, with a minimum of three (3) months immediately available for analysis. [198]

Supplemental Guidance: Logs are considered "immediately available" for analysis if the logs can be:

- Accessed online;
- Readily recovered from archived media; or
- Restorable from back-up.

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.8

Control Objective: The organization is able to detect failures of critical security control systems in a timely manner.

Standard: Asset custodians and data owners are required to:

(a) Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: [199]
    1. Firewalls; IDS/IPS;
    2. FIM;
    3. Anti-malware;
    4. Physical access controls;
    5. Logical access controls;
    6. Audit logging mechanisms; and
    7. Segmentation controls (if used); and

(b) Develop processes for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: [200]
    1. Firewalls;
    2. IDS/IPS;
    3. FIM;
    4. Anti-malware;
    5. Physical access controls;
    6. Logical access controls;
    7. Audit logging mechanisms; and
    8. Segmentation controls (if used).

Supplemental Guidance: Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment.

The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.

Procedures: This is accomplished using the City's network monitoring system.

---

[198] PCI DSS v3.2 Requirement 10.7
[199] PCI DSS v3.2 Requirement 10.8
[200] PCI DSS v3.2 Requirement 10.8.1

PCI DSS CONTROL 10.9

Control Objective: The organization ensures that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. [201]

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for monitoring all access to network resources and cardholder data are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.

Procedures: Policies are emailed and posted to the City's Intranet site. Policies are also distributed through the City's security awareness training system.

[201] PCI DSS v3.2 Requirement 10.9