The City *of*
WAUKESHA
Information Technology

ITSec 10: TRACKING ACCESS TO SENSITIVE DATA POLICY

Responsible Business Unit: IT	Creation Date: 5/17/18
Affected Business Unit: All	Effective Date: 7/3/2018
Created by: Chris Pofahl	Expiration Date: [Expiration Date]

Introduction

It is critical to have a process or system that links user access to system components accessed. Audit logs provide the ability to trace back suspicious activity to a specific user

Purpose

Requirement 10 of PCI DSS requires Logging mechanisms and the ability to track user activities for 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. In addition, all sensitive data including, but not limited to Bank Account and routing numbers, Medical Terms and Personal Identifiable Information (PII), should be handled in the same manner as card holder data. PII includes, but is not limited to U.S. Individual Taxpayer Identification Number (ITIN),U.S. Social Security Number (SSN),U.S. / U.K. Passport Number, U.S. Driver's License Number, U.S. Social Security Number (SSN).

Scope

1. **Policy Justification**
   a. This Policy related document
   b. Additionally, this Policy related document insures the integrity, availability, and security of the City of Waukesha’s digital assets.
2. **Affected Staff**
   a. All City departments, offices, divisions, and agencies
   b. All represented and non-represented employees, contractors, and temporary workers
3. **Significantly Related Documents and Policies**
   a. ITSec 1: FIREWALL CONFIGURATION POLICY
   b. ITSec 2: SYSTEM AND PASSWORD POLICY
   c. ITSec 3: STORING SENSITIVE DATA POLICY
   d. ITSec 4: TRANSMISSION OF SENSITIVE DATA POLICY
   e. ITSec 5: ANTIVIRUS POLICY
   f. ITSec 6: VULNERABILITY MANAGEMENT POLICY

g. ITSec 7: ACCESS TO SENSITIVE DATA POLICY
h. ITSec 8: USER ACCESS AND AUTHENTICATION POLICY
i. ITSec 9: PHYSICAL ACCESS TO SENSITIVE DATA POLICY
j. ITSec 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA
k. ITSec 11: TESTING SECURITY SYSTEMS AND PROCESSES POLICY
l. ITSec 12: MAINTING AN INFORMATION SECURITY POLICY
m. ITSec 13: SECUTIY AWARENESS TRAINING POLICY
n. ITSec 14: DISPOSING OF SENSITIVE DATA POLICY

4. Policy Maintenance

a. Review this policy annually by Information Technology Board

5. Policy Statement

a. This procedure covers all logs generated for systems within sensitive data environments, based on the flow of cardholder data over the City of Waukesha network, including the following components:
    i. Operating System Logs.
    ii. Database Audit Logs.
    iii. Firewalls & Network Switch Logs.
    iv. IDS Logs.
    v. Antivirus Logs.
    vi. Video recordings.
    vii. File integrity monitoring system logs.

b. Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.

c. Review of logs is to be carried out by means of the City of Waukesha's network monitoring system.

d. The following personnel are the only people permitted to access log files: IT Incident Response Team.

e. The network monitoring system software should configured to alert the City of Waukesha Incident Response Team to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to:

f. A dashboard browser-based interface, monitored by the City of Waukesha IT Incident Response Team.

g. Email / SMS alerts to the City of Waukesha IT Incident Response Team.

h. The City of Waukesha IT Incident Response Team also receives details of email alerts for informational purposes.

i. The following Operating System Events are configured for logging, and are monitored by the network monitoring system:
    i. Any additions, modifications or deletions of user accounts.
    ii. Any failed or unauthorized attempt at user logon.
    iii. Any modification to system files.

iv. Any access to the server, or application running on the server, including files that hold cardholder data.

v. Actions taken by any individual with root or administrative privileges.

vi. Any user access to audit trails.

vii. Any creation or deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

j. The following Database System Events are configured for logging, and are monitored by the network monitoring system (the City of Waukesha to define software and hostname):

i. Any failed user access attempts to log in to the Oracle database.

ii. Any login that has been added or removed as a database user to a database.

iii. Any login that has been added or removed from a role.

iv. Any database role that has been added or removed from a database.

v. Any password that has been changed for an application role.

vi. Any database that has been created, altered, or dropped.

vii. Any database object, such as a schema, that has been connected to.

viii. Actions taken by any individual with DBA privileges.

k. The following Firewall Events are configured for logging, and are monitored by the network monitoring system (the City of Waukesha to define software and hostname):

l. ACL violations.

i. Invalid user authentication attempts.

ii. Logon and actions taken by any individual using privileged accounts.

iii. Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified).

m. The following Switch Events are to be configured for logging and monitored by the network monitoring system (the City of Waukesha to define software and hostname):

i. Invalid user authentication attempts.

ii. Logon and actions taken by any individual using privileged accounts.

iii. Configuration changes made to the switch (e.g., configuration disabled, added, deleted, or modified).

n. The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system (the City of Waukesha to define software and hostname):

i. Any vulnerability listed in the Common Vulnerability Entry (CVE) database.

ii. Any generic attack(s) not listed in CVE.

iii. Any known denial of service attack(s).
iv. Any traffic patterns that indicated pre-attack reconnaissance occurred.
v. Any attempts to exploit security-related configuration errors.
vi. Any authentication failure(s) that might indicate an attack.
vii. Any traffic to or from a back-door program.
viii. Any traffic typical of known stealth attacks.

o. The following File Integrity Events are to be configured for logging::
   i. Any modification to system files.
   ii. Actions taken by any individual with Administrative privileges.
   iii. Any user access to audit trails.
   iv. Any Creation or Deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

p. For any suspicious event confirmed, the following must be recorded on F17 - Log Review Form, and the City of Waukesha [ROLE NAME] informed:
   i. User Identification.
   ii. Event Type.
   iii. Date & Time.
   iv. Success or Failure indication.
   v. Event Origination (e.g. IP address).
   vi. Reference to the data, system component or resource affected

6. Enforcement

a. Process Violation – See City of Waukesha HR Policy *B20 - Software Usage and Standardization* approved this 2nd day of February 2010.

b. Additionally, see related regulation (governance, security, regulatory, HIPAA, SOX, ITIL, ISO, COBIT, PCI DSS, Homeland Security, State of Wisconsin, Federal Government, etc.) as applicable. U.S. State Breach Notification Laws, U.S. State Social Security Number Confidentiality Laws, U.S. Patriot Act, U.S. Federal Trade Commission (FTC) Consumer Rules, U.S. Health Insurance Act (HIPAA).

7. Standards Supporting this Policy

a. PCI DSS
b. U.S. State Breach Notification Laws
c. U.S. State Social Security Number Confidentiality Laws
d. U.S. Patriot Act
e. U.S. Federal Trade Commission (FTC) Consumer Rules
f. U.S. Health Insurance Act (HIPAA).

8. Procedures Enforcing this Policy

Approval

The Person(s) listed below approve this ITSec 10: TRACKING ACCESS TO SENSITIVE DATA POLICY

Approval guideline for IT use on the date specified.

Approver Name	**Approved On**
[Approved by]	[Approved]