ITSec 9: PHYSICAL ACCESS TO SENSITIVE DATA POLICY

Responsible Business Unit: IT
Affected Business Unit: All
Created by: Chris Pofahl

Creation Date: 5/17/2018
Effective Date: 7/3/2018
Expiration Date: [Expiration Date]

Introduction

Access to sensitive information in both hard (physical files) and soft (electronic) media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

Purpose

Requirement 9 of PCI DSS requires any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

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**
    ITSec 1: FIREWALL CONFIGURATION POLICY
    ITSec 2: SYSTEM AND PASSWORD POLICY
    ITSec 3: STORING SENSITIVE DATA POLICY
    ITSec 4: TRANSMISSION OF SENSITIVE DATA POLICY
    ITSec 5: ANTIVIRUS POLICY
    ITSec 6: VULNERABILITY MANAGEMENT POLICY

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

4. **Policy Maintenance**
    a. Review this policy annually by Information Technology Board
5. **Policy Statement**
    a. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
    b. Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
    c. Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
    d. Employees should ensure that technologies are used and setup in acceptable network locations
    e. A list of devices that accept payment card data should be maintained.
    f. The list should include make, model and location of the device
    g. The list should have the serial number or a unique identifier of the device
    h. The list should be updated when devices are added, removed or relocated
    i. POS devices surfaces should be periodically inspected to detect tampering or substitution.
    j. Personnel using the devices should be trained and aware of handling the POS devices
    k. Personnel using the devices should verify with the IT Department the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
    l. Personnel using the devices should be trained to report suspicious behavior and indications of tampering of the devices to the appropriate personnel.
    m. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
    n. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
    o. Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.

p. Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
q. Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
r. Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on City of Waukesha sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
s. Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorized.
t. All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
u. Strict control must be maintained over the external or internal distribution of any media containing card holder data and must be approved by management, and comply with IT Security Policies related to sensitive data, which includes but is not limited to: transmitting, storing , disposing and accessing sensitive data.
v. Strict control must be maintained over the storage and accessibility of media.
w. All computers that store any sensitive data must have a password protected screensaver enabled to prevent unauthorized use.

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 9: PHYSICAL ACCESS TO SENSITIVE DATA POLICY

Approval guideline for IT use on the date specified.

Approver Name	Approved On
[Approved by]	[Approved]