The City of
WAUKESHA
Information Technology

ITSec 7: ACCESS TO SENSITIVE DATA POLICY

Responsible Business Unit: IT	Creation Date: 4/27/2018
Affected Business Unit: All	Effective Date: 4/27/2018
Created by: Chris Pofahl	Expiration Date: [Expiration Date]

Introduction

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

Purpose

Requirement 7 of PCI DSS calls for all access to sensitive cardholder should be controlled and authorized. Any Job functions that require access to cardholder data should be clearly defined. Additionally, this policy defines how other sensitive data should be accessed. Sensitive data includes, but is 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. 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. Regarding credit card information, any display of the card holder should be restricted at a minimum of the first 6 or the last 4 digits of the cardholder data.
   b. Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
   c. Privileges should be assigned to individuals based on job classification and function (Role based access control)
   d. Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
   e. No other employees should have access to this confidential data unless they have a genuine business need.
   f. If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained.
   g. The City of Waukesha will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
   h. The City of Waukesha will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
   i. The City of Waukesha will have a process in place to monitor the PCI DSS compliance status of the Service provider.
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 7: ACCESS TO SENSITIVE DATA POLICY
Approval guideline for IT use on the date specified.

Approver Name	Approved On
[Approved by]	[Approved]