The City of
WAUKESHA
Information Technology

ITSec 3: STORING SENSITIVE DATA POLICY

Responsible Business Unit: IT	Creation Date: 1/03/2017
Affected Business Unit: All	Effective Date: 3/2/2017
Created by: Chris Pofahl	Expiration Date: [Expiration Date]

Introduction

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities.

Purpose

Requirement 3 of PCI DSS defines how card holder data is stored. This Policy Document addresses the methods for storing sensitive data. **In addition, all 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. ITAV-0.1 ANTIVIRUS POLICY
   b. ITVS-0.1 VULNERABILITY SCANNING POLICY
   c. ITFW-0.1 FIREWALL CONFIGURATION POLICY
4. **Policy Maintenance**
   a. Review this policy annually by Information Technology Board
5. **Policy Statement**

   a. All sensitive cardholder data stored and handled by the City of Waukesha and its employees must be securely protected against unauthorized use at all times. Any sensitive card data that is no longer required by the City of Waukesha for business reasons must be discarded in a secure and irrecoverable manner.
   b. If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
   c. PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,
   d. It is strictly prohibited to store:
      i. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
      ii. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
      iii. The PIN or the encrypted PIN Block under any circumstance.

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 ITSSD-0.1 STORING SENSITIVE DATA POLICY Approval guideline for IT use on the date specified.

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