# ITSec 4: TRANSMISSION OF SENSITIVE DATA POLICY

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

Creation Date: 5/17/2018
Effective Date: 6/19/2018
Review Date: 7/3/2019

## Introduction

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

## Purpose

Requirement 4 of PCI DSS defines how card holder data is transmitted. This Policy Document addresses the methods for transmitting card holder data, and other 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. 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
o. PCI DSS Cybersecurity Policy

**4. Policy Maintenance**

a. Review this policy annually by Information Technology Board

**5. Policy Statement**

a. All sensitive data must be protected securely if it is to be transported physically or electronically.

~~b. Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.~~

~~c. If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism.~~

~~d.~~b.

Strong cryptography and security protocols must be used to safeguard sensitive data during transmission over open, public networks. ~~The transportation of media containing sensitive cardholder data to another location must be authorized by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.~~

**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 4: TRANSMISSION OF SENSITIVE DATA POLICY

Approval guideline for IT use on the date specified.

| **Approver Name** | **Approved On** |
|---|---|
| [Approved by] | [Approved] |
| ITB | 6/6/2018 |
| Common Council | 6/19/2018 |