Introduction

Secure Compliance Solutions (SCS) shall provide Subject Matter Experts to complete an External Penetration Test of the Wheaton Park District's information system, in accordance with PCI DSS regulations. Using standard Vulnerability Assessment tools, SCS will identify threats and weaknesses of the Park District's network perimeter defenses. SCS Penetration Testers will attempt to exploit those weaknesses; acting from the perspective of an external attacker.

The objectives of the Penetration Test are twofold:

1. To determine vulnerabilities or other attack vectors a malicious user can exploit to gain unauthorized access to assets that affect the fundamental security of the system, files, logs and/or cardholder data.
2. To confirm that the applicable controls, such as scope, vulnerability management, methodology, and segmentation, required in PCI DSS are in place, and to identify where security controls are inadequate.

At the conclusion of the Penetration Test, SCS shall furnish to Wheaton Park District, a comprehensive report detailing identified security weaknesses, along with suggested corrective actions.

Opportunity Statement

The Wheaton Park District is a municipal government agency that provides leisure and recreational services to the city of Wheaton, IL. Wheaton Park District takes payment for services in the form of payment cards, and thus is subject to the Payment Card Industry-Data Security Standard (PCI-DSS) regulations.

The Wheaton Park District Chief Information Officer has requested that Secure Compliance Solutions submit this Statement of Work to describe the scope, terms of service and price for a Penetration Test to be conducted in 2017, prior to annual self-attestation through the PCI Standards Council. A Penetration Test is a fundamental requirement (11.3) of the PCI DSS v.3.2 regulation. In accordance with PCI DSS direction, SCS shall follow NIST SP. 800-115 methodology guidance in the execution of this test.

In accordance with PCI-DSS regulations, SCS must complete this test in 2017.

Services Overview

SCS will attempt to compromise the access controls on designated systems by employing the following methodology:

- **Planning** – SCS shall work with the Wheaton Park District CIO to fine tune the scope and timing of the test. At that point, the CIO shall notify the Park District's Managed IT Service Provider, Advanced Intelligence Engineering (AIE) of the pending test. By leaving AIE out of the pre-test planning, the Penetration Test will also test AIE's Incident Response capability. No actual testing will occur during this phase. (1 day)

- **Discovery** – SCS will connect to the network via the public internet. At the start of the test, SCS will run a variety of information gathering tools in order to enumerate ports and protocols exposed by the Park District security devices. SCS shall scan any computers or devices found during discovery for vulnerabilities, using a wide variety of tools and techniques. The tools and techniques used will be consistent with current industry trends regarding exploitation of vulnerabilities. (2 days)
    - The vulnerability scans will include all 41 externally-facing IP addresses.
- **Attack** –SCS will attempt to exploit weaknesses, and attempt to gain further access into the network. SCS will attempt to penetrate the network up to and including the point at which sensitive data can be accessed. SCS shall not remove data or cause systems to falter because of its testing. (2 days)
    - SCS will run an uncredentialled (Black Box) Penetration Test.
- **Reporting** – Throughout the penetration test, SCS will document and record the process, will detail security vulnerability findings as we discover them, and provide recommendations for vulnerability remediation. SCS will provide a final report of the penetration test which will include data accessed via the network, and any information regarding exploitation of vulnerabilities and the attempt to gain access to sensitive data. (4 days)
    - Within the duration of the test, upon request, SCS shall rerun select components of its testing, following AIE's remediation efforts, to ultimately reflect WPD's/AIE's security strengthening progress.

Scope

SCS will offer the following security services:

- Subject matter expertise and the toolset to execute an external penetration test on customer designated devices. We can operate with as little or as much knowledge as desired by the customer contact.
- Vulnerability Assessment – Using a variety of software scanning tools and technical tests, SCS will identify vulnerabilities presented by the Wheaton Park District network provided in Appendix A. As part of the final report, SCS will provide an interpretation of vulnerability scan results including suggested remediation actions.
- System Exploitation – SCS will attempt to exploit or gain entry into all systems within the project scope outlined in Appendix A.

Out of Scope

- Based on SCS' understanding of the Park District's internal network security controls, we assume the entire network comprises the cardholder data handling environment. Therefore, we will not conduct internal subnet to subnet scanning or testing.
- SCS will not test wireless access as part of this exercise.
- SCS will not conduct social engineering testing of any kind during this exercise.
- SCS will not conduct physical environment penetration testing during this exercise.

Project Assumptions

- AIE IT Administrators will be aware of the Penetration Test in advance of its execution.
- Wheaton Park District does not currently maintain a Disaster Recovery Plan.
- Wheaton Park District does not currently maintain a formal IT Change Management Process.
- SCS Penetration Tester(s) will attempt to gain administrative access to systems as part of its test.
- The Wheaton Park District systems environment is comprised primarily of Windows and Linux servers, web applications and networking/security appliances.
    - The organization's Exchange (mail) environment and Security Camera Administration Portal are accessible from the Internet.
- SCS will execute all penetration testing exercises up to 40 hours of effort to attempt to exploit the cardholder data handling environment.
- While conducting the Penetration Test, SCS Security Analysts will monitor the Park District's AlienVault environment to validate its appropriate detection of unauthorized attempts to gain access within the environment.

Project Duration

- The External Penetration Test will take approximately 7 Business Day(s) to complete, with a final report being provided within 2 week(s) after the work is completed.
    - The Penetration Test will be considered complete once all efforts have been exhausted up to a maximum of 40 testing hours.
- SCS and Client will jointly determine the start date and allowable times for the engagement testing to be started within 30 days of contract signature.

Terms and Conditions

Secure Compliance Solutions will provide the professional certified Security specialist and supporting staff to complete the scoped work

Deliverables

SCS will provide the following deliverables as part of this engagement:

#	Deliverable	Description
1	Penetration Testing Report	A comprehensive report defining technical and process-based weaknesses associated with Wheaton Park District's Information Security posture and strategy, along with recommendations for corrective actions.

Performance of Services

Initial and additional consulting or other optional custom services and related deliverables must be documented and signed by authorized representatives of both parties.

Changes: Any changes to the obligations of either party, or to any other material aspect of this Proposal will require a written change order signed by authorized representatives of both parties that describes the changes and any related cost or schedule adjustments.

Delivery Approach Engagement Milestones

Estimation of engagement hours is as follows over a 3 week period:

Activity	Estimated Hours	Steps
Vulnerability Scan, Penetration testing and output evaluation	35 - 40	• Configure and run vulnerability scan • Evaluate results • Exploit system vulnerabilities • Develop Pen Test Report
Project Management and Finalize Report including suggested remediation	20	• Complete Pen Test Report and Recommendations
Report Presentation	2	• Present report findings to customer.

These estimates may change, based on client availability and complexity of requirements. Any deviation greater than 20% will be reported to the client Representative for authorization to continue the work.

Site and Resource Access

If required and approved, Wheaton Park District shall provide to Secure Compliance Solutions personnel access to facilities via badges, keys, and /or escorts to perform the agreed work. Wheaton Park District will assist in the identification and ensure access to key staff and availability to work with SCS. Any project delays related to Client site and/or resource access may result in deliverable delays.

Proposal Assumptions

- All time frames and milestones are estimates. Factors outside of the SCS control can/ will impact estimates and include but are not limited to:
    - Wheaton Park District team response times to requests, operational limitations, omitted information and business decisions.
    - Third party vendor performance
- All applicable technical specifications and current documentation and regional feedback is provided to SCS in a timely manner.
- All documentation provided in this engagement will be provided in English only.
- This SOW does not include subsequent phases with actions such as:
    - Assistance to fully address/ remediate all vulnerabilities identified
    - Building a program to proactively manage system vulnerabilities

Professional Service Fees
Fixed Fee: $9,500

SCS will provide ethical hacking and penetration testing services for this project scope on a flat fee basis of $9,500 over a three-week engagement.

By mutual agreement, Wheaton Park District shall pay all applicable approved travel charges which includes reasonable and customary travel and living expenses incurred in the performance of Services. Unless otherwise specified in this Proposal, any applicable travel charges will be billed at actual costs as incurred by Secure Compliance Solutions.

Remediation Activities
If Wheaton Park District elects to engage SCS for remediation of any identified vulnerabilities found during the initial scan, the work will be billed to Wheaton Park District on a Time and Materials basis, at a rate of $185/hour. However, if remediation work can be completed within the monthly five hour allowance as defined in the SCS MSSP Statement of Work, SCS will not charge Wheaton Park District any additional money.

Prior to the commencement of remediation work, the Wheaton Park District representative shall inform SCS in writing of its authorization to execute the remaining work

Payments

Wheaton Park District will be invoiced on a monthly basis for the work performed in support of this Statement of Work. Payment shall be in U.S. dollars and will be due thirty (30) days from the date of each invoice. Payments made later than the due date are subject to and may incur accrued interest from the date due to the date paid up to the maximum percentage allowed by applicable law. If a payment is late, SCS shall be entitled to suspend performance of the services and, at its option, terminate the proposal on written notice.

Agreed to:
Secure Compliance Solutions (SCS)

By: _____
Authorized Signature

Name: Andrew L. Soodek

Date: 10/31/2017

Agreed to:
Wheaton Park District

By: _____
Authorized Signature

Name: _____

Date: 10/30/17

Appendix A

Location	Public IP Address	Known Use
Arrowhead	173.161.118.217	
	173.161.118.218	firewall
	173.161.118.219	Security Cameras
	173.161.118.220	
	173.161.118.221	
	104.193.118.46	firewall
	166.241.105.8	firewall
Clocktower	96.95.115.130	firewall
Community Center	63.250.255.14	firewall
	63.250.220.17	
	63.250.220.18	
	63.250.220.19	
	63.250.220.20	outbound traffic from servers
	63.250.220.21	Exchange
	63.250.220.22	webtrack
	63.250.220.23	DC
	63.250.220.24	
	63.250.220.25	
	63.250.220.26	
	63.250.220.27	
	63.250.220.28	
	63.250.220.29	
	63.250.220.30	
	63.250.220.31	
	104.193.118.162	firewall
	50.76.64.241	firewall
	50.76.64.242	
	50.76.64.243	
	50.76.64.244	
	50.76.64.245	
Cosley Zoo	96.81.219.77	firewall
Leisure Center	96.92.247.57	firewall
Lincoln Marsh	96.95.65.117	firewall
	104.193.118.150	firewall
Museum	23.25.21.113	firewall
	104.193.118.146	firewall
Northside pool	96.81.194.85	firewall
Parks Services Center	96.92.220.237	firewall
	104.193.118.42	firewall
Prairie	50.198.41.209	firewall
	104.193.118.22	firewall