Statement of Work Number 20150517-01

This Statement of Work ("SOW") is entered into by and between **SecureWorks, Inc.**, with its principal place of business located at **One Concourse Parkway, Suite 500, Atlanta, GA 30328** ("**SecureWorks**") and **City of Columbus** with its principal place of business located at **1111 E. Broad St, Columbus, Ohio** ("**Customer**") as of the SOW Effective Date, which is defined by the latest date in the signature blocks below. SecureWorks and Customer hereafter referred to together as the "parties", and each, a "party". This SOW is governed by and subject to the terms and conditions of: (a) the separately signed agreement executed by the parties that expressly authorizes Customer to order the services described herein from SecureWorks, or (b) the SecureWorks Managed Services Agreement which was signed by SecureWorks on December 5, 2012 (the "MSA"). Capitalized terms not defined herein shall have the meaning ascribed to them in the MSA.

1 Scope

Under this SOW, SecureWorks will provide Customer with **PCI Gap Analysis** service ("Service") as such Services are described in detail below.

1.1 PCI Gap Analysis

SecureWorks is an authorized Qualified Security Assessor (QSA) Company by the Payment Card Industry Security Standards Council (PCI SSC). SecureWorks will review and conduct compliance validation on select system components where cardholder data is processed, stored or transmitted, unless otherwise specified. We will do so using a combination of comprehensive review and sampling methodologies.

We will include in scope any system(s) or system component(s) related to authorization and settlement where cardholder data is processed, stored or transmitted. We will also include the following:

- All external connections into network(s) or appropriately deployed network segment(s) that store transmit or process cardholder data. This includes employee remote access, third party access for processing and maintenance.
- All connections to and from the authorization and settlement environment, for example, connections and infrastructure for employee access, including devices like firewalls and routers.
- Any data repositories outside of the card holder areas and authorization and settlement environments where account numbers are stored.
- Outsourcing and PCI vendor management - If you are an organization that outsources processing, transmitting or storage of cardholder data to third-party service providers, and a Report On Compliance is part of this Statement of Work, then we must document the role of each service provider. However, these service providers are responsible for validating their own compliance with the PCI Data Security Standard (PCI DSS) independent of their customers. Additionally, merchants and service providers must contractually require all associated third parties with access to cardholder data to adhere to the PCI DSS. Customer Environment
- City of Columbus is a Level 2 merchant
- City of Columbus is required to complete an SAQ -
- SecureWorks will complete the SAQ and provide an AOC
- The network is segmented to reduce the scope of the Cardholder Data Environment
- Up to 32 servers/workstations/other that store/process/transmit cardholder data

- Up to 5 applications that store/process/transmit cardholder data
- Up to 1 interview/elicitation sessions to complete onsite at one of the facilities listed.
- Assessment will be performed from one of the facilities listed in Locations of Services section below

1.2 Out of Scope

Locations, devices or personnel that are not specifically listed as in scope are out of scope.

Note: If any IP addresses, hosts, facilities or web applications within scope are owned or hosted with a service provider or other third party, it will be necessary for Customer to obtain permission from that party before SecureWorks will perform any Services, or you may provide a suitable alternate environment for the performance of the Service.

1.3 Location of Services

The Services may be performed either onsite at the Customer location defined below and/or remotely at one or more SecureWorks secure facilities. SecureWorks and Customer will determine the location of the performance of the Services to be performed hereunder.

In most cases, the collection of the required Customer Data will be gathered onsite and the drafting of the Report (as defined below) and recommendations will be built remotely.

Customer Location:

1601 Arlingate Lane, Columbus, Ohio

2 Timeline and Services Schedules

- Onsite work will be performed Monday-Friday, 8 am - 6 pm Local time.
- Remote work will occur Monday-Friday, 8 am - 8 pm for the assigned resource(s)
- Work performed outside of the hours listed above as requested or required by Customer will incur additional Service charges.

3 Methodology

3.1 PCI Gap Analysis

SecureWorks will rely on guidance from the card brands compliance programs, and the PCI SSC. For certain technical control testing methods, SecureWorks relies on our own subject matter expertise regarding current and emerging risks and vulnerabilities, as there is no standards body capable of keeping current with emerging and fast changing technical risk categories.

3.1.1 Phase I: Review the Presumed Cardholder Area

Without adequate network segmentation (or "flat network"), the entire network is in scope of the PCI DSS. Network segmentation can be achieved through internal firewalls, routers with appropriate access control lists, or other combinations of technologies that restrict access to a network segment. A critical component to reducing the scope of the cardholder environment is a clear and effective restriction of a network segment to the cardholder environment. We will review the following types of formal documentation you have:

- Network diagrams

- Host configurations and standards
- System configurations
- System architecture
- Policies and procedures
- Technical standards
- Encryption standards
- Previous test and scan results
- Other documentation as needed

We will perform technical testing both inside and outside the presumed cardholder area. Inside the cardholder area, our testing will focus on what cardholder data exist and where. This discovery phase often uncovers devices that we may be able to move outside, reducing overall cost of compliance. Testing outside the presumed cardholder area will allow us to identify any data which has gone unnoticed - a frequent contributing factor in breaches.

3.1.2 Phase II: PCI DSS Gap Analysis

We will analyze your controls and how they compare to the PCI DSS. We will review the documentation and conduct a series of interviews with key personnel. After we have an initial understanding of the most probable definition of the cardholder area, we will evaluate your controls as compared to the PCI DSS. We will evaluate how you:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

This phase mainly focuses on your PCI program as documented, with limited technical testing or validation. Instead, we want to see how you have designed your program and controls. The design is critical to reducing the scope and cost of compliance, as well as to performing validation. If your assessor doesn't understand the controls as designed, it is not possible to validate that they both function properly and fully mitigate risk. Where gaps exist in the documentation of your controls, we will work with you to determine what controls exist and how to formalize them.

3.1.3 Phase III: Controls Validation

SecureWorks will validate that controls in place are consistent with those required by the PCI DSS. We will be checking to make sure that the controls are implemented as designed and documented, not merely that they exist. This phase includes technical testing, observation, review of configurations, etc. We may also review previous testing conducted, such as penetration tests, quarterly scans, wireless testing and any other technical testing you have performed.

3.1.4 Phase IV: Remediation Plan Development

Our remediation plan will focus on true security, compliance with the PCI DSS and affordability. Remediating gaps in your program can be an expensive undertaking if it isn't done right the first time. If your remediation plan doesn't focus on true security, you add the risks of negative publicity, increased regulatory scrutiny and cleaning the direct effects of a breach. And after all the expensive and time consuming work you've already done, you'll have the same or greater work effort to remediate later.

We will discuss your gaps, various options you may have regarding compensating controls, network segmentation, technology implementation and other important decision points regarding your security and compliance efforts. We will work with you to develop a remediation plan that is right for your organization, appropriately reduces risk and takes into account compensating controls, where appropriate.

We will work to architect a solution that takes into consideration options other than technologies and services on top of your current infrastructure. Instead, we will look for ways to reduce the scope of your cardholder data environment and to simplify your ongoing maintenance. This "scope-reducing approach" results in a quicker time to remediation, lower costs and less work on you after you are compliant.

3.1.5 PCI Remote Remediation Retainer Option

You will have access to SecureWorks' PCI experts for up to one year from the delivery of the PCI engagement. After creating the customized remediation plan with you, we want to make sure that you are able to implement the appropriate changes in your environment. We will establish a timeline for periodic checkpoints with your consultant to discuss your progress and provide guidance. You can feel confident in knowing that we will stand by our recommendations and help you implement the changes needed to become PCI compliant.

If you are audited during this time on your PCI compliance by the card brands, the PCI SSC, your acquiring bank, or another QSA company, we can be available to answer the tough questions. We will support our findings and help guide you through the process.

Each organization differs in their remediation and testing needs. We haven't done the assessment, so it is impossible to know how much support you may need. SecureWorks understands this and wants to provide you with the right amount of support to get you compliant without excessive cost. Therefore, we will provide you with hours for remote support, testing, advisory services and guidance as a part of this engagement. If you find that you need more than what we've agreed to we are here to help.

SecureWorks will provide formal policies, procedures, standards and guidance in template form to cover PCI requirements. These documents were created specifically to help organizations satisfy PCI requirements. These documents are only templates, but we can help you customize them to your environment as a part of our remediation support. We can build your documentation in a way that will accurately reflect your program and controls, but just as importantly will reflect what QSAs and auditors want to see.

4 Deliverables

4.1 PCI Gap Analysis

SecureWorks will provide preliminary draft findings to the technical point of contact for review and clarification. The final report will be issued after review and discussion are complete. Presentation of the findings and exact deliverables are custom tailored to the type of work performed, and to customer needs. Final reporting and deliverables will be defined during the project, as well as interim or ad-hoc reporting. SecureWorks deliverables typically follow a standard format with two sections:

The **first section** is targeted toward a non-technical audience - Senior Management, Auditors, Board of Directors and other concerned parties:

- **Executive summary:** A jargon and buzz-word free true executive-level summary.
- **Summary of findings and recommendations:** Describes the environment and high-level findings and root causes. We make recommendations based on risk to your organization.
- **Compliance status:** Describes the compliance status measured against the PCI Standard.

The **second section** is targeted to technical staff and provides more granular detail:

- **Summary of methods:** Contains details specific to the engagement methodology.
- **Detailed findings and recommendations:** Documents the details of any findings, as well as recommendations for remediation. Evidence of controls and information sufficient to replicate the findings is included. Recommendations are based on these root causes and prioritized for a risk-based remediation with an estimation of relative work effort. Any strong controls in place that have been identified are described, as well as their impact to the security of the organization.
- **Cardholder data environment:** Describes the PCI Cardholder Data Environment and any network segmentation controls in place.
- **Attachments:** Provides details and specific examples are provided, including screen shots, technical details, code excerpts and other relevant observations. This section also contains documents or data that are relevant but do not fit in other categories.

4.2 Report Timing

Within three (3) weeks of completing a Project, SecureWorks will issue a draft formal Report to Customer designated point of contact. Customer shall have two (2) weeks from delivery of such draft formal Report to provide comments concerning the nature and scope of the Project to be included in the final Report (the "Report Review Period"). If there are no comments received from Customer before the expiration of the Report Review Period, the Report shall be deemed final and SecureWorks will finalize for distribution.

5 Service Fees and Expenses

5.1 Service Fees

PCI Gap Analysis: $27,500.00_USD

5.2 Optional Services

RETAINER Option	$4,000 USD _____Customer Initials
Fees for PCI: Remediation Retainer	
Retained Hours	16
Retained Hourly Rate	$250.00
Cost	$4,000.00 USD

5.3 Billing for the Services

- Services Fees are 50% billable upon SOW execution
- 50% billable upon delivery of draft report

Terms for PCI Remediation Retainer:

- 100 percent billable upon contract execution.
- Hours will be calculated in quarter-hour increments.
- Includes hours spent on delivering work, reporting, project management and all other work performed in this engagement.
- Any unused hours at the end of the term will be forfeited.

- This is a fixed-work-effort contract; not a fixed-price contract. Additional blocks of hours may be retained at the rate above by change order or an additional Statement of Work. In order to avoid interruptions in service delivery, customer may authorize further work effort through email at a rate of $295 per hour, invoiced monthly.

5.4 Out-of-Pocket Expenses

The Service fees outlined above include all incidental out-of-pocket expenses such as report preparation and reproduction, faxes, copying, etc.

The following out-of-pocket expenses are included in the Service fees: those related to transportation, meals and lodging to travel to perform the Services.

6 Service Scheduling

SecureWorks will contact Customer designated representative within five business days after the execution of this Statement of Work to schedule a time for the services outlined hereunder to be performed. Services outlined within this SOW require a minimum of four (4) weeks advance notification to schedule. SecureWorks will use commercially reasonable efforts to meet Customer requests for dates and times for the delivery of Services, including performance of the Services during Customer designated downtime windows, after business hours, meeting Customer deliverable deadlines, and other Customer scheduling requests. An email confirmation of an agreed upon schedule, sent by SecureWorks, confirmed and returned by email by Customer, shall constitute formal acceptance of such schedule. Once scheduling of any onsite work at Customer facility has been mutually agreed to, any changes by Customer to the onsite work within two (2) weeks of the onsite work to be performed will incur a $2,000 re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by SecureWorks.

7 Customer Obligations

Customer acknowledges that SecureWorks' ability to perform the Services hereunder is contingent upon the following:

- Customer resources are scheduled and available.
- For onsite Services to be performed, Customer has provided suitable workspace and necessary accesses for SecureWorks' staff and equipment.
- Access to Customer computer systems, devices and network as necessary to perform the Services is made available to SecureWorks.
- Replies to all document requests and other information are timely and in accordance with the delivery dates established in the planning phase.
- Customer scheduled downtime allows adequate time for SecureWorks' performance of the Services.
- Until this SOW is fully executed by both parties, Customer understands that the fees proposed herein are only valid for 90 days from the date received.

8 SOW Term

The term of this SOW shall commence on the SOW Effective Date and terminate on the earlier to occur of (i) the date which is one (1) year thereafter, or (ii) the completion of the Services (the "SOW Term").

The term of the Services shall commence upon the completion of a kick-off call between SecureWorks and Customer and terminate on the earlier to occur of (i) the SOW Term, or (ii) the completion of the Services (the "Services Term").

Upon completion of the Services, the Customer designated contact will receive an email confirmation from SecureWorks. Unless otherwise notified in writing to the contrary by the Customer designated contact within thirty (30) days of such email confirmation, the Services and this SOW shall be deemed complete.

9 Disclaimers

9.1 Onsite Services

Notwithstanding SecureWorks' employees' placement at the Customer location, SecureWorks retains the right to control the work of such employees. For international travel, onsite Services may require additional documentation, such as Visas, visitor invitations, etc. which may affect timing of the Services and reimbursable expenses.

9.2 Security Services

Should this SOW include security scanning, testing, assessment, forensics, or remediation Services ("Security Services"), Customer understands that SecureWorks may use various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. Customer hereby authorizes SecureWorks to perform such Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services or otherwise approved by Customer from time to time) on network resources with the internet protocol ("IP") Addresses identified by Customer. Customer represents that, if Customer does not own such network resources, it will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to SecureWorks, to permit SecureWorks to provide the Security Services. SecureWorks shall perform the Security Services during a timeframe mutually agreed upon with Customer. The Security Services, such as penetration testing or vulnerability assessments, may also entail buffer overflows, fat pings, operating system specific exploits, and attacks specific to custom coded applications but will exclude intentional and deliberate denial of service ("DoS") attacks. Furthermore, Customer acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding the Customer systems and accepts those risks and consequences. Customer hereby consents and authorizes SecureWorks to provide any or all the Security Services with respect to the Customer systems. Customer further acknowledges it is Customer responsibility to restore network computer systems to a secure configuration after SecureWorks' testing.

9.3 Compliance Services

Should this SOW include compliance testing or assessment or other similar compliance advisory Services ("Compliance Services"), Customer understands that, although SecureWorks' Compliance Services may discuss or relate to legal issues, SecureWorks does not provide legal advice or services, none of such Compliance Services shall be deemed, construed as or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any

written summaries or reports provided by SecureWorks in connection with any Compliance Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.

9.4 Payment Card Industry (PCI) Compliance Services

Should this SOW include PCI compliance auditing, testing or assessment or other similar PCI compliance advisory Consulting Services ("PCI Compliance Services"), Customer understands that SecureWorks' PCI Compliance Services do not constitute any guarantee or assurance that security of Customer systems, networks and assets cannot be breached or are not at risk. These PCI Compliance Services are an assessment, as of a particular date, of whether Customer systems, networks and assets, and any compensating controls meet the applicable PCI standards. Mere compliance with PCI standards may not be sufficient to eliminate all risks of a security breach of Customer systems, networks and assets. Furthermore, SecureWorks is not responsible for updating its reports and assessments, or enquiring as to the occurrence or absence of such, in light of subsequent changes to Customer systems, networks and assets after the date that the final Report is created, absent a separately signed statement of work expressly requiring the same.

9.5 Record Retention

SecureWorks will retain a copy of the Customer Reports and supporting Customer Data in accordance with SecureWorks' record retention policy, which provides such retention for a period commensurate with such Customer Reports and supporting Customer Data usefulness and SecureWorks' legal and regulatory requirements and SecureWorks' directives.

Unless Customer gives SecureWorks written notice to the contrary prior thereto, then thirty (30) days after delivery of its final report, SecureWorks shall have the right, in its sole discretion, to dispose of all acquired hard drive images and other report backup information acquired in connection with its performance of its obligations under this SOW.

This SOW is agreed to by the parties. Any terms and conditions attached to a purchase order submitted by Customer in connection with this SOW are null and void.

	SecureWorks, Inc.		City of Columbus 1111 E. Broad St, Columbus, Ohio
By:	.....	By:	.....
Printed:	.....	Printed:	.....
Title:	.....	Title:	.....
Date:	.....	Date:	.....

SFDC: