SECUREWORKS STATEMENT OF WORK

STATEMENT OF WORK NUMBER 20150505-03

This **STATEMENT OF WORK ("SOW")** is by and between **SecureWorks, Inc.** ("Dell SecureWorks") and **City of Columbus** with its principal place of business located at **1111 E. Broad St. Suite 300 Columbus, OH 43205** ("Customer"). Unless a separate signed agreement has been executed that expressly authorizes Customer to order all services described herein from Dell SecureWorks, this Statement of Work is subject to and governed by the Dell SecureWorks Master Services Agreement (the "MSA"), which is incorporated by reference in its entirety. The MSA is available at www.Dell.com/securityterms. Any purchase order terms and conditions set forth in your purchase order for the same services are null and void.

1. 0 Scope

Geographic Locations

Some work for this engagement may be performed remotely, as necessary and appropriate. The scope of this engagement includes travel to the following areas:

- Columbus, Ohio 43205

Wireless network testing

- Up to 3 Access Points in scope
- Work will be performed at **one** of the facilities listed in the Geographic locations above.

Timelines and Schedules

- On-site work will occur Monday-Friday, 8 a.m.–6 p.m. local time
- Remote work will occur Monday-Friday, 8 a.m.–8 p.m. Eastern time
- Work required outside of these normal business hours will incur an upcharge to be approved by customer

Out of Scope

- Locations, devices, and personnel not specifically listed above 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 you to obtain permission from that party before Dell SecureWorks will perform testing in writing or through email. Or you may provide a suitable alternate testing environment.

2.0 Statement of Work

Wireless Network (Wi-Fi) Testing

Based on the IEEE 802.11 wireless networking standards, Wi-Fi wireless networks have inherent risks due to their shared physical medium – electromagnetic waves. These networks provide organizations better usability and allow employees or guests to roam throughout the physical location and remain connected. But Wi-Fi technologies also impose risks to an organization. Risks can come from

improperly secured infrastructure, rogue access points and wireless clients themselves.

MAC filtering, WEP encryption and pre-shared keys are no longer effective defensive measures that protect the information and clients using the wireless network. Most of these measures can be bypassed or broken within minutes exposing the internal infrastructure.

Dell SecureWorks will conduct configuration reviews, technical testing and scanning for rogue access point detection. We will passively monitor the wireless network to determine weaknesses first, and then, if requested (see Options), actively attack the network to gain access by breaking encryption keys or bypassing other security measures. Results of the test may include, as appropriate:

- Wi-Fi signal leakage
- Security design flaws
- Encryption keys (WEP/WPA)
- Analysis of defensive measures
- Rogue Access Points
- Wi-Fi client information

Site Survey

Dell SecureWorks will perform a site survey, passively and/or actively searching for rogue devices. Data gathered will be compared to known authorized access points and clients to determine if any rogue devices exist, to the extent possible.

Wireless Connectivity Architecture Evaluation

During our wireless connectivity architecture evaluation we will perform the following tasks:

- Wireless security configuration
- Encryption usage and configuration
- Ability to detect rogue access points or clients
- Overall wireless security controls

Wireless Security Testing

During our wireless security testing we will perform the following tasks:

- Run tests against the wireless access points
- Run tests against the wireless clients
- Attempt to bypass encryption usage and configuration
- Attempt to bypass overall security controls and gain access to a non-public network.

Dell SecureWorks uses a structured and iterative process, testing the network architecture, systems configurations, processes, and procedures that affect the ability to protect your wireless assets from unauthorized access.

At your request, we will attempt to detect, analyze, and compromise the wireless networks in place. We will use wireless specific security tools, such as Net Stumbler the Aircrack suite, Kismet, InSSIDer, etc. If we are successful in compromising the wireless network, we will then document the findings and provide information on how the compromise took place.

Wireless clients are a critical part of the security of a wireless network. However, clients are often overlooked during testing. At your request, Dell SecureWorks can establish rogue access points and attempt to coerce clients to attach, in order to demonstrate the ability of an attacker to compromise laptops and other devices which connect to the wireless network.

This threat exists not only on a corporate campus but also in coffee shops, airports and other public places where laptops may be used. Attackers can take this opportunity to compromise the laptop,

which then reenters the corporate network. Dell SecureWorks has seen many organizations whose internal network has been compromised in exactly this way.

3.0 Deliverables

Draft and Final Report

Dell 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. Dell 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 potential risk to your organization.
- **Remediation priority recommendations:** Prioritizes high-risk findings based on severity of risk including recommendation for curative actions.

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. Descriptions of techniques used and the causes of success or failure are detailed, as appropriate. Vulnerabilities are mapped according to the OWASP Top 10.
- **Attachments:** Provides details and specific examples, 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.

As appropriate, Dell SecureWorks will deliver a presentation outlining preliminary results of the assessment to key stakeholders. The presentation will identify findings, recommendations and next steps. The presentation will be at a level appropriate the audience and the setting. Discussion and feedback are encouraged.

Report Timing

Within three weeks of concluding the work described above, we will issue a draft formal report to your point of contact. The three weeks following delivery of this draft report are your opportunity to provide comments concerning the nature and scope of the engagement to be included in the report. If there are no comments in the three-week comment period, we will finalize the report for distribution. If no changes are required, we encourage you to accept the formal report prior to the three week waiting period to expedite final delivery.

4.0 Timing and Fees

Fees for this engagement are: $8,240 USD

Terms for this engagement

- 50 percent billable before commencement
- 50 percent billable after the draft report is delivered

Out-of-Pocket Expenses

The fees outlined in our scope of services include all incidental out-of-pocket expenses such as report preparation and reproduction, faxes, copying, etc. Fees also include transportation, meals and lodging to travel to perform any of our services.

Scheduling and Reporting

Services outlined within this statement of work require a minimum of 2 weeks advance notification to schedule.

SecureWorks will make commercially reasonable efforts to meet Client's requests for dates and times for the contracted work to be performed, including the work to be performed during Client's designated downtime windows, after business hours, meeting Client deliverable deadlines, and other Client scheduling requests. Email confirmation of an agreed upon schedule, sent by SecureWorks, confirmed and returned by email by the Client, shall constitute formal acceptance of such schedule. Once scheduling of any onsite work has been mutually agreed upon for work at the Client's location, and the schedule is formally accepted by the Client, changes by the Client to the onsite portion of the schedule within 2 weeks of the onsite work will incur a $2,000 re-scheduling fee. This fee does not apply to re-scheduling of work that does not require travel by SecureWorks.

Within three weeks of completing the portion of our engagement outlined in the statement of work section SecureWorks will issue a draft formal report to Client's designated point of contact. Client shall have three weeks from delivery of such draft to provide comments concerning the nature and scope of the engagement to be included in the report. If there are no comments received from Client in the three week period following delivery, the report shall be deemed final and SecureWorks will finalize for distribution.

The designated Client contact will receive an email confirmation from SecureWorks upon the completion of work performed under this Statement of Work. Unless otherwise notified in writing by such Client contact within thirty (30) days of such email confirmation, all of the work performed under this Statement of Work shall be deemed complete at the time of such email confirmation and if there is a remaining balance owed by Client, Client shall be invoiced and Client agrees to pay such invoice in accordance with the terms hereunder.

Assumptions

SecureWorks has made the following assumptions in creating this SOW:

- SecureWorks will contact Client's 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. The services will be scheduled to commence at least 2 weeks from such initial communication between SecureWorks and Client's designated representative.
- For the purpose of testing, each in-scope IP is considered to be a separate host, regardless of potential load balancing, firewalling, etc.
- Customer testing windows allow adequate time for performance of work.
- Required resources are scheduled and available. Specifically, suitable workspace for our staff and equipment, access to your computer systems and network for testing, building access, etc.
- Replies to all document requests and other information are timely and in accordance with the delivery dates established in the planning phase.
- Your management team supports your personnel's availability to participate in the project. This is crucial to timely and successful completion.
- The proposed fees are good for 90 days.

5.0 Term

The term of this SOW will be for one (1) year from the date of a purchase order certified by the City Auditor.

6.0 Disclaimers

Applicable to Onsite Services: Notwithstanding employees' placement at the Client location, SecureWorks retains the right to control the work of the employee. For international travel, Onsite Services may require additional documentation, such as Visas, visitor invitations, etc. which may affect timing and out of pocket costs.

Applicable to Security Services: Should a Statement of Work include security scanning, testing, assessment, forensics, or remediation Services ("Security Services"), Client 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. Client 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 Client from time to time) on network resources with the IP Addresses identified by Client. Client represents that, if Client 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 Security Services during a timeframe mutually agreed upon with Client. 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 Attacks. Furthermore, Client acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding the Client's systems and accepts those risks and consequences. Client hereby consents and authorizes SecureWorks to provide any or all the Security Services with respect to the Client's systems. Client further acknowledges it is the Client's responsibility to restore network computer systems to a secure configuration after SecureWorks' testing.

Applicable to Compliance Services: Should a Statement of Work include compliance testing or assessment or other similar compliance advisory Services ("Compliance Services"), Client understands

that, although SecureWorks' Compliance Services may discuss or relate to legal issues, SecureWorks does not provide legal advice or services, none of such Services shall be deemed, construed as or constitute legal advice and that Client 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 Client's legal or regulatory compliance.

Applicable to PCI Compliance Services: Should a Statement of Work include PCI compliance auditing, testing or assessment or other similar PCI compliance advisory Consulting Services ("PCI Compliance Services"), Client understands that SecureWorks' PCI Compliance Services do not constitute any guarantee or assurance that security of Client's systems, networks and assets cannot be breached or are not at risk. These Services are an assessment, as of a particular date, of whether Client's 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 Client's 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 Client's systems, networks and assets after the date of SecureWorks' final report, absent a signed Statement of Work expressly requiring the same.

This Statement of Work is agreed to by the parties. Any terms and conditions attached to a purchase order submitted by Client in connection with this Statement of Work are null and void:

SECUREWORKS, INC.	City of Columbus
By: _____	By: _____
Title: _____	Title: _____
Date: _____	Date: _____