SECUREWORKS STATEMENT OF WORK

STATEMENT OF WORK NUMBER 20150430-02

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"). This Statement of Work is subject to and governed by the SecureWorks Managed Services Agreement which was signed by SecureWorks on December 5, 2012 (the "MSA"), which is incorporated by this reference in its entirety.

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

Basic Penetration Test
The internal testing includes the following scope:

- Up to 128 internal IP addresses
- Testing will be performed from facilities listed in the Geographic Locations section above

Web Application Testing

The following web applications are within scope for testing:

- This is for two (2) Web Applications – specific URLs to be provided at initiation of contract.
- Applications have been scoped as "Advanced" with the following characteristics:
    - Has one or more of the following:
        - Login and user accounts
        - Search function
        - HTML forms
        - File upload/download
        - Forums
        - Process credit card payments or use a shopping cart
        - Content Management System admin section (CMS)
    - Does not have any of the following:
        - Heavy use of AJAX/JSON/Flash/Silverlight
        - Based on SharePoint or SAP
- Testing does not include subdomains
- Includes anonymous testing and up to two authenticated user accounts
- Application URLs will be provided before the engagement's commencement
- All testing will be performed from Dell SecureWorks technical testing facilities

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

Basic Penetration Test

The objective of a basic penetration test is to validate host configurations and produce a list of known vulnerabilities existing on in-scope systems. The testing includes exploitation of vulnerabilities to reduce false positives.

Pre-Engagement

A critical component of a Dell SecureWorks engagement is to clearly establish and agree to the rules of engagement. During our initial scheduling and kickoff sessions, the rules of engagement for the testing are established. Topics to be covered include:

- Goals and objectives for the testing
- Definition of scope, validation of targets
- Testing timelines and schedules
- Rules of engagement, levels of effort and risk acceptance
- Reporting requirements and deliverables, timelines and milestones
- Key personnel, roles and responsibilities, escalation rules and emergency planning
- Our source IP address ranges, tools and techniques

The consultant will send a confirmation email following project kick-off to ensure agreement on these items.

Execution

A technical network security assessment is designed to identify critical flaws in your network that an attacker could exploit. Testing may include any networked device, including firewalls, routers or other network infrastructure devices, intrusion detection and prevention systems, web servers, email systems, virtual private networking (VPN) systems, etc. We will use a combination of automated and manual scanning with commercial and publicly available tools, as well as custom scripts and applications that we have developed.

The types of vulnerabilities typically detected by this testing include:

- Microsoft Windows, Linux, and Unix operating system vulnerabilities and patches
- Known and published host application and service vulnerabilities, such as:
    - Apache, Microsoft IIS, IBM WebSphere and other web servers
    - SMTP (email) Servers
    - Remote access services, such as SSH, Telnet, RDP

    - Other server services (NTP, FTP, SSL wrappers, etc.)
- Network device vulnerabilities, such as firewalls, VPNs, routers
- Thousands of other vulnerabilities

Automated tools can greatly assist in reducing work effort and costs associated with repetitive and time-consuming tasks, but manual techniques and analysis are also performed in each step to have the greatest understanding of your environment. Manual validation of findings reduces false positives; manual vulnerability testing reduces false negatives. False positives on a report lead to wasted effort in remediation. False negatives can expose an organization to risk of intrusion.

Basic Penetration Test Step I: Scope Validation

We will validate the target list provided. This is a safety measure and will ensure the accuracy of subsequent findings. We may perform such activities as:

- Ping sweeps, port scans and route tracing
- Footprinting of networks and systems
- Internet domain name registration searches
- Internet registry number searches
- Domain name service (DNS) lookups

Basic Penetration Test Step II: Enumeration and Vulnerability Mapping

Enumeration involves actively trying to identify services running, applications used, version numbers, service banners, etc. Testing in this phase is at a more noticeable level of activity, which might reveal that we are performing types of reconnaissance activities that typically precede an attack.

In vulnerability mapping, the consultant will take what has been learned about the environment and attempt to determine vulnerabilities that are present. Some vulnerabilities will be apparent just using the information learned from the first two steps. However, many vulnerabilities can only be investigated with probe-and-response testing. In this type of test, the consultant sends data to a service or application and looks for a certain response that indicates a vulnerability may be present.

Automated scanning tools occasionally fail to report some vulnerabilities, so we conduct additional manual testing, which does not rely on automated scanning. A testing methodology that solely relies on automated scan results can give a false sense of security.

Basic Penetration Test Step III: Vulnerability Exploitation

Automated scanning tools often report false positives – reported vulnerabilities that are not actually present. For vulnerabilities discovered through automated scanning, we take steps to ensure report findings are accurate. This step ensures that the vulnerabilities reported are an accurate representation of your environment. Without this often overlooked step, time may be wasted attempting to remediate vulnerabilities that don't exist.

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. The goal is to further validate vulnerabilities by executing known exploits and observing the results. The consultant will devise and develop possible attacks and testing methods. We will give more emphasis to attacks that cannot or typically have not been carried out by automated means, as well as those that would expose you to the highest risk (reputation, direct loss, liability, compliance) if compromised by a malicious attacker.

As appropriate, testing will include various attacks, such as buffer overflows, format string attacks, arbitrary code execution and default credentials. We may also attempt customize attacks, which may

be unique to your systems or configurations. However, we will not perform Denial of Service (DOS) attacks, bruteforcing passwords, complex password guessing, or other high-impact/low-value testing without specific written approval.

A Note on Web Applications

Web applications are characteristically the most vulnerable applications, and Dell SecureWorks has services designed to thoroughly test and assess web application security. If we find web applications within the range of IP address within scope for this project, we will perform testing on the web application server, not on the application itself. This testing should not be considered a comprehensive or focused test of your web application.

Web Application Testing

Dell SecureWorks' methodology is based on industry best practice frameworks for penetration testing and application testing. Reference documents include OWASP Testing Guide, Open Source Security Testing Methodology Manual (OSSTMM), vendor-specific security documents and our own experience with risk and technical testing.

Project Planning and Rules of Engagement

A critical component of any testing such as this is to clearly establish and agree to the rules of engagement. During our initial scheduling and kickoff sessions, we will work with you to establish the rules of engagement for the testing. During this call, one of our consultants will walk you through these and ensure that you understand them. Topics to be covered include:

- Testing windows and special scheduling requests
- Goals and objectives, reporting requirements and deliverables, timelines and milestones
- Hosts, types of testing, thresholds and limits of testing within scope
- Key personnel, roles and responsibilities, escalation rules, emergency planning
- Our source IP address ranges, tools and techniques
- Any other necessary items

The consultant will send you a confirmation email to make sure we are all in agreement on these items.

Web Application Testing

Dell SecureWorks will actively put your application to the test. We will use automated and manual means to comprehensively assess the security of the application as it is presented to the Internet at the given site address.

We will start with automated tools. Scanning tools quickly enumerate and map the application, performing the most mundane and otherwise labor-intensive activities. These tools will detect known vulnerabilities and errors in web applications. After the scans have completed, Dell SecureWorks will analyze the results for false positives and for any patterns that emerge. Automated testing reveals potential vulnerabilities, such as:

- Known injection flaws
- Backup files
- Known platform and codebase vulnerabilities

- Error handling issues
- Known configuration issues

Next we will perform manual testing against the application. Dell SecureWorks' consultants are well trained and highly experienced in performing web application testing. In manually testing the applications, Dell SecureWorks uses a combination of commercial, open-source and custom tools, as well as reviewing code presented by the web application. This approach allows us to manipulate the application, as well as to infer secure coding practices used in the application development lifecycle. Manual testing is where the majority of the more significant vulnerabilities are found.

Once we have identified vulnerabilities in the application, we will then use manual techniques to actively test and exploit the vulnerabilities. This manual testing includes reviewing code snippets, manipulating variables (e.g., cookie tampering) and testing business logic. These techniques allow us to selectively review code for common mistakes. This scope of work does not include a detailed source code analysis, but if such analysis is needed, we can provide the service as a separate engagement.

We may request snippets of code from the backend application for further analysis. We do this in order to validate some potential vulnerabilities and to increase our efficiency. For example, it may take hours of testing to exhaustively map a particular vulnerability, whereas looking at the back-end code would take only minutes. Or some testing may result in findings that are not readily apparent from the outside but that attackers could use to their advantage. In these cases, it is to everyone's best interest to work together.

Our testing may include checks for at least the following categories of vulnerabilities, as appropriate, using a black box testing approach to your environment.

Current OWASP Top 10

1. Injection Flaws
2. Broken Authentication and Session Management
3. Cross-Site Scripting (XSS) Vulnerabilities
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

Previous OWASP Vulnerabilities

1. Malicious File Execution
2. Information Leakage and Improper Error Handling
3. Unvalidated Input
4. Buffer Overflow
5. Failure to Restrict URL Access
6. Insecure Cryptographic Storage
7. Insufficient Transport Layer Protection

Privileged Testing

All of our testing is first conducted with minimal to zero knowledge of your environment, processes or applications. To be comprehensive in testing, we must consider the capabilities that an authorized user on the systems may have. As such, we will use multiple user accounts - normally a representation of one anonymous and two authenticated user roles - to test what an authorized user may accomplish. This will be primarily a manual exercise and look to test, at a minimum, the following:

- Authorized user's ability to elevate privileges
- Authorized user's ability to view other user/account data
- Authorized user's ability to add/modify/delete other account data
- Authorized user's existing access is appropriate based upon role

A credentialed web application assessment allows you to evaluate several additional risks, beyond what an anonymous assessment will give you. The first set of risks is that an authorized user account may gain unauthorized access to (1) the application itself (e.g., application administrator); (2) other client data; and (3) the host server or platform (e.g., server administrator or root) – these risks are important because even trusted people can have their account credentials stolen. Second, you ensure user account tracking and validation is done properly (i.e., ensuring user cookies or tokens can't be easily hijacked). Lastly, you can identify issues where a legitimate user can fall victim to an attacker through various means (XSS, CSRF, SQL Injection, etc.).

Ranking Findings

Dell SecureWorks uses our own proprietary risk ranking methodology designed to be easy to understand. This methodology presents risks as Critical, High, Medium, Low and Informational priority based on many factors, including ease of exploitation, business criticality of the host and prevalence of the threat.

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.
- **Risk analysis matrix:** Details high-risk findings with recommendations for curative actions.
- **Remediation priority matrix:** Prioritizes high-risk finding remediation based on severity of risk to business process, not just technology.

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.

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: $47,840.00 US

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,

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: _____