**Technical Support Services Contract**
**City of Waukesha – Sikich LLP**

This Contract is by and between the City of Waukesha, a Wisconsin municipal corporation, referred to herein as the City; and Sikich LLP, 1415 West Diehl Road, Suite 400, Naperville, Illinois 60563, referred to herein as Sikich. Together, the City and Sikich are referred to as the Parties.

**Recitals**

The City published a Request for Proposals, referred to as the RFP, for technical services in connection with the performance of penetration testing of the City's computer network.

The RFP contained a specific scope of services to be incorporated into the successful bidder's contract.

Sikich submitted a proposal in response to the RFP, and was selected by the City to be awarded the contract to perform the services.

Sikich is willing to perform the consulting services according to the scope of services stated in the RFP and Sikich's responsive Proposal, and to accept the award of the contract for the services.

Now, therefore, the City and Sikich agree and contract as follows:

1. **Scope of Work.** Sikich shall perform the services described on Schedule A, Scope of Work; according to the standards of Schedule C, Rules of Engagement, and the terms and conditions of this Contract. The performance of these services is referred to herein as the Work. Schedules A and C are incorporated into this Contract by reference.

2. **Standard of Services.** Sikich will perform the Work according to generally-accepted industry practices and the standards of the professions of the individual employees performing the Services for Sikich. Sikich warrants and represents to the City that all personnel involved in the performance of the Work shall be fully trained and certified to perform all services according to that standard of care.

3. **Fees.** The City shall pay to Sikich the fees shown in Schedule B, which is incorporated into this Contract by reference. Sikich shall invoice the City, monthly. Invoices shall detail amounts in excess of the minimum monthly fees. All invoices shall be payable net 30 days.

4. **City Is Exempt from Sales Taxes.** The City is exempt from state excise, sales, and use taxes. Invoices to the City shall not add sales, excise, or use taxes. Sales tax exemption certificates will be provided to Sikich on request.

5. **Time.** Sikich shall perform the Work promptly upon execution of this Contract, and at the times mutually-agreed-upon by the City and Sikich.

6. **Standard of Work.** Sikich will perform the Work according to generally-accepted industry practices and the highest standards of the professions of the individual employees performing the Work for Sikich.

7. **Ownership of Work Product.** All materials produced in the performance of the Work shall be the sole property of the City, and shall be kept confidential and not disclosed to any third party without the prior written permission of the City.

8. **Changes.** This Contract, including the Scope of Work and fees, can only be amended by the written, mutual agreement of the Parties.

9. **Indemnification**. Sikich shall indemnify and hold the City harmless from any and all third-party claims, demands, causes of action, lawsuits, judgments, penalties, or other liabilities of any kind, including reasonable attorney fees and court costs, to the extent caused by Sikich's negligence or intentional misconduct.

10. **Insurance.** Sikich shall maintain insurance of the following kinds and for not less than the following limits, at Sikich's sole expense, at all times during the performance of the Work. Policies shall be occurrence, and not claims-made, policies, except for professional liability-errors and omissions. All policies shall be from insurers licensed to issue such policies in Wisconsin. Upon the execution of this Contract, Sikich shall deliver a certificate of insurance to City showing that all requirements of this section are met.

    **a.** Commercial general liability, including products-completed operations, $1,000,000 per occurrence, $2,000,000 aggregate per project.

    **b.** Automobile liability, $1,000,000 bodily injury, $1,000,000 property damage.

    **c.** Professional liability-errors and omissions, $1,000,000.

11. **Limitation of Liability.** Sikich shall not be liable for consequential and incidental damages arising from its performance of the Work. There shall be no other limitations of liability.

12. **Record Keeping.** Sikich shall keep all documents and records generated in the performance of the Work for no less than 7 years after completion of the Work, and shall make them available to the City at the City's request. Sikich acknowledges that such documents and records may be subject to Wisconsin's Open Records Law.

13. **No Smoking.** The City is a smoke-free environment. Sikich shall ensure its employees will not smoke or use tobacco products, and will not use electronic cigarettes, while on City property.

14. **No Illegal Drug Use.** The City is an illegal-drug-free environment. Sikich shall ensure its employees will not possess, use, or be under the influence of any illegal drug or controlled substance while on City property or while performing any Work.

15. **Cooperation by City.** The City shall cooperate with the Sikich in the performance of the Work, and shall respond timely to all reasonable requests for information and access.

16. **Parties Are Independent Contractors.** Nothing in this Contract shall be construed to create any relationship between the Parties other than independent contractors. Unless specifically provided in this Contract, the Parties are not agents for one another, have no authority to bind the other to contracts, and have no vicarious liability for the other's acts or omissions.

17. **Governmental Immunities and Notice Requirement Preserved.** Nothing in this Contract shall be construed to be a waiver or modification of the governmental immunities or notice requirements imposed by Wis. Stats. §893.80 or any other law.

18. **Assignment Prohibited.** This Contract, and the Sikich's responsibility to perform the Work under this Contract, may not be assigned by the Sikich without the City's written consent.

19. **Notices.** All notices required by this Contract, and all other communications between the Parties, shall be addressed as follows:

To the City: Attention: Chris Pofahl
City of Waukesha
201 Delafield Street

Waukesha WI 53188

To Sikich:

20. **Corporate Authorization.** The individuals executing this Contract on behalf of Sikich warrant and represent that they are duly authorized to bind Sikich to this Contract. Sikich warrants and represents that the execution of this Contract is not prohibited by Sikich's articles of incorporation, by-laws, operating agreement, or other internal operating orders, or by any applicable law, regulation or court order. Sikich shall provide proof upon request.

21. **Assistance of Counsel, Voluntary Contract.** Sikich acknowledges that it has either had the assistance of legal counsel in the negotiation, review and execution of this Contract, or has voluntarily waived the opportunity to do so; that it has read and understood each of this Contract's terms, conditions and provisions, and their effects; and that it has executed this Contract freely and not under conditions of duress.

22. **Adequacy of Consideration.** The Parties acknowledge that the consideration expressed in this Contract is adequate and sufficient to make the obligations contained in this Contract binding upon the Parties.

23. **Costs of Enforcement.** The Parties agree that in the event legal action is necessary to enforce any term or condition of this Contract, then the breaching Party will pay the non-breaching Party's costs incurred in such legal action, including actual attorney fees. If a judgment is taken, then costs of enforcement will be added to the judgment.

24. **Severability.** If any term of this Contract is held unenforceable by a court having jurisdiction, then to the extent the unenforceable term can be severed from the remainder of this Contract without affecting the enforceability of the remainder of this Contract or substantially frustrating its purpose, it will be so severed, and the remainder of this Contract will remain in effect and enforceable.

25. **Survival and Parties Bound.** Unless specifically limited in this Contract, any term, condition or provision of this Contract will survive the execution of this Contract or any stated time periods, to the extent necessary for their performance. This Contract is binding upon, and inures to the benefit of, the Parties' successors, assigns, heirs, executors, trustees and personal representatives.

26. **Governing Law and Jurisdiction.** This Contract will be construed and enforced according to the laws of Wisconsin. If a lawsuit arises out of this Contract, it shall be filed in the state Circuit Court for Waukesha County, Wisconsin. The Parties consent to personal and subject-matter jurisdiction in Wisconsin, and waive all jurisdictional defenses.

27. **Integration.** This Contract constitutes the entire agreement of the Parties formed by the City's RFP and Sikich's responsive proposal.

**City of Waukesha**

| | |
|---|---|
| By Shawn N. Reilly, Mayor | Attested by Gina L. Kozlik, City Clerk |
| Date:_____ | Date:_____ |

To certify that funds are provided for payment:

Richard L. Abbott, Director of Finance
Date:

**Sikich LLP**

By (print name)
Title:
Date:

By (print name)
Title:
Date:

Authorized by Common Council on April 16, 2019.

# Schedule A - Scope of Work

# Service Descriptions

To accomplish the goals of City of Waukesha, Sikich will perform the following services, according to the Rules of Engagement, Schedule C (as completed by the City).

## External Network Penetration Testing

The Sikich external penetration test provides a “hacker’s eye” view of your Internet-connected systems. In this test, a trained, experienced security consultant attempts to gain access to your systems using the tools and techniques employed by professional computer criminals and other attackers.

External penetration tests are a critical part of an organization’s overall information security program. External penetration tests from Sikich are designed to be compliant with PCI DSS requirements and provide valuable information to City of Waukesha and their IT department.

### REQUIREMENTS

Requirement 11.3 of the PCI DSS states that external penetration testing is required at least once a year as part of your regular audit process. This requirement applies to all entities, regardless of level, that store, process or transmit cardholder data.

From PCI DSS Requirement 11.3.1:

*“Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).”*

### OUR SERVICE

Sikich penetration testing is conducted using a proven methodology to systematically analyze the City of Waukesha Internet environment. The testing can be performed as a zero-knowledge assessment, taking the perspective of an outside attacker without knowledge of the network, or completed using additional information agreed upon by City of Waukesha and Sikich (such as a device listing or user accounts) to focus the assessment.

Sikich follows a methodology based on National Institute of Standards and Technology (NIST) Special Publication 800-115, with which the Penetration Testing Execution Standard (PTES) aligns, and that encompasses the following phases:

### Planning (Pre-Engagement Interactions)

- Kickoff call with scope review
- Rules of Engagement creation

### Reconnaissance (Intelligence Gathering)

- Network surveying and mapping
- Device discovery and enumeration
- Service detection and port scanning
- Operating system identification

### Vulnerability Detection (Threat Modeling and Vulnerability Analysis)

- Security holes and vulnerability identification
- User account and password review
- Operating system security testing
- Service security testing
- Application security testing

### Attack and Penetration (Exploitation and Post-Exploitation)

- Vulnerability exploitation
- Results and risk analysis

### Reporting

- Vulnerability and exploitation attempt enumeration
- Remediation action recommendation creation

Sikich will communicate with City of Waukesha throughout the planning and execution of the penetration test. We will immediately halt testing and contact City of Waukesha if we discover significant vulnerabilities, observe that our testing is having an adverse impact on the systems or discover indications of a previous successful attack.

## OUR REPORTS

Part of the value of a penetration test depends on the ability of City of Waukesha to understand and take action on the results. Our reports are written to meet the needs of your IT department, internal and external auditors and examiners. Our reports clearly define the scope of the testing, the methodology used and the results of the testing, and make recommendations to address any findings.

# Internal Network Penetration Testing

Internal attacks are consistently ranked as the number-one source of compromise because internal network security is often a penetrable line of defense. Sikich internal penetration testing analyzes your internal network to assess the security from an attacker with physical access (such as a malicious or disgruntled customer, employee, contractor, maintenance staff, etc.), an attacker who has breached the external perimeter, or a virus or worm that has unknowingly been released on the network.

## OUR SERVICE

An internal penetration test follows the same general methodology as an external penetration test. These actions are taken against internal servers, workstations and networking devices. This testing includes the following phases:

### Planning (Pre-Engagement Interactions)

- Kickoff call with scope review
- Rules of Engagement creation

### Reconnaissance (Intelligence Gathering)

- Network surveying and mapping
- Device discovery and enumeration
- Service detection and port scanning
- Operating system identification

### Vulnerability Detection (Threat Modeling and Vulnerability Analysis)

- Security holes and vulnerability identification
- User account and password review
- Operating system security testing
- Service security testing

### Attack and Penetration (Exploitation and Post-Exploitation)

- Vulnerability exploitation
- Results and risk analysis

### Reporting

- Vulnerability and exploitation attempt enumeration
- Remediation action recommendation creation

Sikich will perform the internal penetration test overtly. Overt testing is done with the knowledge and cooperation of the IT, network and information security staffs, which will focus our testing time

on the most valuable targets and enable us to quickly answer any questions we may have about the network and systems. This equates to the grey box testing requested.

## Wireless Review and Testing

Wireless access is critical in supporting mobile users and business applications in an effort to maintain efficiency and agility. Wireless technology advances have improved security, flexibility and reliability to the point that enterprises have begun deploying wireless more pervasively throughout their organizations, supporting more users, devices and applications than ever before.

Wireless networks also introduce multiple avenues for attack and penetration that are either much more difficult or completely impossible to execute with a standard, wired network. Wireless networks only know the boundaries of their own signal: streets, parks, nearby buildings and cars all offer a virtual “port” into your wireless network.

### WIRELESS ENCRYPTION REVIEW

Wireless networks, while convenient, can also pose large risks to an organization, especially if they are not secured properly.

Sikich will assess the security of wireless networks through the following methods:

- Attempting to brute force encryption keys
- Attempting to bypass MAC address filtering
- Sniffing for sensitive traffic

### WIRELESS CONFIGURATION REVIEW

While wireless networks are often secured to some degree, the level of security can typically be improved upon. Sikich will conduct a wireless configuration review to examine the security in place on these networks and report on how to improve potentially weak areas.

Sikich will:

- Review wireless configuration files
- Review wireless encryption and key management
- Review wireless network architecture and segmentation
- Attempt to break out of defined segmentation and access other areas of the network

# Scope and Assumptions

In determining the level of effort and resources applied to these services, it is critical to understand the composition of the networking environment and application that will be tested. The fees set forth in this Statement of Work (SOW) are based on the following assumptions. In the event that any assumptions prove to be inaccurate and Sikich incurs additional work as a result thereof, additional fees may apply.

Sikich understands the following regarding the City of Waukesha environment:

- One (1) location in Waukesha, WI
- Testing is to comply with the PCI DSS
- Owns six (6) VLANs
- Sikich will test up to 60 servers
- Sikich will test up to 250 workstations
- One (1) location included for wireless testing
    - 10 wireless access points
    - Four (4) SSIDs on the access points
- There are 30 active externally-facing IP addresses

City of Waukesha has stated that testing may take place during normal business hours and will be conducted on site.

# Schedule and Milestones

All reasonable attempts will be made to meet the dates requested. City of Waukesha understands and agrees that changes in major factors (such as a “Project Change Control”) could impact the projected timeframe.

| Service | Location | Start Date | Completion Date |
|---|---|---|---|
| External Network Penetration Testing | Remote and on-site | To be determined | Estimated 6 weeks from start date |
| Internal Network Penetration Testing | On-site | To be determined | Estimated 6 weeks from start date |
| Wireless Review and Testing | On-site | To be determined | Estimated 6 weeks from start date |

Upon the start of each service, Sikich will coordinate with City of Waukesha to set up a complete project schedule.

# Fees and Payment Schedule

In estimation to complete the activities based on the included scope, Sikich will perform the following services annually as part of a five-year engagement.

## External Network Penetration Testing

Sikich will conduct in-depth penetration testing to emulate actual attack vectors taken by professional hackers against the external environment to meet PCI DSS Requirement 11.3.

| Service Phase | Fee |
|---|---|
| Project Setup, Kickoff and Discovery<br><br>*Includes:*<br>• *Creation of the project in the Sikich project management portal*<br>• *Project kickoff conference call*<br>• *Network surveying and mapping*<br>• *Device discovery and enumeration*<br>• *Service detection and port scanning* | Included |
| Testing and Reporting<br><br>*Includes:*<br>• *Manual and automated testing of network and operating system vulnerabilities*<br>• *Up to two (2) hours of retesting on identified vulnerabilities to be completed within 30 days of receipt of the draft report*<br><br>*Deliverables:*<br>• *Draft combined penetration test report of scope and methodology, findings and recommendations for remediation and compliance with the PCI DSS*<br>• *Final combined penetration test report* | Included |
| Total | $6,600 |

# Internal Network Penetration Testing

Sikich will conduct in-depth penetration testing to emulate actual attack vectors taken by professional hackers against the internal environment.

| Service Phase | Fees |
|---|---|
| **Project Setup, Kickoff and Discovery**<br><br>*Includes:*<br>• *Creation of the project in the Sikich project management portal*<br>• *Project kickoff conference call*<br>• *Building and shipping internal penetration testing device*<br>• *Up to two (2) hours of configuration and setup of device on client network in preparation of testing*<br>• *Network surveying and mapping*<br>• *Device discovery and enumeration*<br>• *Service detection and port scanning* | Included |
| **Testing and Reporting**<br><br>*Includes:*<br>• *Testing of internal network*<br>• *Automated information gathering and scanning*<br>• *Manual testing of internal network mimicking actual attack vectors*<br>• *Up to two (2) hours of retesting on identified vulnerabilities to be completed within 30 days of receipt of the draft report*<br><br>*Deliverables:*<br>• *Draft combined penetration test report of scope and methodology, findings and recommendations for remediation*<br>• *Final combined penetration test report* | Included |
| **Total** | **$7,800** |

# Wireless Review and Testing

Sikich will conduct in-depth testing to emulate actual attack vectors taken by professional hackers against the wireless networks.

| Service Phase | Fees |
|---|---|
| **Project Setup, Kickoff and Discovery**<br><br>*Includes:*<br>• *Creation of the project in the Sikich project management portal*<br>• *Project kickoff conference call* | Included |

| Service Phase | Fees |
|---|---|
| **Wireless Review and Testing**<br><br>*Includes*:<br>• *Remote wireless testing of Waukesha access points*<br>• *Remote wireless access point identification (including rogue networks)*<br>• *Remote testing of wireless encryption*<br>• *Remote review of wireless network configurations*<br><br>*Deliverables*:<br>• *Findings from the wireless review and testing will be included in the penetration test report along with wireless access points and associated configurations* | Included |
| Total | $2,000 |

## Additional Testing and Consulting Time (As Needed)

Sikich has provided services within this SOW that are limited to a fixed amount of time. These hours have been chosen as a median of how much time clients similar in size and makeup to your organization have traditionally needed. Should City of Waukesha require additional time in any of these areas (such as retesting for penetration testing), Sikich will bill this time at an hourly rate, which allows City of Waukesha to only pay for exactly how much additional time is needed.

| Service | Fees |
|---|---|
| Information Security Testing and Consulting | $282/hour |

## Payment Schedule

A benefit of the multi-year testing program is the ability to pay a quarterly flat rate throughout the length of the contract with Sikich. This flat rate allows City of Waukesha to easily budget for their information security and compliance fees over multiple years.

Sikich will invoice the initial quarterly installment of **$4,100** upon receipt of the signed SOW. After the initial invoice, Sikich will invoice subsequent installment amounts at the start of each quarter for the duration of the contract.

### EXPENSES

Travel time is included in the fee structure outlined in this SOW. Applicable project expenses (flights, mileage, hotel, meals, shipping, equipment, etc.) will be billed to City of Waukesha at actual cost as they are incurred.

Schedule C - Rules of Engagement

PLANNING DOCUMENT

# Rules of Engagement

Sikich will be conducting penetration testing based on the information contained within this planning document. City of Waukesha should list all target systems and review all planning details prior to the commencement of the project.

SIKICH®

*Created April 11, 2019*

# Contents

**Introduction** ..... **4**
Methodology Phases ..... 4
Phase I: Planning ..... 4
Phase II: Reconnaissance ..... 5
Phase III: Vulnerability Detection ..... 5
Phase IV: Exploitation ..... 7
Phase V: Reporting ..... 7
**External Network Testing** ..... **9**
External Targets ..... 9
Source IP Addresses ..... 9
**Internal Network Testing** ..... **10**
Internal Targets ..... 10
Realistic Internal Targeting ..... 10
Internal Testing Facilitation ..... 11
**Wireless Testing** ..... **13**
Wireless Targets ..... 13
**Additional Details** ..... **14**
Projected Timeframe ..... 14
Testing Restrictions ..... 14
Deliverables ..... 15
Testing for Compliance ..... 15
Network Segmentation Testing for Compliance ..... 15
IT Staff Awareness ..... 16
Network Diagram ..... 16
Secure Document Exchange ..... 16
Sampling ..... 16
Exclusions ..... 17
**Contact Information** ..... **18**
City of Waukesha Contacts ..... 18
Primary City of Waukesha Contact ..... 18
Secondary City of Waukesha Contact ..... 18
Sikich Contacts ..... 19

Sikich Lead Penetration Tester.....19

Sikich Technical Manager.....19

Sikich Project Manager .....19

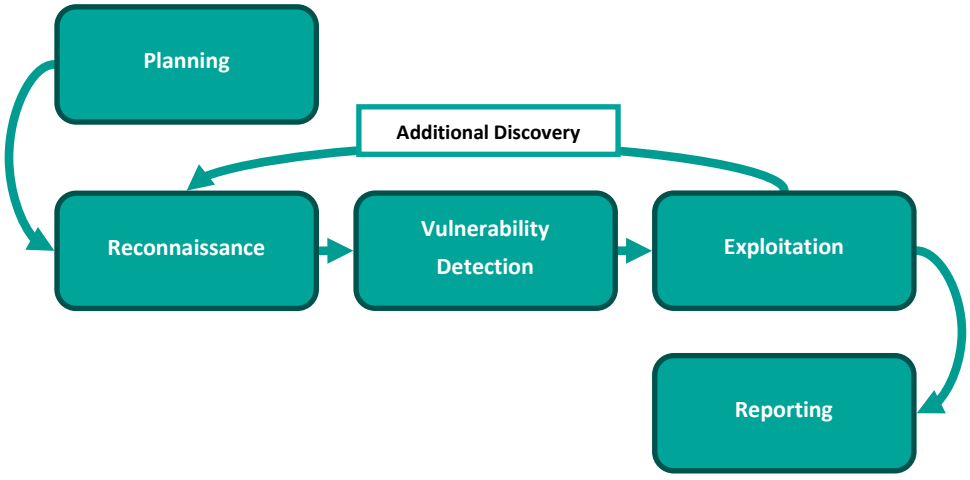
# Introduction

City of Waukesha (City of Waukesha) has engaged Sikich LLP (Sikich) to conduct a series of penetration tests:

- The **external penetration test** simulates an attack against the City of Waukesha systems accessible from the Internet. This type of attack might be carried out by a disgruntled customer, an ex-employee from a remote location or organized criminals located overseas.
- The **internal penetration test** simulates an attack against the City of Waukesha systems from within the City of Waukesha internal network. This type of attack might include a rogue employee with limited access to the City of Waukesha network who is trying to escalate his/her privileges to access sensitive data or a vendor/contractor who comes on site and plugs a laptop into a corporate network jack.
- The **wireless penetration test** simulates an attack against the City of Waukesha wireless networks. This type of attack might be performed by a malicious user using a guest wireless network who is trying to access unauthorized systems or information.

## Methodology Phases

When performing this penetration test, Sikich follows a methodology based on National Institute of Standards and Technology (NIST) Special Publication 800-115 that encompasses the following phases:




### PHASE I: PLANNING

In the planning phase, Sikich creates a Rules of Engagement document that defines targets, documents management approval and sets testing goals.

## PHASE II: RECONNAISSANCE

In the reconnaissance phase, Sikich attempts to identify and obtain information about the targets within scope. This includes pertinent information about the organization such as names and contact information of IT staff, information employees may have posted to Internet forums or other items Sikich might uncover through focused Internet searches.

Sikich scans targets on commonly used TCP and UDP ports and attempts to identify active services (e.g., web server, mail server) running. Devices or services that are powered off, offline or inaccessible during scanning will not yield results. Unexpected downtime of the target environment may impact the amount of reconnaissance completed on individual devices or services.

Sikich also attempts to obtain further information about potential web applications by searching for pertinent data, including unlinked content, hidden directories and version numbers of application components.

## PHASE III: VULNERABILITY DETECTION

During the vulnerability detection phase, Sikich attempts to discover and validate vulnerabilities on the systems enumerated in the reconnaissance phase, including by performing vulnerability scans. Sikich does not attempt to verify each of the vulnerabilities identified during scanning but provides the results of these automated tests to City of Waukesha.

Sikich utilizes updated vulnerability detection methods and tools based on the most recent threats and techniques identified. Through testing of the targeted systems and services, Sikich focuses on discovering vulnerabilities in five (5) domains:

- **Application Security** – Strengths and weaknesses of application code, configuration, patch levels and protection of data that resides in the application
- **Access Control** – Strengths and weaknesses of controls over files, directories, web content and other data
- **Network Security** – Strengths and weaknesses of networking devices and security of network traffic
- **Operating System Security** – Strengths and weaknesses of operating systems' security (e.g., Windows, UNIX)
- **User Management** – Security of user accounts, passwords and other unique identifiers

For web application testing targets that are specified, Sikich focuses on discovering the Top 10 Web Application Security Vulnerabilities identified by the Open Web Application Security Project (OWASP). Sikich may also perform cursory reviews for these vulnerabilities on any undefined web applications discovered during testing. At this time, the OWASP Top 10 Web Application Security Vulnerabilities are:

- **Injection Flaws** – Injection flaws, such as SQL, NoSQL, OS and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The

attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

- **Broken Authentication** – Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
- **Sensitive Data Exposure** – Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
- **XML External Entities (XXE)** – Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution and denial of service attacks.
- **Broken Access Control** – Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
- **Security Misconfiguration** – Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
- **Cross-Site Scripting (XSS)** – XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites or redirect the user to malicious sites.
- **Insecure Deserialization** – Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks and privilege escalation attacks.
- **Using Components with Known Vulnerabilities** – Components, such as libraries, frameworks and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
- **Insufficient Logging & Monitoring** – Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems and tamper, extract or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

### PHASE IV: EXPLOITATION

In the exploitation phase, Sikich takes the vulnerability information and uses it to obtain access to otherwise restricted data, take control of systems, impersonate users and perform other actions designed to demonstrate the potential consequences of the vulnerabilities discovered.

Unless otherwise specified in this document, Sikich may engage in, but will not be limited to, any or all of the following attack vectors:

- Brute-force attacks
- Client-side (i.e., user) attacks
- Custom payload execution
- Injection attacks
- Man-in-the-middle (MITM) attacks
- NetBIOS name spoofing
- Persistent access software installs

As part of the exploitation phase, Sikich may discover access to systems and services that were not specifically defined targets and attempt to further its attacks by accessing and reviewing those resources. These resources may include, but would not be limited to:

- Social media services
- Cloud and third-party hosting services
- Corporate email
- Directory services

Throughout this phase, Sikich attempts to bypass security controls designed to segment sensitive data or systems. Sikich will also attempt to chain exploits in sequence to further penetrate your organization's systems, escalate access privileges to systems and identify additional vulnerabilities.

As this engagement has clear goals and is limited by time, Sikich will prioritize attack paths that are likely to lead to system-level access or sensitive information. Sikich will not attempt to identify or validate every vulnerability that could potentially exist in the tested environment.

### PHASE V: REPORTING

In the reporting phase, Sikich documents discovered vulnerabilities and attempts at exploitation as well as recommend remediation actions. Sikich also records the results of City of Waukesha efforts made toward remediating identified vulnerabilities.

As part of its testing methodology, Sikich performs additional discovery, repeating reconnaissance, vulnerability detection and exploitation phases as needed, as it uncovers more information or successfully leverages exploits to gain access to additional systems or networks.

It's important to remember that a penetration test is a point-in-time measurement. It is limited in time and resources, whereas a real attacker may not be. New security vulnerabilities are discovered every day. Additionally, Sikich prioritizes attack paths that may lead to system-level access or sensitive information and, therefore, may not interact with every system or service. As a result, it is nearly impossible to identify all vulnerabilities within an environment or application.

Penetration testing simulates a malicious entity attacking City of Waukesha, which has an inherent risk. Sikich makes efforts to avoid the disruption of normal business operations during testing. As an extra precaution, City of Waukesha should verify the target systems have proper operational security in place, such as regular backups and log file rotation.

# External Network Testing

Based on the defined scope, Sikich will simulate a scenario in which an external attacker without knowledge of the environment attempts to compromise systems, infiltrate the internal network and access sensitive data.

## External Targets

Please list all external IP addresses and hostnames that will be targeted for testing.

| IP Address | Hostnames | Description |
|---|---|---|
| 205.213.2.3 | vpn.waukesha-wi.gov | |
| 205.213.2.10 | permits.waukesha-wi.gov | |
| 205.213.2.25 | fireapps.waukesha-wi.gov | |
| 205.213.2.30 | rds-apps.waukesha-wi.gov | |
| 205.213.2.33 | ftp.waukesha-wi.gov | |
| 205.213.2.49 | waukesha-wi.gov | |
| 2058.90.189.153 | waukesha-wi.gov | |
| (Example) 100.9.9.9 | example.com, www.example.com | Web server |

## Source IP Addresses

Sikich will perform external testing from the following source IP addresses.

- 12.155.240.66-78
- 52.179.195.186
- 147.75.74.177-190
- 147.75.89.1-14
- 209.170.231.0/28

For efficient testing, we recommend that you prevent our source IP addresses from being blacklisted in any intrusion prevention system (IPS), web application firewall (WAF) or any other security system. While these security systems should still be configured to block individual attacks, they should not shun all future traffic from our IP addresses.

# Internal Network Testing

Based on the defined scope, Sikich will simulate a scenario in which an outside attacker has plugged a malicious device into the internal corporate network and attempts to compromise systems, escalate privileges and access sensitive data.

## Internal Targets

Please supply all internal networks that will be targeted for testing. City of Waukesha should indicate areas of high risk (e.g., the cardholder data environment for testing related to complying with the Payment Card Industry Data Security Standard (PCI DSS)) so that Sikich can specifically target these systems.

| Network | Description | High Risk |
|---|---|---|
| (Example) 10.0.0.0/24 | Application servers | X |
| | | |

### REALISTIC INTERNAL TARGETING

We understand that it can be difficult to list every network, system and supporting service that you'd like us to target as we simulate an attacker who would not have targeting limitations. To simulate a realistic attack, you may authorize us to target any resources that we discover that may not be specified above.

| | |
|---|---|
| **City of Waukesha authorizes realistic targeting** | |
| **City of Waukesha does not authorize realistic targeting** | |

If City of Waukesha authorizes Sikich to target networks that are not explicitly defined, Sikich will make commercially reasonable efforts to inform City of Waukesha and verify City of Waukesha's ownership of any discovered resources before further attacks.

City of Waukesha asserts that they have specified in either the Testing Restrictions or Exclusions section of this document any internal systems or networks that they do not own or do not wish to be targeted, including those that may be accessible over a VPN.

## INTERNAL TESTING FACILITATION

Sikich may utilize one or more of the methods listed below to facilitate internal testing. Some of these methods may require additional configuration information.

| Method | Description | Additional Configurations |
|---|---|---|
| ☐ **Laptop** | Sikich will ship a laptop that City of Waukesha will connect to the internal network. Sikich will perform testing remotely through the device.<br><br>Please indicate where Sikich should ship the laptop.<br><br>John Doe<br>221B Baker Street<br>Suite 403<br>Chicago, IL 60601<br><br>Once the test is complete, please ship the system back to the address below within seven calendar days.<br><br>Sikich LLP<br>13400 Bishops Lane<br>Suite 300<br>Brookfield, WI 53005 | For laptops and virtual machines, Sikich requires a network interface that can create an outbound connection to the Sikich IP address **209.170.231.11** on port **1194/tcp**. You may need to open firewall rules to allow this connection.<br><br>**IP Address:** 10.1.1.50 or DHCP<br>**Netmask:** 255.255.255.0<br>**Gateway:** 10.1.1.1<br><br>Additional network interfaces can be configured under the Starting Points section. |
| ☐ **Virtual Machine** | Sikich will create a VMware virtual machine that City of Waukesha will download and connect to the internal network. Sikich will perform testing remotely through the VM.<br><br>Recommended RAM: 4 GB<br>Recommended disk space: 50 GB<br>File format: OVF (importable into VMware and HyperV hypervisors) | |
| ☐ **VPN** | City of Waukesha will provide Sikich with VPN access to the internal network. Sikich will perform testing remotely over the VPN.<br><br>Note: Testing exclusively over a VPN limits the number of attacks that can be performed and is not recommended. | N/A |
| ☐ **On Site** | Sikich will conduct internal testing on site. City of Waukesha may be responsible for any applicable travel fees. | N/A |

## Starting Points

Sikich will attempt to elevate privileges, gain unauthorized access and locate sensitive data from each starting point. Segmentation security controls can be tested by specifying starting points on both sides of the segmentation perimeter.

For each starting point, please provide network information that you wish to assign to the Sikich testing device interface.

| Description | IP Address (or DHCP) | Netmask | Gateway |
|---|---|---|---|
| (Example) Workstation network | DHCP | --- | --- |
| (Example) Server network | 10.4.4.4 | 255.255.255.0 | 10.4.4.1 |

# Wireless Testing

Based on the defined scope, Sikich will simulate a scenario in which an attacker without access to wireless networks attempts to compromise systems, infiltrate the internal network and access sensitive data.

## Wireless Targets

Please list all wireless networks and SSIDs that will be targeted for testing.

| Subnet | SSID | Description | Type |
|---|---|---|---|
| (Example) 10.X.X.X/26 | ACME | Internal wireless | 802.11n (2.4 Ghz) |
| | | | |
| | | | |

# Additional Details

During the course of the project, the penetration testing team may conduct different automated and manual testing throughout different times and days of the scheduled timeframe. The type of testing and when it is performed are primarily determined based on risks identified during the course of the testing and will vary for each test.

Additional details regarding the engagement, including those related to compliance goals, target exclusions and sampling, are included below.

## Projected Timeframe

Based upon communication with City of Waukesha, Sikich has compiled the following tentative schedule to serve as a guideline for the engagement.

| Stage | Anticipated Date |
|---|---|
| Start of testing | April 29, 2019 |
| Completion of testing | May 24, 2019 |
| Delivery of draft report | June 7, 2019 |
| Completion of retesting | July 3, 2019 |
| Delivery of final report | July 19, 2019 |

## Testing Restrictions

City of Waukesha can indicate any testing date or time restrictions for specific systems and services below. City of Waukesha can also indicate if any extra precautions should be taken for specific systems to avoid disrupting normal business operations. While Sikich will make its best effort to accommodate these requests to avoid any unexpected disruptions, City of Waukesha acknowledges that there are inherent risks with any penetration testing.

| System/Service | Restriction |
|---|---|
| (Example) 10.9.9.9 | No testing during daily database backups (10:00 p.m.-4:00 a.m. Central Time) |
| (Example) XYZ Web Application | Do not perform automated testing on the “Contact Us” page because every submission generates an email. |

Please note that all times are in Central US time if not specified. Requiring after-hours testing may incur additional cost.

Penetration testing simulates a malicious entity attacking City of Waukesha, which has an inherent risk. Sikich makes efforts to avoid the disruption of normal business operations during testing. As an extra precaution, City of Waukesha should verify the target systems have proper operational security in place, such as regular backups and log file rotation.

## Deliverables

Sikich will deliver a draft penetration test report that outlines identified vulnerabilities and attack paths, and provides additional details. Sikich will also post each vulnerability as a to-do item within the Basecamp project management system.

Sikich will conduct up to four (4) hours of retesting (two (2) hours each for external network/application and internal network targets) on remediated vulnerabilities within 30 days of delivering the draft report. Subsequent retesting can be completed at a time-and-materials consulting rate.

Following retesting, Sikich will generate a final penetration test report containing remediation notes and management responses.

## Testing for Compliance

This testing is being performed in support of compliance with the PCI DSS. City of Waukesha asserts that the testing scope contains all systems in the cardholder data environment (CDE) and any system components that, if compromised, could impact the security of the CDE.

### NETWORK SEGMENTATION TESTING FOR COMPLIANCE

PCI DSS Requirement 11.3.4 requires penetration testing to validate that segmentation controls and methods are operational, effective and isolate all out-of-scope systems from systems in the CDE.

In addition, the PCI DSS states:

*"To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE."*

Please advise us by indicating whether City of Waukesha is using segmentation to reduce the scope of their compliance requirements.

| | |
|---|---|
| **Segmentation to reduce PCI DSS scope** | |
| **No segmentation** | |

If segmentation is being used to reduce PCI DSS compliance scope, City of Waukesha should provide Sikich with at least one internal testing starting point outside of the PCI environment from which to perform testing. Sikich will attempt to bypass segmentation controls to gain entry to secured areas.

Please provide a brief description of any segmentation and any additional testing that should be performed.

| Segmentation Method | Segmentation Testing |
|---|---|
| (Example) A user workstation network is segmented from the PCI server network that processes cardholder data. | Sikich will use a starting point within this network and attempt to bypass segmentation controls. |
| (Example) City of Waukesha maintains a corporate network outside of the Amazon Web Services (AWS) instance that hosts their PCI networks. City of Waukesha stated that no resources have privileged access to the AWS instance and that employees use a two-factor client-to-site VPN to gain access into the PCI networks as needed. | Sikich will attempt to bypass and gain access to the two-factor VPN from the Internet. |

## IT Staff Awareness

Please advise us by indicating which type of testing you would like Sikich to use when conducting our testing.

| | |
|---|---|
| **Covert (IT staff is not aware)** | |
| **Overt (IT staff is made aware)** | |

## Network Diagram

Please provide a network diagram so that we can verify that we've included all of your systems in scope.

## Secure Document Exchange

Sikich and City of Waukesha will determine a secure method for exchanging sensitive documents during this engagement. This can be done by agreeing on passwords or providing PGP keys that can be used to encrypt sensitive documents.

## Sampling

Sikich will review test instance of the Security Information and Event Management (SIEM), which City of Waukesha reported as being representative samples of the production applications. Because Sikich will not review NIDS rules of the SIEM.

# Exclusions

Unless otherwise specified, Sikich will exclude any targets that are not defined in this document.

# Contact Information

During the course of the testing, Sikich may discover certain conditions that would prompt the testing team to contact City of Waukesha prior to the conclusion of the testing. Sometimes the testing team will need to further explore a condition based on the current environment in order to fully understand its impact and potential risk before discussing with City of Waukesha.

The Sikich testing team will use its best discretion on when to contact City of Waukesha based on conditions that may include:

- A security hole that presents significant risk to City of Waukesha systems or data
- Evidence or indication of a previous compromise or intrusion attempt
- Knowledge or indication of possible adverse impact to a target

## City of Waukesha Contacts

Please identify two contacts for coordinating the testing and results:

### PRIMARY CITY OF WAUKESHA CONTACT

| | |
|---|---|
| **Name** | |
| **Email** | |
| **Work Phone** | |
| **After-Hours Phone** | |

### SECONDARY CITY OF WAUKESHA CONTACT

| | |
|---|---|
| **Name** | |
| **Email** | |
| **Work Phone** | |
| **After-Hours Phone** | |

# Sikich Contacts

Likewise, City of Waukesha may wish to contact the Sikich testing team during the course of the testing process. Please use the following information as the primary contacts in the event you need to contact the testing team.

## SIKICH LEAD PENETRATION TESTER

| | |
|---|---|
| **Name** | Will Bonk |
| **Email** | **will.bonk@sikich.com** |
| **Work Phone** | 262.317.8597 |
| **After-Hours Phone** | 715.630.5077 |

## SIKICH TECHNICAL MANAGER

| | |
|---|---|
| **Name** | Samuel Gibson |
| **Email** | **samuel.gibson@sikich.com** |
| **Work Phone** | 262.317.8587 |
| **After-Hours Phone** | 715.271.2631 |

## SIKICH PROJECT MANAGER

| | |
|---|---|
| **Name** | Shannon Mikulak |
| **Email** | **shannon.mikulak@sikich.com** |
| **Work Phone** | 877.403.5227 x207 |
| **After-Hours Phone** | N/A |

Sikich LLP
877.403.5227
**support@sikichlabs.com**
**http://www.sikichlabs.com**