PRESIDIO
Future. Built.

NG RM

Williamson County
Baseline Security Assessment

SOW# 1003116609657Pro-1

PROPOSAL TEAM

Name	Company	Role	E-mail
Brett Marlier	Presidio	Account Manager	bmarlier@presidio.com
Tim Nicolaou	Presidio	Solution Architect	tnicolaou@presidio.com
Richard Semple	Williamson County	Director IT	rsemple@wilco.org

CHANGE REVISION RECORD

Revision	Date	Author	Notes
v1.0	5/29/2019	Tim Nicolaou	First Client Release
V1.1	6/28/2019	Tim Nicolaou	Replaced references to Presidio travel policy with Williamson County's. Added Williamson County's travel policy as appendix C. See related revisions in sections 1.2.9, and 4.3.

TABLE OF CONTENTS

1 Executive Summary 4
1.1 Background 4
1.2 Scope of Services 4
2 Methodology and Approach 7
2.1 Engagement Management and Control 7
2.2 External Vulnerability Assessment 7
2.3 Internal Vulnerability Assessment 8
2.4 Wireless Infrastructure Assessment 9
2.5 Web Applications Assessment 10
2.6 External Penetration Testing 11
2.7 Internal Penetration Testing 13
2.8 Remediation Assessment 14
3 Deliverables 16
4 Assumptions 17
4.1 General 17
4.2 General Client Responsibilities 17
4.3 Travel 18
4.4 Internal Vulnerability Assessment 19
5 Terms and Conditions 20
5.1 General 20
5.2 Payment Schedule 20
5.3 Authorization for Scanning/Testing Activities 20
5.4 Deliverable Review and Acceptance 21
5.5 Project Change Request Process 21
6 Authorization to Proceed 22
APPENDIX A – About Presidio Cyber Security 23
Overview 23
APPENDIX B – Processes and Guidelines 24
Presidio Process for Network Degradation or Outage 24
Process to Report Observed Incidents or Critical Risks 24
Engagement Data Management 24
Appendix C – Williamson County Vendor Reimbursement Policy 25

1 EXECUTIVE SUMMARY

1.1 Background

Williamson County ("WilCo") has identified a need to determine the status of its information security and the level of risk it is currently incurring. To this end, WilCo is requesting that Presidio perform an assessment of its information security strategy and implementation or a subset thereof, as defined in the Engagement Scope section below, and provide to WilCo a clear picture of current risk levels.

1.2 Scope of Services

1.2.1 Engagement Management and Control

- **Engagement Management level**
  - Regular
    - Status meeting frequency – Weekly, during active periods of the project.
- Engagement Kickoff
  - Remote
- Deliverable Presentation
  - Remote

1.2.2 External Vulnerability Assessment

- [redacted] public IPs
- [redacted] active hosts
- Testing to be performed during business hours

1.2.3 Internal Vulnerability Assessment

- [redacted] servers
- [redacted] user endpoints
- Network scanning location(s): [redacted]
- [redacted]
- Password strength analysis is included
- Testing is to be performed Remote
- Testing to be performed during business hours

1.2.4 Wireless Infrastructure Assessment

- Onsite Requirements:
  - [redacted]

- 1 location(s) will be visited within 1 trip(s)

- [redacted]

[redacted]

1.2.5 Web Applications Assessment

- Authenticated scanning
  - 1 production application
  - [redacted]
  - 2 role(s) admin and user
- UnAuthenticated scanning
  - [redacted]production application
  - [redacted]
- Testing to be performed during business hours

1.2.6 External Penetration Testing

- [redacted]active external hosts to be tested
- OSINT-based Social Engineering included
- Evade Detection and Black Box testing are not included
- Testing to be performed during business hours

1.2.7 Internal Penetration Testing

- [redacted]
- <= 10,000 AD Users
- Targeted objective: Test network access as unauthenticated user
- Targeted objective: Test network access as authenticated user, attempt to pivot and test VLAN segregation
- Testing to be performed during business hours
- Testing will be performed on-site.

1.2.8 Remediation Assessment

- Conduct a single (1) Re-test of discovered issues defined as remediated
- Remediation assessment will be performed no more than 180 days after initial deliverable is completed

1.2.9 Travel

- Travel listed in section 4.3 is included in the fixed price milestones; additional travel initiated and approved in advance by WilCo will be reimbursed as defined in Appendix C – Williamson County Vendor Reimbursement Policy, and may incur an Engagement Change Authorization for additional travel time.

2 METHODOLOGY AND APPROACH

2.1 Engagement Management and Control

Detailed project planning is key to ensuring that the proposed engagement will meet requirements and help to reduce the risk of an ineffective project.

2.1.1 Regular

- Identify and schedule Presidio resources
  - Identify and schedule Presidio resources as appropriate to the engagement
- Hold kickoff meeting with key stakeholders
  - Review details of scope of work and methodology
  - Introduce key project team members and define roles and responsibilities
  - Review timelines, meetings, and additional requirements
  - Schedule implementation for discovery software
  - Schedule status meeting and other recurring touchpoints, as required
- Conduct status meetings at a frequency defined in this document
  - Review engagement progress
  - Identify engagement risks
  - Identify upcoming tasks
  - Request any additional customer or Presidio involvement
- Maintain and distribute engagement status report and schedule
  - All documents provided in Presidio formats
- Schedule Deliverable Presentation
  - Schedule mutually agreeable deliverable presentation

2.2 External Vulnerability Assessment

Presidio will review the external security of WilCo network, including data collection from publicly available sources (OSINT), scanning of in-scope networks, and vulnerability collation and validation. This process provides a clear picture of the risk from an external attacker (with the exception of detailed attacks into the structure of web applications), as well as a picture of the data WilCo is intentionally or unintentionally exposing on the public Internet.

- OSINT
  - Search common sources for WilCo data
  - Identify any customer networks not identified in scope
  - Identify any sensitive customer data available publicly
- Scheduling and target validation

  - Review target networks from scope and validate
  - Review additional networks from OSINT and verify testing
    - Testing of additional networks may incur a project change
  - Determine scheduled testing windows
  - Validate customer and tester contact information
- Network Scanning
  - Perform any required customization of scanning tools
  - Perform tool-based scan of in-scope networks
- Vulnerability Validation
  - Review discovered vulnerabilities and validate as appropriate
- Documentation
  - Prepare written report
    - Vulnerability
    - Risk Score
    - Suggested remediation
  - Prepare spreadsheet-based summary of vulnerabilities

2.3 Internal Vulnerability Assessment

Presidio will review the security of WilCo's network from inside the Internet perimeter. This will include basic validation of Active Directory (or other identity management platform) as well as both authenticated and unauthenticated scanning of in-scope hosts as defined in the scope of services. This will enable Presidio to provide a view of the risks based on privileged and service accounts, patching levels, as well as vulnerabilities with a high degree of confidence. WilCo will be able to clearly understand the risk should their perimeter protection be bypassed as is common in many current attack scenarios.

- Scheduling and target validation
  - Review target networks from scoping and discovery and validate
  - Determine scheduled testing windows
  - Validate customer and tester contact information
- Credentialed Network Scanning
  - Scan network with automated tools and customer-supplied administrative credentials
  - Determine vulnerabilities and patching status on all systems
- Active Directory Validation
  - Review existing accounts
    - Determine number and type of stale accounts
    - Review status of privileged accounts

  - Review password policy
  - Collect and perform basic review of Group Policy Objects
- Password Strength Analysis
  - Performed only if stated in Scope of Services
  - Securely obtain Active Directory passwords
  - Perform off-site analysis of passwords
    - Validate password complexity in use
    - Validate passwords meet written password standards
    - Determine any default or common passwords
    - Ensure all privileged accounts are correctly protected
- Vulnerability Validation
  - Review vulnerabilities and validate as appropriate
- Documentation
  - Prepare written report
    - Vulnerability
    - Risk Score
    - Suggested remediation
    - If applicable, password strength statistics and weak password details will be provided
  - Prepare spreadsheet-based summary of vulnerabilities

2.4 Wireless Infrastructure Assessment

Wireless networking can provide an avenue of entry to the network from outside the physical security perimeter. Presidio will test the security and configuration of both secured and unsecured ('guest') networks, validating the encryption, access control, and configuration of the platform to ensure that it is appropriate for the business' requirements.

- On-site scoping
  - Discover wireless networks
  - Validate wireless networks are owned by customer
- Testing
  - Scan wireless environment
  - Perform active testing against wireless networks
    - Encryption attacks
    - Access control attacks
    - Man-in-the Middle attacks

    - If access is obtained, determine possible compromise
        - Test wireless segmentation
- Validate guest network segmentation as appropriate
- Configuration review
    - Collect configurations for in-scope devices in text format
        - Review on-line configurations as required
    - Review management and control plane configuration
        - Review management protocols
        - Review control plane protection
        - Review device configuration standards
- Documentation
    - Prepare written report
        - Active testing issues
        - Configuration and control plane issues
        - Appropriate risk-level indication

2.5 Web Applications Assessment

Web Applications continue to present serious exposures to many customers. Presidio's Web Application testing extends the external or internal testing to include evaluation of the controls and function of web applications, and the associated vulnerabilities (including the OWASP Top 10. Examples include cross-site scripting, XML/SQL injection, input attacks, and similar).

The following tasks will be performed:

- Scoping
    - Validate URLs and testing windows with customer
    - Validate customer contact information
    - Collect any application documentation
    - Validate any credentials and roles for in-scope authenticated testing
- Discovery and Application Scope
    - Review all application documentation
    - Perform application discovery
        - Manual walk-through of application and pages
        - Tool-based spidering
        - Brute-force content discovery
    - Map application and identify input/output fields

- Testing
  - Perform automated and manual testing, including:
    - Configuration and Deployment Management Testing
    - Identity Management
    - Authentication & Authorization Testing
    - Session Management (authenticated testing only)
    - Input Validation Testing
    - Error handling
    - Business Logic Testing (authenticated testing only)
    - Weak Cryptography Implementations
    - Client-side Testing
- Validation
  - Perform appropriate validation of any discovered issue
- Documentation
  - Prepare written document
    - Vulnerability
    - Any suggested remediation
    - Risk Score

2.6 External Penetration Testing

Penetration testing focuses on assessing an organization's current security posture by simulating avenues of approach an attacker might take and determining the effectiveness of in-place security controls. During the penetration testing phase, Presidio will perform a testing cycle consisting of reconnaissance, initial compromise, privilege escalation, lateral movement, and achievement of targeted objectives. External Penetration Testing is conducted from a source outside of the LAN/WAN environment.

If Black Box Testing is selected in Scope of Services, only the identity of the company will be disclosed to the penetration testers. Target system validation will not occur until after reconnaissance steps are complete.

If OSINT-based social engineering is selected in Scope of Services, penetration testers will gather and use data to perform social engineering and phishing attacks as part of the penetration test to better simulate current attacker tactics.

If Evade Detection is selected in Scope of Services, penetration testers will use stealth techniques to avoid detection while conducting all steps.

The following tasks are performed as part of this phase, as defined in the Scope of Services:

- Scoping

  - Validate systems for testing
  - Validate testing windows
  - Validate contacts
  - Validate starting scenario and targeted objectives
  - Define Rules of Engagement
- Reconnaissance
  - Open source intelligence (OSINT) reconnaissance
  - Enumerate hosts and services
  - Perform additional reconnaissance as required
- Initial Compromise
  - Attempt to obtain initial access to systems through methods like:
    - Direct exploitation
    - Man-in-the-middle compromise
    - Misconfigured services and permissions
    - Weak security practices
    - Default or easily guessable credentials
    - Sensitive file exposure
    - Password spraying
    - Additional methods as appropriate. The above list is a sample of techniques; Presidio will expand on this list as required to achieve appropriate results.
- Escalation
  - Perform local privilege escalation
  - Validate additional hosts accessible
- Lateral Movement
  - Through compromised user accounts and systems, pivot to additional hosts
  - Perform additional penetration testing on accessible hosts
  - Continue testing cycle to achieve target objectives, compromise of sensitive data, and highest level of permissions possible
- Targeted Objectives
  - If possible, obtain access to identified target objectives
  - Attempt to discover possible critical data during testing cycle
- Clean-up
  - Remove any testing artifacts
  - Ensure any tools and access methods are removed

- Documentation
  - Prepare written report
  - Defined attack path
  - Systems and users compromised and methods used
  - Suggested remediation/mitigation steps
  - List of any artifacts, tools, or access that couldn't be removed

2.7 Internal Penetration Testing

Penetration testing focuses on assessing an organization's current security posture by simulating avenues of approach an attacker might take and determining the effectiveness of in-place security controls. During the penetration testing phase, Presidio will perform a testing cycle consisting of reconnaissance, initial compromise, privilege escalation, lateral movement, and achievement of targeted objectives. Internal Penetration Testing is conducted from a source inside the LAN/WAN environment.

If Evade Detection is selected in Scope of Services, penetration testers will use stealth techniques to avoid detection while conducting all steps.

If Network Device Penetration is selected in Scope of Services, penetration testers will attempt to compromise and use network devices and protocols (such as routing protocols) to further compromise systems and/or observe network traffic.

If Command and Control Testing is selected in Scope of Services, penetration testers will attempt to establish command and control channels to communicate with Presidio systems outside of LAN/WAN environment.

The following tasks are performed as part of this phase, as defined in the Scope of Services:

- Scoping
  - Validate systems for testing
  - Validate testing windows
  - Validate contacts
  - Validate starting scenario and targeted objectives
  - Define rules of engagement
- Reconnaissance
  - Open source intelligence (OSINT) reconnaissance
  - Enumerate hosts and services
  - Perform additional reconnaissance as required
- Initial Compromise
  - Attempt to obtain initial access to systems through methods like:
    - Direct exploitation

- Man-in-the-middle compromise
- Misconfigured services and permissions
- Weak security practices
- Default or easily guessable credentials
- Sensitive file exposure
- Password spraying
- Additional methods as appropriate. The above list is a sample of techniques; Presidio will expand on this list as required to achieve appropriate results.

- Escalation
  - Perform local privilege escalation
  - Validate additional hosts accessible
- Lateral Movement
  - Through compromised user accounts and systems, pivot to additional hosts
  - Perform additional penetration testing on accessible hosts
  - Continue testing cycle to achieve target objectives, compromise of sensitive data, and highest level of permissions possible
- Targeted Objectives
  - If possible, obtain access to identified target objectives
  - Attempt to discover possible critical data during testing cycle
- Clean-up
  - Remove any testing artifacts
  - Ensure any tools and access methods are removed
- Documentation
  - Prepare written report
  - Defined attack path
  - Systems and users compromised and methods used
  - Suggested remediation/mitigation steps
  - List of any artifacts, tools, or access that couldn't be removed

2.8 Remediation Assessment

During the remediation assessment scope element, Presidio will validate that issues detected and reported as remediated by the customer have, in fact, been resolved. Additionally, where the external and internal vulnerability assessment elements are incorporated, Presidio will fully rescan both of these and provide summary reporting on both all detected issues and on any resolved issues. Should issues be resolved in phases requiring on-site travel (wireless, some social engineering, physical security and similar) and the customer wishes a full test, Presidio will issue

a Change Request to add travel time to this element to allow consultants to visit the facilities that are in scope

The following tasks will be performed:

- Scoping
    - Determine remediated vulnerabilities
    - Schedule scanning windows for vulnerability scans
    - Determine if any travel is required and generated appropriate change requests
- Testing
    - Perform vulnerability scan all in scope external networks
    - Perform vulnerability scan all in scope internal networks
    - Remotely validate remediation of issues
- Reporting
    - Generate summary reporting on resolved and still existing issues
    - Generate spreadsheet reporting on vulnerability scanning
        - Full updated PDF report will not be provided
    - Upload activity to NGRM Program Portal if deployed at customer site as part of initial engagement
        - Not all engagements will have this portal deployed.
        - If the NGRM portal is not deployed, risk score will not be recalculated

3 DELIVERABLES

Deliverable	Description	Format
Status Report	Artifact which depicts key task areas, actions, owners, estimated completion dates, task status and overall project status and delivered following each status meeting.	PDF
Executive Summary	Overview of the assessment, including approach, methodology, and summary of findings. Format to be appropriate for non-technical, executive audience. Report will include all phases and tasks.	PPT/PDF
Assessment Findings Report	Report showing all findings from the project. All risks (associated to vulnerabilities) will be listed with a risk score, references, and a suggested remediation.	PDF
Vulnerability Registers	Sortable list of discovered vulnerabilities from external and internal vulnerability scanning activities.	Excel
Remediation Report	Report showing remediated vulnerabilities and status of remaining open issues. Risk score will not be recalculated.	PDF

Deliverables will be released via secure exchange only to the WilCo project sponsor or to others with written permission from the project sponsor.

Final presentations and closeout must be completed within thirty (30) days after the day the original documentation deliverable is released to WilCo. If the deliverable presentations are not completed in this timeframe, Presidio will consider this phase completed and will invoice accordingly.

4 ASSUMPTIONS

Presidio made the following assumptions when developing this Statement of Work. These assumptions serve as the foundation to which the project estimate, approach, and timeline were developed. Any changes to the following assumptions must be processed using the procedures the section titled "Project Change Request Process"

4.1 General

The following project assumptions are made and will be verified as part of the engagement:

- All Presidio activities will take place during normal working hours (Monday through Friday, 8:00 a.m. to 5:00 p.m., excluding holidays) unless noted as "Off Hours" in this SOW.
- Any items or tasks not explicitly listed as in-scope within this SOW are considered to be outside of the scope and not associated with this SOW and price.
- If integration of the product is performed at a Presidio facility, then transfer of ownership (acceptance) occurs upon the receipt and integration of goods at Presidio, regardless of shipment, as manufacturers will not accept returns of opened products.
- Changes to the Design, Equipment List or proposed timeline presented to Client in this SOW will require a Project Change Request. A Project Change Request could impact the cost of the project
- Presidio will not be held responsible for troubleshooting networks, applications and/or hardware if Client has no formal change management documented processes and policies
- Presidio may engage subcontractors and third parties in performing a portion of this work.
- Some activities included in this project may be performed on Presidio's premises.
- Additional required tasks discovered after the execution of this SOW that are not mentioned in this SOW will require a Project Change Request.
    - Presidio will provide clear guidance on the changes required to ensure optimal deployment.

4.2 General Client Responsibilities

The following items are listed as responsibilities of Client for this engagement. Client is responsible for performing the items and activities listed in this section or arranging for them to be performed by a third-party if appropriate.

- Provide a single Client point of contact with the authority and the responsibility of issue resolution and the identification, coordination and scheduling of Client personnel to participate in the implementation of the SOW.
- Participate in any required design sessions or workshops.
- Supply current equipment configuration for review if applicable.

- Provide all required physical access to Client's facility (identification badge, escort, parking decal, etc.), as required by Client's policies; and provide all required functional access (passwords, IP address information, etc.), as required for Presidio to complete the tasks.
- Provide to Presidio all required IP addresses, passwords, system names, and aliases.
- Validate the site readiness prior to the dispatch of Presidio personnel to perform the services being contracted.
- Provide adequate facilities for the installation of the hardware. This includes all necessary peripheral hardware (KVM ports or monitors, keyboards, mice, network access, etc.) as well as electrical and spatial needs and required antivirus software.
- Provide Presidio administrator access on appropriate devices for the completion of the engagement.
- Provide requested documentation or information needed for the project within two (2) business days, unless otherwise agreed to by all parties.
- Provide to Presidio all relevant Client information security and information technology policies and procedures.
- Provide to Presidio all requested information about and administrative access to Client's technical infrastructure for the duration of the project, including, but not limited to, each technology component described in each phase listed above.
    - For phases that include a Technical Configuration Review activity, remote access is required, AND administrative access must be sufficient to fully analyze the entire configuration of each technology component.
- Provide a work area and network connectivity for Presidio consultants for on-site work when needed.
- Client will make all network and endpoint changes and configurations as required to integrate Presidio's tools.

4.3 Travel

Presidio has made the following assumptions for travel:

- Presidio will complete the following travel as part of this engagement:
    - Up to 2 trip(s)
    - Up to 5 day(s) total
- The following phase(s) will be performed on-site:
    - Wireless Infrastructure Assessment
    - Internal Penetration Test
- Costs for travel listed in this section are included in the fixed price fee.

4.4 Internal Vulnerability Assessment

- Customer will provision a virtual host to Presidio's specifications or will provide connectivity and power for a Presidio-provided system. Customer will allow Presidio remote access to these systems to allow for internal scanning.
- Customer will provide VPN-based remote access to the provisioned virtual host or will allow other remote access as determined during the kickoff meeting
- The following specifications are required to run the necessary software during this phase
  - Windows Server 2008, 2012 or 2016
  - (4) >= 2.4G vCPU
  - (16) GB RAM
  - (40) GB Hard Drive
  - Local admin rights

5 TERMS AND CONDITIONS

5.1 General

This Service Agreement is governed by DIR Contract Number DIR-TSO-3847 between PRESIDIO and the Texas Department of Information Resources.

5.2 Payment Schedule

Upon acceptance of this Agreement (as indicated by its execution below) Presidio agrees to provide to Customer, and Customer agrees to purchase from Presidio, services in accordance with this Statement of Work (SOW) and the following terms and conditions.

Presidio shall complete the following milestones in accordance with this SOW. Presidio shall invoice Customer as indicated below, plus applicable expenses, according to this SOW.

Milestone	Cost
Upon Project Kickoff	$ 15,100.00
Baseline Assessment Deliverables Release	$ 41,550.00
Executive Presentation Complete	$ 7,560.00
Remediation Assessment Complete	$ 11,340.00
Total	**$ 75,550.00**

Pricing is valid for 60 days from the last revision date of this SOW.

Bill To
Williamson County
301 SE Inner Loop
Georgetown, Texas 78626
Attention: Accounts Payable

5.3 Authorization for Scanning/Testing Activities

Presidio is authorized to perform vulnerability, web application, penetration testing and social engineering activities for the services performed in this Statement of Work (SOW). Such activities shall be confined to the infrastructure described in the SOW under Section 1.2. Presidio is not authorized to assess any other networks under this agreement. The security assessment involves the use of network tools and techniques designed to detect security vulnerabilities, and it is impossible to identify and eliminate all the risks involved with the use of these tools and techniques. WilCo understands that penetration testing may be disruptive and explicitly accepts the risk of such disruption. Presidio will take all reasonable precautions to minimize any impact. WilCo hereby authorizes employees of Presidio to conduct penetration testing activities of the

application(s) and system(s) described in this SOW. This authorization shall be in effect from the day of the engagement kickoff meeting to the day the final deliverable from the engagement is provided to WilCo.

Pursuant to granting this authorization, WilCo declares that:

- WilCo owns the systems to be tested and the undersigned has the proper authority to allow Presidio to perform vulnerability, web application and penetration testing security activities.
- WilCo has created a full backup of all systems to be tested and has verified that the backup procedure will enable WilCo to restore systems to their pretest state.

5.4 Deliverable Review and Acceptance

With the exception of Project Status Reports, each deliverable material, as defined in this Statement of Work, will be approved in accordance with the following procedure.

Within 5 business days of receipt, Customer will either accept the deliverable material or provide the Presidio project manager a written list of requested changes. If no written response, either accepting or requesting changes, is received from Customer within 5 business days, then the deliverable material shall be deemed accepted.

If a written list of requested changes is received within 5 business days, the Presidio project team will review and ensure that these changes do not impact the accuracy or veracity of the report and other deliverables. If this is the case, Presidio will make the appropriate revisions and will, within 5 business days, re-submit the updated version to Customer.

Once the updated version is received, Customer has 5 further business days to review and request changes for the final document. If no written response, either accepting or requesting changes, is received from Customer within five (5) business days, then the deliverable material shall be deemed accepted.

No further alternations of the document will be performed after these two revisions without approval from the Presidio account team. Additional revisions and changes may incur additional effort and charges at the discretion of the Presidio account team.

5.5 Project Change Request Process

In the event that both Presidio and Client agree to a change in this Statement of Work, a written description of the agreed upon change will be prepared using a Project Change Request (PCR) form, which both parties must sign. The PCR form will be used to describe the change, the rationale for the change, and to specify any change in the charges, estimated schedule, or other terms. Depending on the extent and complexity of the requested changes, Presidio may charge for the effort required to analyze it. When charges are necessary to analyze a change, Presidio will provide a written estimate and begin the analysis upon written authorization from Client. The terms of a mutually agreed upon Change Authorization will prevail over those of this Statement of Work or any previous Change Authorization.

6 AUTHORIZATION TO PROCEED

The use of signatures on this Statement of Work is to ensure agreement on project objectives and the work to be performed by Presidio.

Presidio signature signifies our commitment to proceed with the project as described in this document. Please review this document thoroughly, as it will be the basis for all work performed by Presidio on this project.

This Statement of Work is valid for a period of sixty (60) days from the date that this Statement of Work is provided by Presidio to Client unless otherwise agreed to by both parties.

Williamson County

Signature Date

Printed Name

Presidio

Kim Dukes (Jul 1, 2019)

Signature Date

Kim Dukes Director of Sales Operations

Printed Name & Title

Please sign and return the entire document to Brett Marlier bmarlier@presidio.com

Thank you!

APPENDIX A – ABOUT PRESIDIO CYBER SECURITY

Overview

Presidio has been providing technical security assessment and governance, risk, and compliance services to clients for over decade. Our experience spans all major verticals, including retail, education, healthcare, government, banking, and more. Presidio's consultants are highly experienced and certified professionals with strong backgrounds in security, compliance, and fundamental technology areas.

The mission of the Presidio security practice is to help organizations design, implement and maintain sound cyber security programs. These programs are consistent with industry best practices and relevant compliance mandates and are designed to ensure the security of sensitive information in an ever-changing risk environment.

Our approach focuses on business risk, whether in discovering unknown risks, or managing known ones. Without the knowledge of what is at risk, and to what extent, it is difficult for our clients to establish effective security programs. As such, we can assist in identifying these risks across multiple domains of security and in creating effective programs to manage them one known. These programs are founded in effective policies, procedures, and standards which drive the appropriate implementations of technical and non-technical controls. We focus on the three core principles of cyber security:

- Confidentiality - the protection of information resources from unauthorized access or disclosure.
- Integrity - the accuracy, reliability and completeness of information and systems and the prevention of unauthorized modification.
- Availability - the assurance that information is accessible by authorized individuals as needed and when needed.

The Presidio Cyber Security practice provides unique offerings in four areas, all of which combine to provide Next Generation Risk Management (NGRM):

- Information Security Program Architecture
- Technical Vulnerability Assessments and Penetration Testing
- Governance, Risk, and Compliance Assessment
- Network Security Architectures

A $2.8 billion corporation focusing on practical thinking for a connected world, Presidio has more than 2,800 employees in 60 offices throughout the United States.

APPENDIX B – PROCESSES AND GUIDELINES

Presidio Process for Network Degradation or Outage

Presidio and WilCo will exchange specific contact information (including cell phone numbers) prior to starting any scanning or testing activities. Either party observing a service disruption will contact the other party. Presidio will stop running the scan tool and work with WilCo to determine why the disruption occurred and how to successfully complete the assessment without causing any further disruption. No denial-of-service (DoS) attacks will be intentionally initiated against any WilCo assets.

Process to Report Observed Incidents or Critical Risks

Presidio will contact the WilCo contact immediately if any critical risks are identified (those which present sufficient risk to warrant immediate remediation), including any observed incidents of attempted intrusion (from a party other than the authorized Presidio consultant[s]), while executing this engagement. Presidio will immediately provide to WilCo all information gathered relevant to the critical risk(s) identified.

Engagement Data Management

The deliverables produced from this engagement should be managed with strict policies and procedures due to the sensitive nature of the raw data collected during the engagement and the associated findings WilCo's policies should specify which person(s) in an organization should have access to the data. Presidio consultants will store and transmit engagement-related data using appropriate encryption.

APPENDIX C – WILLIAMSON COUNTY VENDOR REIMBURSEMENT POLICY

Williamson County
Vendor Reimbursement Policy

The purpose of this Williamson County Vendor Reimbursement Policy ("Policy") is to provide clear guidelines to vendors on Williamson County's expectations and requirements regarding allowable reimbursable expenditures and required backup. The Policy will also minimize conflicts related to invoice payments and define non-reimbursable items. This Policy is considered a guideline and is not a contract.

This Policy may be altered, deleted or amended, at any time and without prior notice to vendors, by action of the Williamson County Commissioners Court. Unenforceable provisions of this Policy, as imposed by applicable law, regulations, or judicial decisions, shall be deemed to be deleted. Any revisions to this Policy will be distributed to all current vendors doing business with the County.

1 Invoices and Affidavits

1.1 Invoices must adequately describe the goods or services provided to County and include all required backup (i.e. reimbursable expenses, mileage log, timesheets, receipts detailing expenses incurred etc.) that is in a form acceptable to the Williamson County Auditor. Invoices that do not adequately describe the goods or services provided to County or contain backup that is satisfactory to the Williamson County Auditor will be returned to vendor for revisions and the provision above relating to invoice errors resolved in favor of the County shall control as to the required actions of vendor and when such invoice must be paid by the County.

1.2 In the event an invoice includes charges based upon hourly billing rates for services or any other rates based upon the amount of time worked by an individual or individuals in performing services, whether the charges are being billed directly to the County or whether they are the basis of invoices from subcontractors for which the vendor seeks reimbursement from the County, the charges shall be accompanied by an affidavit signed by an officer or principal of the vendor certifying that the work was performed, it was authorized by the County and that all information contained in the invoice that is being submitted is true and correct.

1.3 Upon County's request, vendor must submit all bills paid affidavits wherein vendor must swear and affirm that vendor has paid each of its subcontractors, laborers, suppliers and material in full for all labor and materials provided to vendor for or in connection with services and work performed for County and, further, vendor must swear and affirm that vendor is not aware of any unpaid bills, claims, demands, or causes of action by any of its subcontractors, laborers, suppliers, or material for or in connection with the furnishing of labor or materials, or both, for services and work performed for County.

2 Travel Reimbursement

2.1 The County will only cover costs associated with travel on vendors outside a 50 mile radius from Williamson County, Texas.

2.2 The County will only cover costs associated with travel as documented work for County. If a vendor is also doing business for another client, the travel costs must be split in proportion to the amount of work actually performed for County and the other client. The only allowable travel expense will be for the specific days worked for Williamson County.

2.3 No advance payments will be made to vendor for travel expenditures. The travel expenditure may only be reimbursed after the expenditure/trip has already occurred and vendor has provided the Williamson County Auditor with all necessary and required backup.

2.4 Vendors must submit all travel reimbursement requests on each employee in full. Specifically, a travel reimbursement request must include all related travel reimbursement expenses relating to a particular trip for which vendor seeks reimbursement. Partial travel reimbursement requests will not be accepted (i.e. vendor should not submit hotel and mileage one month then the next month submit rental car and airfare). If the travel reimbursement appears incomplete, the invoice will be sent back to the vendor to be submitted when all information is ready to submit in full.

2.5 Reimbursement for transportation costs will be at the most reasonable means of transportation (i.e.: airline costs will be reimbursed for coach rate, rental car costs will only be reimbursed if rental car travel was most reasonable means of travel as compared to travel by air).

2.6 The County will not be responsible for, nor will the County reimburse additional charges due to personal preference or personal convenience of individual traveling.

2.7 The County will not reimburse airfare costs if airfare costs were higher than costs of mileage reimbursement.

2.8 Additional expenses associated with travel that is extended to save costs (i.e. Saturday night stay) may be reimbursed if costs of airfare would be less than the cost of additional expenses (lodging, meals, car rental, mileage) if the trip had not been extended. Documentation satisfactory to the Williamson County Auditor will be required to justify expenditure.

2.9 County will only reimburse travel expense to necessary personnel of the vendor (i.e. no spouse, friends or family members).

2.10 Except as otherwise set forth herein, a vendor must provide a paid receipt for all expenses. If a receipt cannot be obtained, a written sworn statement of the expense from the vendor may be substituted for the receipt.

2.11 Sales tax for meals and hotel stays are the only sales taxes that will be reimbursed. Sales tax on goods purchased will not be reimbursed. A sales tax exemption form is available from the Williamson County Auditor's Office upon request.

2.12 The County will not pay for any late charges on reimbursable items. It is the responsibility of the vendor to pay the invoice first and seek reimbursement from the County.

3 Meals

3.1 Meal reimbursements are limited to a maximum of $50.00 per day on overnight travel. On day travel (travel that does not require an overnight stay), meal reimbursements are limited to a maximum of $20.00 per day. The travel must be outside the Williamson County, Texas line by a 50 mile radius.

3.2 Receipts are required on meal reimbursement amounts up to the maximum per day amount stated for overnight or day travel. If receipts are not presented, the vendor can request per diem (per diem limits refer to 3.2). However, a vendor cannot combine per diem and meal receipts. Only one method shall be allowed.

3.3 Meals are reimbursable only for vendors who do not have the necessary personnel located within a 50 mile radius of Williamson County, Texas that are capable of carrying the vendor's obligations to County. Meals will not be reimbursed to vendors who are located within a 50 mile radius of Williamson County, Texas.

3.4 County will not reimburse for alcoholic beverages.

3.5 Tips are reimbursable but must be reasonable to limitation of meal allowance

3.6 No meals purchased for entertainment purposes will be allowed.

3.7 Meal reimbursement must be substantiated with a hotel receipt.

4 Lodging

4.1 Hotel accommodations require an itemized hotel folio as a receipt. The lodging receipt should include name of the motel/hotel, number of occupant(s), goods or services for each individual charge (room rental, food, tax, etc.) and the name of the occupant(s). Credit card receipts or any other form of receipt are not acceptable.

4.2 Vendors will be reimbursed for a single room rate charge plus any applicable tax. If a single room is not available, the vendor must provide documentation to prove that a single room was not available in order to justify the expense over and above the single room rate. A vendor may also be required to provide additional documentation if a particular room rate appears to be excessive.

4.3 Personal telephone charges, whether local or long distance, will not be reimbursed.

5 Airfare

5.1 The County will only reimburse up to a coach price fare for air travel.

5.2 The County will exclude any additional charges due to personal preference or personal convenience of the individual traveling (i.e. early bird check in, seat preference charges, airline upgrades, etc. will not be an allowable reimbursement)

5.3 Air travel expenses must be supported with receipt copy of an airline ticket or an itinerary with actual ticket price paid. If tickets are purchased through a website, vendor must submit a copy of the webpage showing the ticket price if no paper ticket was issued.

5.4 Cancellation and/or change flight fees may be reimbursed by the County but vendor must provide the Williamson County Auditor with documentation in writing from a County department head providing authorization for the change.

5.5 The County will not reimburse vendor for tickets purchased with frequent flyer miles.

6 Car Rental

6.1 Vendors that must travel may rent a car at their destination when it is less expensive than other transportation such as taxis, airport shuttles or public transportation such as buses or subways.

6.2 Cars rented must be economy or mid-size. Luxury vehicle rentals will not be reimbursed. Any rental costs over and above the cost of a mid-size rental will be adjusted.

6.3 Vendors will be reimbursed for rental cars if the rental car cost would have been less than the mileage reimbursement cost (based on the distance from vendor's point of origin to Williamson County, Texas) had the vendor driven vendor's car.

6.4 Vendors must return a car rental with appropriate fuel levels as required by rental agreement to avoid the car rental company from adding fuel charges.

6.5 Rental agreement and credit card receipt must be provided to County as back up for the request for reimbursement.

6.6 Insurance purchased when renting vehicle may also be reimbursed.

6.7 Car Rental optional extras such as GPS, roadside assistance, and administrative fees on Tolls will not be reimbursed.

7 Personal Car Usage

7.1 Personal vehicle usage will be reimbursed in an amount equal to the standard mileage rate allowed by the IRS.

7.2 Per code of Federal Regulations, Title 26, Subtitle A, Chapter 1, Subchapter B, Part IX, Section 274(d), all expense reimbursement requests must include the following:

7.2.1.1 Date
7.2.1.2 Destination
7.2.1.3 Purpose
7.2.1.4 Name of traveler(s)
7.2.1.5 Correspondence that verifies business purpose of the expense

7.3 The mileage for a personal vehicle must document the date, location of travel to/from, number of miles traveled and purpose of trip.

7.4 Mileage will be reimbursed on the basis of the most commonly used route.

7.5 Reimbursement for mileage shall not exceed the cost of a round trip coach airfare.

7.6 Reimbursement for mileage shall be prohibited between place of residence and usual place of work.

7.7 Mileage should be calculated from employee's regular place of work or their residence, whichever is the shorter distance when traveling to a meeting or traveling to Williamson County, Texas for vendors who are located outside of Williamson County, Texas by at least a 50 mile radius.

7.8 When more than one person travels in same vehicle, only one person may claim mileage reimbursement.

7.9 Tolls, if reasonable, are reimbursable. Receipts are required for reimbursement. If a receipt is not obtainable, then written documentation of expense must be submitted for reimbursement (administrative fees on Tolls will not be reimbursed).

7.10 Parking fees, if reasonable are reimbursable for meetings and hotel stays. For vendors who contract with a third party for visitor parking at vendor's place of business, Williamson County will not reimburse a vendor based on a percentage of its contracted visitor parking fees. Rather, Williamson County will reimburse Vendor for visitor parking on an individual basis for each time a visitor uses Vendor's visitor parking. Receipts are required for reimbursement. If a receipt is not obtainable, then written documentation of expense must be submitted for reimbursement.

7.11 Operating and maintenance expenses as well as other personal expenses, such as parking tickets, traffic violations, and car repairs and collision damage are not reimbursable.

8 Other Expenses

8.1 Taxi fare, bus tickets, conference registrations, parking, etc. must have a proper original receipt.

9 Repayment of Nonreimbursable Expense.

Vendors must, upon demand, immediately repay County for all inappropriately reimbursed expenses whenever an audit or subsequent review of any expense reimbursement documentation finds that such expense was reimbursed contrary to these guidelines and this Policy. Williamson County reserves the right to retain any amounts that are due or that become due to a vendor in order to collect any inappropriately reimbursed expenses that a vendor was paid.

10 Non-Reimbursable Expenses

In addition to the non-reimbursable items set forth above in this Policy, the following is a nonexhaustive list of expenses that will not be reimbursed by Williamson County:

10.1 Alcoholic beverages/tobacco products
10.2 Personal phone calls
10.3 Laundry service
10.4 Valet service (excludes hotel valet)
10.5 Movie rentals
10.6 Damage to personal items
10.7 Flowers/plants
10.8 Greeting cards
10.9 Fines and/or penalties
10.10 Entertainment, personal clothing, personal sundries and services
10.11 Transportation/mileage to places of entertainment or similar personal activities
10.12 Upgrades to airfare, hotel and/or car rental
10.13 Airport parking above the most affordable rate available

10.14 Excessive weight baggage fees or cost associated with more than two airline bags
10.15 Auto repairs
10.16 Babysitter fees, kennel costs, pet or house-sitting fees
10.17 Saunas, massages or exercise facilities
10.18 Credit card delinquency fees or service fees
10.19 Doctor bills, prescription and other medical services
10.20 Hand tools
10.21 Safety Equipment (hard hats, safety vests, etc.)
10.22 Office Supplies
10.23 Lifetime memberships to any association
10.24 Donations to other entities
10.25 Any items that could be construed as campaigning
10.26 Community outreach items exceeding $2 per item
10.27 Technology Fees
10.28 Sales tax on goods purchased
10.29 Any other expenses which Williamson County deems, in its sole discretion, to be inappropriate or unnecessary expenditures.