STATEMENT OF WORK (CONSULTING SERVICES AGREEMENT)

This Statement of Work (SOW) is executed on June__, 2025 between Securance LLC ("Securance") and the Village of Orland Park ("Client"). Paul Ashe will act as the Securance Engagement Manager and will be your central point of contact. This SOW pertains directly to the request for services detailed below.

A. SCOPE

Securance intends to perform the following activities, as agreed upon between management of Securance and Client:

Project Scope Item	Line Item Fee
External, Internal, and Wireless Network Vulnerability Assessments and Penetration Tests *Includes 10 public IP addresses, approximately 500 internal IP addresses, and 4 SSIDs and 13 wireless network locations.*	$7,440
Cybersecurity Risk Assessment and Benchmarking Against the NIST Cybersecurity Framework and CIS Controls	$9,920
Next-Generation Firewall Configuration Review – Sample of 2 Firewalls	$4,712
Mobile Device Security Assessment *Includes 227 iPhones and iPads and an assessment of the MaaS 360 MDM solution.*	$3,968
Router and Switch Configuration Review – Sample Basis	$2,976
Endpoint Security Assessment	$2,480
Review of Data Communications Between SaaS Provider and the On-Premises Network	$3,472
CJIS Compliance Review*	$14,440
Management Report – Executive Summary, NIST and CIS Controls Gap Analysis, and Security Testing Results	$4,960
Remediation Roadmap	$1,984
Technical Vulnerability Assessment Reports – 1-Year Follow-up	$992
Knowledge Transfer	~~$3,968~~ **FREE VALUE ADD**
Status Reporting	~~$2,976~~ **FREE VALUE ADD**
1 Year Follow-up	
External Network Vulnerability Assessment and Penetration Test	~~$3,968~~ **FREE VALUE ADD**
Project Total with Optional CJIS Compliance Review	~~**$68,696**~~ **$57,344**

*Securance's process for reviewing CJIS compliance will include the following activities:

1. Interview key personnel, including the Local Agency Security Officer (LASO), responsible for the security of criminal justice information (CJI).
2. Review policies and procedures governing how CJI is handled and secured.
3. Review interagency agreements that outline the process of sharing, sending, and receiving CJI.
4. Review agreements with vendors and contractors for access to or the storage of CJI.
5. Verify that all personnel, including agency and IT staff members and vendors, with access to CJI and applications, systems, or networks that store, process, or transmit CJI have completed the

proper screening and security awareness training. Ensure that personnel screening, fingerprint, and security awareness training records are current.

6. Review the incident management plan and process, including:
    a. Incident handling capabilities
    b. Tracking and documentation of security incidents
    c. Incident response roles and responsibilities
    d. Training
    e. Automated mechanisms employed to support the process
7. Review audit and accountability controls within CJI systems, including:
    a. Auditable events
    b. Content of audit records
    c. Retention of audit records
8. Review logical access controls, including:
    a. Account management
    b. Access control criteria, mechanisms, and enforcement
    c. Least privilege
    d. Remote access to CJI systems
9. Review the identification and authentication policies and procedures. Review the use of identifiers and authenticators such as passwords, one-time passcodes, and personal identification numbers (PINs).
10. Review the network diagram and verify that CJI systems are configured to provide only essential capabilities and to restrict or prohibit the use of unnecessary functions, ports, protocols, and services.
11. Review the media protection policy and the processes for secure media storage, transportation and disposal. Determine how CJI is protected from unintentional or unauthorized viewing.
12. Conduct a physical inspection to verify that CJI and information systems' hardware, software, and media are physically protected through access controls.
13. Review information integrity controls, including:
    a. Boundary protections
    b. How CJI is encrypted at rest and in transit
    c. Intrusion detection and prevention tools and techniques
    d. Patch management
    e. Protections against malware, spam, and spyware
14. Review mobile and wireless security, including:
    a. Usage restrictions and implementation guidance for mobile devices
    b. Mobile device management
    c. Wireless network security

B. STAFF

Securance will staff this project with one or more Senior IT Consultants and the Engagement Manager. The Engagement Manager will be responsible for the execution of certain fieldwork items. Additions to the team may be made as needed or requested by Client's Project Manager.

C. TIMESCALE

The start date for this project will be determined upon execution of the SOW.

D. DELIVERABLES

Upon completion of all fieldwork associated with this project and the scope items listed in Section A, Securance will submit a draft management report to Client for review and approval. In addition, throughout the course of the project, Securance will participate in meetings and discussions with Client, as agreed upon or as requested.

E. DEPENDENCIES AND ASSUMPTIONS

The following dependencies and assumptions apply to the services to be provided under this SOW:

1. Securance will provide a Client Assistance Memo to Client prior to commencing the project.
2. Securance will have full access to all Client participants and personnel, as required for interviews, meetings, and/or discussions, throughout the duration of the project.
3. Client will hold meetings with the Securance Engagement Manager, as necessary, to assess progress.
4. Each component of the project will be performed at a mutually agreed-upon time to minimize disruption to Client personnel.

F. PRICING AND PAYMENT

Our pricing for this effort is $57,344.00. Securance will submit an invoice after delivering the draft cybersecurity audit report. All fees are due and payable via ACH/EFT upon receipt of invoice. Securance will deliver the final cybersecurity audit report after receiving payment from client.

Should any material changes in scope occur or unforeseen situations arise, Securance will first determine their potential impact on the project approach, schedule, and professional fees, then present any changes to Client for discussion and consideration.

By agreeing to the terms of this SOW, Client will not offer employment to, or hire, any Securance professionals assigned to this project for a six-month period after completion of the project without Securance's explicit written consent. Reciprocally, Securance will not offer employment to, or hire, any Client professionals assigned to this project for a six-month period after completion of the project without Client's explicit written consent.

Securance will not undertake to perform any obligations of Client, whether regulatory or contractual, assume any responsibility for the management of Client's compliance function, form any part of Client's internal control structure, or act, or appear to act, in a capacity equivalent to that of a member of management or an employee of Client.

By signing below, signor represents and affirms that they are duly authorized to bind the organization to this SOW.

Accepted and agreed: **VILLAGE OF ORLAND PARK**	Accepted and agreed: **SECURANCE LLC**
By: _____ *Please Sign*	By: _____ *Please Sign*
Name: _____ *Please Type*	Name: _____ *Please Type*
Title: _____ *Please Type*	Title: _____ *Please Type*
Date: _____ *Please Type*	Date: _____ *Please Type*