Sterling Legal Group

SOW xx002 for agreement to perform consulting services to Oakwood

DATE	SERVICES PERFORMED BY:	SERVICES PERFORMED FOR:
Sept 19th 2025	DKB Innovate 321 Sycamore Ave. Albany, NY 76543	Sterling Legal Group 123 South Street Manhattan, NY 54321

Index

Engagement Resources

Name	Role	Contact
Zachary Gafford	Solutions Engineer	Xxx-xxxx xxx.xxxx@xxxx.com

Executive Summary

Sterling Legal Group recently experienced a serious security incident where a partner's email account was compromised through a sophisticated phishing attack. While no data was exfiltrated, this incident highlighted the urgent need to leverage Microsoft 365 Business Premium features for comprehensive security hardening and compliance. This proposal outlines a plan to fully implement M365's advanced security, compliance, and training capabilities to protect sensitive client data and meet industry standards.

Current Environment

Security	No Multi-Factor Authentication (MFA) enforced.
Group Policy	No conditional access policies configured.
Email Gateway	Default email filtering settings.
Corporate Policy	Data scattered across SharePoint, OneDrive, and local desktops without a unified policy.

Project Goals & Scope

- Prevent unauthorized account access.
- Protect against phishing, malware, and other email-based threats.
- Implement basic Data Loss Prevention (DLP) to safeguard sensitive client information.
- Provide an action plan for ongoing user security training.

Proposed Solution

PS.1 Identity & Access Management

Mandatory Multi-Factor Authentication (MFA): Enforce MFA for all Microsoft 365 user and administrator accounts, including service and break-glass accounts, to block unauthorized sign-ins.

Granular Conditional Access: Deploy Azure AD (Microsoft Entra ID) Conditional Access policies to verify user risk, device compliance, location, and sign-in patterns before granting access. Policies will include blocking legacy authentication protocols and requiring compliant devices for sensitive apps.

Passwordless Authentication: Enable passwordless sign-in options such as Microsoft Authenticator push approvals and FIDO2 security keys to eliminate password-based attack vectors.

Privileged Identity Management (PIM): Implement just-in-time (JIT) access for administrative roles so elevated rights are granted only when needed and automatically expire, with full audit trails.

Device Compliance & Encryption: Enforce device compliance policies via Microsoft Intune, requiring BitLocker full-disk encryption for all Windows endpoints and ensuring recovery keys are securely stored in Azure AD.

Continuous Monitoring & Auditing: Activate Azure AD Identity Protection to detect risky signins and compromised credentials, and centralize all identity and sign-in logs within Microsoft Sentinel, Microsoft's cloud-native SIEM and SOAR platform, for real-time threat detection, automated incident response, and long-term compliance reporting.

PS.2 Email Security & Threat Protection

Microsoft Defender for Office 365 (Plan 2): Deploy with Safe Links and Safe Attachments to actively scan and detonate email URLs and attachments before delivery.

Advanced Anti-Phishing & Anti-Spam Policies: Enforce enhanced protection levels and block legacy authentication to stop credential-harvesting and bulk email attacks.

Impersonation & Spoofing Protection: Enable targeted protection for executives, partners, and key domains to prevent business email compromise (BEC) and look-alike domain attacks.

Domain-based Message Authentication, Reporting & Conformance (DMARC), SPF, and DKIM: Implement these standards to validate outbound email and reduce the chance of spoofed messages reaching clients.

Quarantine & Automated Remediation: Configure quarantine policies with automated investigation and response (AIR) to isolate suspicious messages and, when confirmed malicious, remediate across mailboxes.

Continuous Monitoring & SIEM Integration: Send Defender for Office 365 alerts and message trace logs to Microsoft Sentinel (SIEM/SOAR) for long-term auditing, analytics, and automated incident response.

PS.3 Data Loss Prevention & Compliance

Data Loss Prevention (DLP): Deploy Microsoft Purview DLP policies to identify and protect client-attorney privileged information and personally identifiable information (PII) across Exchange Online, SharePoint, OneDrive, and Teams, blocking or auditing unauthorized sharing.

Sensitivity Labels & Encryption: Use Microsoft Purview Information Protection to apply automatic and user-driven sensitivity labels to confidential documents and email, enforcing encryption, watermarking, and access restrictions wherever the data travels.

Retention & Records Management: Configure Microsoft Purview Data Lifecycle Management / Records Management to apply retention and disposition policies aligned with ABA and state bar requirements, preserving or defensibly deleting legal records and supporting e-discovery and litigation holds.

PS.4 Security Awareness & Training

Microsoft 365-Integrated Training: Launch a built-in security awareness program that delivers short, engaging modules directly through Microsoft 365.

Simulated Phishing & Targeted Follow-ups: Run regular phishing simulations and provide just-in-time coaching for users who need reinforcement.

Video Walkthroughs for Key Security Steps: Provide step-by-step video training on setting up multi-factor authentication (MFA) and registering FIDO2 security keys, ensuring every employee can easily secure their account.

Quarterly Security Updates: Share concise quarterly briefings on new threats and best practices to keep security awareness fresh.

Implementation Plan

Man-Hours

Phase	Implementation	Details	Time-Frame
Phase1	Assessment & Design	Conduct a security baseline review, validate Microsoft 365 licensing, and finalize identity, email, and compliance policies	(3 days)
Phase2	Identity & Access Hardening	Enforce MFA, configure Conditional Access, and deploy passwordless authentication with security keys.	(4 days).

Phase3	Email Security Deployment	Configure Microsoft Defender for Office 365 with Safe Links, Safe Attachments, and advanced anti-phishing/anti-spam policies.	(2 days)
Phase4	DLP & Compliance	Apply Microsoft Purview DLP rules, retention policies, and sensitivity labels with encryption (3 days). Phase 5: Security Training Rollout – Launch Microsoft 365–integrated awareness program, including MFA/security-key video training and phishing simulations (begins during week two and continues on an ongoing basis).	(5 days)

Supporting documents and checklist

Document	Scope	Link
Deployment Sheet	Guide and check-list (Implantation guide)	Xxxx
Security Key Guide	Instructions for issuing, registering, and recovering hardware or app-based MFA/security keys for Microsoft 365 and Entra ID accounts.	Xxxx
IAM mgmt runbook	Daily/weekly operations guide for Azure AD (Entra ID): account provisioning, access reviews, privileged role management, and password reset procedures.	Xxxx
security training	User-facing training package and quick-reference handouts for phishing simulations, safe email practices, and acceptable use policy.	Xxxx
O365 mailgateway guide	Configuration and maintenance manual for Microsoft 365 Defender / Exchange Online Protection (EOP), including spam filtering, DKIM/DMARC, and mail-flow rules.	Xxxx

Total estimated initial project duration: ~2 weeks, with ongoing training thereafter unless handed off to the firms internal IT team.

Deliverables and Benefits

Deliverables

Deliverable	Summary
MFA	Fully enforced multi-factor authentication (MFA) and Conditional Access policies across all Microsoft 365 accounts.
Email GW	Hardened email protection with Microsoft Defender for Office 365, including Safe Links, Safe Attachments, and anti-impersonation safeguards.
DLP	Implemented Microsoft Purview Data Loss Prevention (DLP), sensitivity labels, and retention policies to meet legal and regulatory requirements.

Training	Completed initial user security awareness training, including video-based MFA and security key setup guidance, with handoff instructions for ongoing internal IT management.

Benefits

Benefit	Solution	Problem
IAM/IDP	Strong identity protection and granular access control to prevent unauthorized account use.	Uncontrolled account access, credential reuse, and unauthorized logins create security gaps and compliance risk.
Advanced Email Security	Enhanced defense against phishing, malware, and impersonation attempts through advanced email security.	Phishing emails and business email compromise (BEC) attempts can lead to account takeover, ransomware, and data breaches.
Data Loss Prevention (DLP)	Safeguarded client data with automated DLP enforcement, encryption, and compliant retention policies.	Accidental or malicious data leaks, unencrypted transmissions, and non-compliant retention of regulated data.
Security Awareness Training	Continuous user education and reduced human risk factor through ongoing security awareness and phishing simulations.	Human error and lack of awareness increase susceptibility to phishing, social engineering, and policy violations.

Assumptions & Exclusions

Requires **Microsoft 365 Business Premium** (or equivalent) licensing for all users.

Any third-party security tools, custom line-of-business application changes, or non-Microsoft integrations are outside the scope of this project.

Ongoing Azure consumption charges (for Defender, Purview, or Sentinel log retention beyond included quotas) are billed directly to the client's Azure subscription.

Licensing & Subscriptions

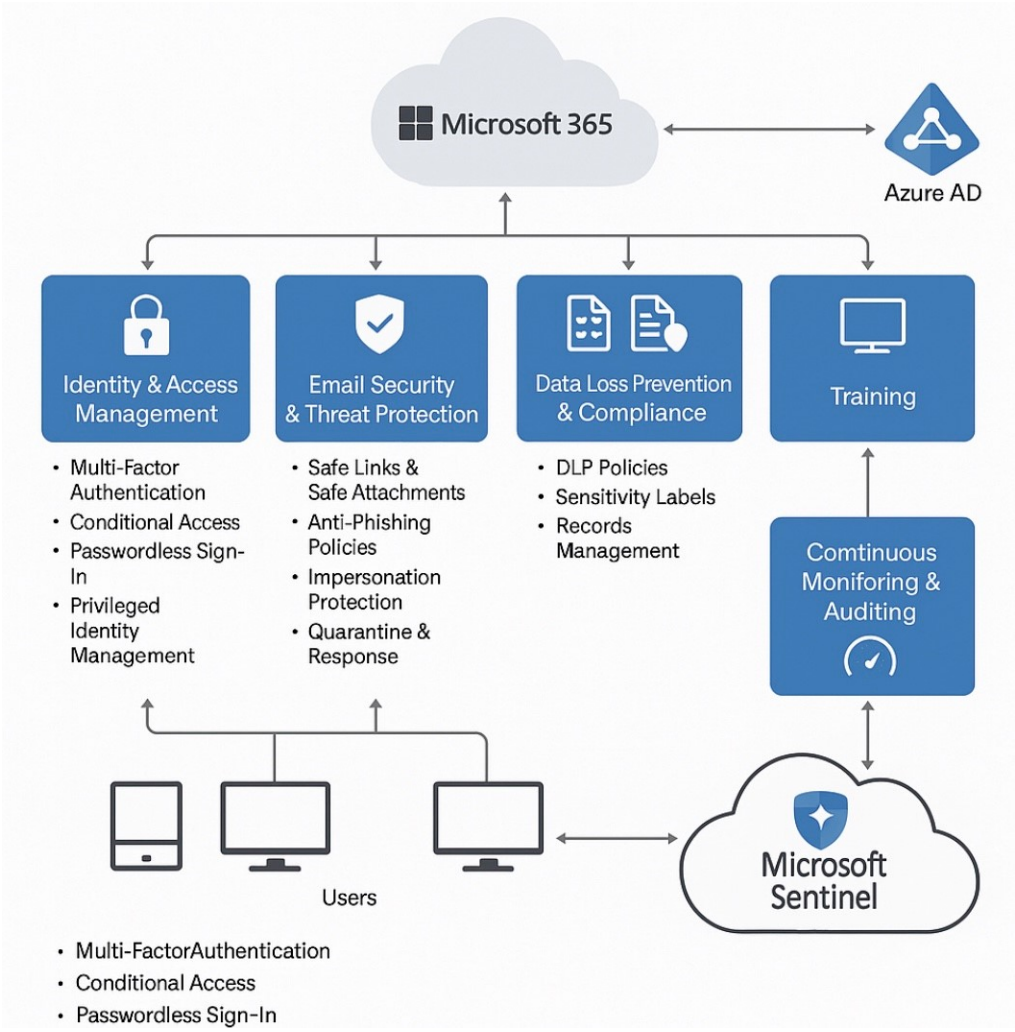
License / Subscription	Notes	Fees & Release Notes
Microsoft 365 Business Premium (In Place)	Base productivity suite providing core security and management features.	Includes Azure AD P1, Intune, and Defender Plan 1 for MFA, conditional access, and baseline email security.
Microsoft Entra ID (Azure AD) Premium P2 (Optional)	Advanced identity and access management.	Adds risk-based conditional access, Identity Protection, and Privileged Identity Management. Without it: no just-in-time admin rights or automated risk-based signin protection.
Microsoft Defender for Office 365 Plan 2 (Optional)	Enhanced email and collaboration security.	Provides Safe Links, Safe Attachments, and automated investigation/response. Without it: email security remains at basic Plan 1 level.
Microsoft Purview (Optional)	Advanced data governance and compliance.	Enables automatic sensitivity labeling, advanced e-discovery, and records management beyond Business Premium. Without it: only manual labeling and basic retention.
Microsoft Sentinel (Optional)	Cloud-native SIEM and SOAR for centralized logs incident response.	Usage-based pricing. Without it: security events remain in native logs with no unified dashboard or automated response.
Microsoft Intune (Included)	Device compliance, patching, and encryption key management.	Included with Business Premium; no additional license required.
Windows BitLocker (Included)	Full-disk encryption for Windows endpoints.	Recovery keys stored in Azure AD; no additional license required.

Decommission and Degassing

Phase	Action	Notes
Review & Confirmation	Verify whether any on-prem servers, network gear, or storage devices will be decommissioned.	Project is primarily Microsoft 365 cloud-based; expect little or no physical decommissioning.

Secure Data Removal (if required)	If any local drives are retired, securely wipe or degauss media and document the process.	Use industry-approved wipe/ degassing methods; capture certificates of destruction.
Hardware Disposal (if required)	Recycle or dispose of retired equipment responsibly.	Follow local e-waste rules and provide disposal certificates.

Solutions Diagram



Out Of Pocket / Invoice

Client will be invoiced all costs associated with out-of-pocket expenses (including, without limitation, costs and expenses associated with patching, cables termination, local transportation and any other applicable business expenses) listed on the invoice as a separate line item. Reimbursement for out-of-pocket expenses in connection with performance of this SOW, when authorized and up to the limits set forth in this SOW, shall be in accordance with client's thencurrent published policies governing travel and associated business expenses.

Completion criteria

Contractor shall have fulfilled its obligations when any one of the following first occurs: Contractor accomplishes the contractor activities described within this SOW, including delivery to client of the materials listed in the section entitled "deliverable materials," and client accepts such activities and materials without unreasonable objections. No response from client within 2business days of deliverables being delivered by contractor is deemed acceptance. Contractor and/or client has the right to cancel services or deliverables not yet provided with 20 business days advance written notice to the other party.

Project change control procedure

A project change request (PCR) will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change, and the effect of the change.
The designated project manager of the requesting party (contractor or client) will review the proposed change and determine whether to submit the request to the other party.
Both project managers will review the proposed change and approve it for further investigation or reject it. contractor and client will mutually agree upon any charges for such investigation, if any. If the investigation is authorized, the client project managers will sign the PCR, which will constitute approval for the investigation charges. Contractor will invoice client for any such charges. The investigation will determine the effect that the implementation of the PCR will have on SOW price, schedule and other terms and conditions of the agreement.
Upon completion of the investigation, both parties will review the impact of the proposed change and, if mutually agreed, a change authorization will be executed. A written change authorization and/or PCR must be signed by both parties to authorize implementation of the investigated changes.

Sign Off

STERLING LG	DKB
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____