



Redwood Consulting

SOW xx005 for
agreement to
perform consulting
services to
Oakwood

DATE	SERVICES PERFORMED BY:	SERVICES PERFORMED FOR:
Sept 19th 2025	DKB Innovate 321 Sycamore Ave. Frisco, TX 76543	Redwood Consulting 123 South Street Manhattan, NY 54321

Index

- Engagement Resources
- Executive Summary
- Current Environment
- Project Goals & Scope
- Proposed Solution
 - PS.1 Server Platform
 - PS.2 Network Modernization
 - PS.3 Backup & Disaster Recovery
 - PS.4 Management & Security
- Implementation Plan
- Deliverables and Benefits
- Assumptions & Exclusions
- Licensing & Subscriptions
- Decommission and Degassing
- Solutions Diagram
- Out Of Pocket / Invoice
- Completion criteria
- Project change control procedure
- Sign Off

Engagement Resources

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





Executive Summary

Redwood Consulting is opening a new 5,000 sq. ft. branch office and requires a complete IT infrastructure design and quote. As a cloudnative and wireless-first company, Redwood seeks a modern, reliable, and secure environment that can be centrally managed and integrated with their Microsoft 365 and Azure AD ecosystem. This proposal provides a full design for networking, conference room technology, secure device management, and guest Wi-Fi.

Current Environment

Greenfield project	no existing IT hardware or cabling.
Microsoft 365 and Azure AD	all new users will have M365 accounts.
Circuit ordered	A 1 Gbps symmetric fiber internet circuit has been ordered.

Project Goals & Scope

- Design a complete networking solution (firewall, switching, Wi-Fi).
- Specify hardware for two conference rooms including TV and video conferencing.
- Provide a solution for secure device management of new laptops.
- Ensure secure guest Wi-Fi access that is isolated from the corporate network.
- Utilize cloud-managed infrastructure wherever possible.

Proposed Solution





PS.1 Network Infrastructure

- Firewall / Security Appliance: Fortinet FortiGate 70G (G-series) next-generation firewall, managed via FortiCloud/FortiManager, with site-to-site VPN, intrusion prevention (IPS), and full FortiGuard threat protection.
- Switching: Fortinet FortiSwitch 148F-FPOE (48 × 1 GbE PoE+ ports, 4 × 10 Gb SFP+ uplinks, ~740 W PoE budget) for cloudmanaged access switching and AP/VoIP power. (FS-124F-FPOE may be used for smaller port counts.)
- Wireless: Four Fortinet FortiAP 431G Wi-Fi 6E indoor access points, centrally managed by FortiGate / FortiLAN Cloud; powered via 802.3bt PoE for high throughput and reliable coverage.
- DHCP & Routing: The FortiGate provides DHCP and inter-VLAN routing for all on-site networks; Azure Virtual Network handles addressing for cloud-hosted workloads.
- VLAN Segmentation & Guest Wi-Fi: Create dedicated VLANs for Guest, Printers/Scanners, IoT/OT devices, and Security Cameras/ NVR, with inter-VLAN traffic restricted by FortiGate policies (guest-to-corporate isolation by default). Bonjour/mDNS gateways can be selectively enabled (e.g., for AirPrint).
- Cabling: Use shielded Cat6a cabling to all AP locations and switch uplinks to ensure reliability, PoE performance, and headroom for future upgrades.

Network Deliverables

Device	Make/Model	QTY	Spec Sheet
--------	------------	-----	------------



*Statement Of Work*

Fortinet FortiGate 70G Firewall	Next-generation firewall with full FortiGuard threat protection, VPN, DHCP, and interVLAN routing, managed via FortiCloud/ FortiManager.	1	FW Specs
Fortinet FortiSwitch 148F-FPOE	48 × 1 GbE PoE+ ports and 4 × 10 Gb SFP+ uplinks for high-performance LAN switching and PoE delivery to APs and VoIP devices.	1	Switch Specs
Fortinet FortiAP 431G Wi-Fi 6E Access Points	Four tri-radio APs providing robust wireless coverage with 802.3bt PoE++, supporting ~300–360 active clients comfortably.	2	AP Specs
VLAN Segmentation & Guest Wi-Fi	Isolated VLANs for Corporate, Guest, Printers/Scanners, IoT/Building Systems, and Security Cameras/NVR, enforced by FortiGate firewall policies.	X	X
Shielded Cat6a Cabling	High-performance cabling for AP locations and switch uplinks to ensure reliable PoE and future upgrade capacity.	1	Cable Specs
FortiCloud / FortiManager Integration	Centralized cloud management for configuration, firmware updates, monitoring, and ongoing policy enforcement.	1	X
Network Diagram & Configuration Exports	Final as-built network diagram, VLAN/IP schema, and FortiGate configuration exports for documentation and future reference.	1	X

PS.2 Conference Room Technology

- Displays: Two commercial-grade 75" 4K UHD LED displays with 120Hz refresh for crisp motion, smooth video, and full screen sharing clarity.
- Video Conferencing Tier: Microsoft Teams Rooms Kits
- Table/Room Microphone Solution
- Wiring & Connectivity: All display & AV wiring done with shielded Cat6a or better, hidden or ceiling/wall-raceway mounting. Power and AV connectivity cleanly routed. Display & AV kit connects to the network via PoE or power over dedicated AV outlets.

Conference Room Deliverables

Device	Make/Model	QTY	Notes
Commercial-Grade Displays	Two 75" 4K UHD LED displays (or optional 65") with 120 Hz refresh for crisp motion, smooth video, and full screen sharing clarity.	2	Display Specs



*Statement Of Work*

Microsoft Teams Rooms Kits	Certified Teams Rooms systems with 4K auto-framing cameras and far-field beamforming microphones/ mic array for native Teams experience.	2	Room Kit Specs
Compute Engine & Touch Controller	Integrated compute appliance to run Teams Rooms for Windows and touch-panel controller for in-room meeting management.	2	Room Kit Specs
Table/Room Microphone Solution	Room-covering array or table microphones with noise suppression and echo cancellation for clear audio pickup of seated and standing participants.	2	Room Kit Specs
Wiring & Connectivity	Shielded Cat6a cabling and concealed AV wiring for displays and conferencing equipment, including PoE or dedicated AV power connections.	1	Cable Specs
Device	Make/Model	QTY	Notes
Quality of Service (QoS) Validation	Network-level prioritization tested to ensure high-quality video conferencing and VoIP performance over the FortiSwitch network.	1	QoS Specs

PS.3 Secure Device Management

- Microsoft Intune Endpoint Management: Enroll all Windows and macOS laptops in Microsoft Intune for centralized, cloud-based provisioning, configuration, and remote wipe. Integrate Intune with Azure AD (Entra ID) to enforce user- and group-based policies.
- Mandatory Device Compliance: Enforce encryption (BitLocker for Windows, FileVault for macOS), automatic OS and security updates, secure boot, and device health checks. Non-compliant devices are automatically blocked from FortiGate-protected networks and Azure resources through Conditional Access.
- Zero-Touch Deployment: Use Windows Autopilot and macOS Automated Device Enrollment to deliver a true plug-and-play setup—new devices ship directly to employees and configure themselves securely on first sign-in.





- Integrated Network Access Control: Coordinate Intune compliance data with FortiGate NAC policies, ensuring that only registered, compliant devices can connect to wired or wireless VLANs.

PS.4 Cloud-Managed Operations

- Unified Fortinet Management: All network components—the FortiGate 70G firewall, FortiSwitch 148F-FPOE, and four FortiAP 431G Wi-Fi 6E access points—are managed through FortiCloud and optionally FortiManager, providing a single console for configuration, firmware updates, and ongoing policy enforcement.
- Identity Integration: Integration with Microsoft 365 / Entra ID enables identity-based access control, allowing user or group policies to follow employees across wired, wireless, and VPN connections.
- Real-Time Analytics & Reporting: FortiGate's FortiView dashboards and FortiAnalyzer/ FortiCloud logs deliver real-time and historical visibility into bandwidth usage, application activity, and security events, with automated alerting and audit-ready reporting.
- Simplified Operations: Cloud-based management supports zero-touch provisioning, remote troubleshooting, and rapid deployment of security updates without on-site visits.

Implementation Plan

Man-Hours

Phase	Implementation	Details	Time-Frame
Phase1	Design & Procurement	Finalize floor plan, structured cabling routes, and AP mounting locations. Produce a full network diagram showing VLANs for corporate, guest, IoT/printers, and security cameras. Confirm Fortinet hardware sizing and order all equipment (FortiGate 70G firewall, FortiSwitch 148F-FPOE, and four FortiAP 431G Wi-Fi 6E APs). Validate Microsoft 365 tenant and Azure AD (Entra ID) readiness for Intune enrollment and identity-based access control.	2 Week



*Statement Of Work*

Phase2	Core Infrastructure Installation	Install shielded Cat6a cabling and racks, label all drops. Rack, power, and connect FortiGate firewall, FortiSwitch, and FortiAPs. Configure FortiGate WAN, VPN to corporate Azure environment (if applicable), DHCP, and inter-VLAN routing. Create and test VLANs for Corporate, Guest, IoT/Printers, and Security Cameras, applying FortiGate firewall policies for isolation.	2 Week
Phase	Implementation	Details	Time-Frame
Phase3	Cloud Integration & Device Management	Integrate FortiGate with FortiCloud/ FortiManager for single-pane cloud management. Connect FortiGate and FortiSwitch to Microsoft Entra ID for identity-based access policies. Deploy Microsoft Intune for zero-touch provisioning of Windows and macOS devices; enforce BitLocker/FileVault, OS patching, and compliance checks tied to Conditional Access. Set up Windows Autopilot to streamline new device enrollment.	2 Week
Phase4	Conference Room & Endpoint Deployment	Install conference-room AV gear (displays, cameras, conferencing endpoints). Enroll and configure all laptops and shared workstations via Intune/Autopilot. Validate video conferencing and VoIP network priority (QoS) over FortiSwitch.	1 Week



*Statement Of Work*

Phase5	Testing, Tuning & Handover	Conduct full end-to-end testing of wireless roaming, VLAN isolation, VPN, and conditional access. Provide focused support for any sign-on or device compliance issues. Deliver final as-built documentation: network diagrams, FortiGate configuration exports, Intune/Autopilot policies, and security baselines. Train internal IT staff on FortiCloud management, Azure AD/Intune integration, and ongoing maintenance.	2 Week
---------------	----------------------------	---	--------

Supporting documents and checklist

Document	Scope	Link
Network Deployment Checklist & Runbook	Step-by-step guide for installing and configuring the FortiGate 70G firewall, FortiSwitch 148F-FPOE, and four FortiAP 431G access points, including VLAN creation, DHCP setup, and VPN configuration.	Xxxx
Document	Scope	Link
As-Built Network & VLAN Diagram	Final, labeled diagram showing cabling, switch ports, VLANs (Corporate, Guest, IoT/Printers, Security Cameras), firewall zones, and VPN connections to Azure.	Xxxx
FortiCloud / FortiManager Configuration Guide	Detailed instructions and exported configs for cloudbased management, monitoring, and future firmware updates.	Xxxx
Microsoft 365 / Entra ID Integration Guide	Documentation of Conditional Access, Azure AD join/hybrid join settings, and how FortiGate integrates with Microsoft identity services.	Xxxx
Device Management & Intune Policy Pack	Complete Intune configuration profiles for BitLocker/FileVault, compliance policies, and Windows Autopilot enrollment.	Xxxx
Conference Room AV Deployment Sheet	Connection diagrams and configuration notes for TVs, cameras, and conferencing equipment.	Xxxx
User & IT Training Materials	Quick-reference guides for employees (connecting to WiFi, VPN, guest network) and for IT staff (FortiCloud/Intune daily operations, password resets, patching).	Xxxx
Post-Deployment Support & Troubleshooting Log	Phase-5 record of any issues found and resolutions for future reference.	Xxxx
SSO Deployment Checklist & Runbook	Step-by-step guide covering Azure AD setup, SAML/OAuth configuration for each SaaS app, and verification steps for cutover.	Xxxx



*Statement Of Work*

Identity Architecture & Access Diagram	Visual diagram showing Azure AD, application connections, Conditional Access flows, and MFA enforcement.	<u>Xxxx</u>
Provisioning & De-Provisioning Guide	Explains SCIM auto-provisioning, group-based assignments, and offboarding steps for IT staff.	<u>Xxxx</u>
User Training & Quick-Reference Guides (SSO)	Employee-facing instructions for signing in via Azure AD SSO, setting up MFA/security keys, and accessing the My Apps portal.	<u>Xxxx</u>
Security & Compliance Documentation	Details on Conditional Access, RBAC, auditing schedules, and integration with Microsoft Sentinel for ongoing monitoring.	<u>Xxxx</u>
Post-Deployment Support & Troubleshooting Log (SSO)	Checklist and issue tracker for Phase 5, recording resolutions to any individual sign-on issues.	<u>Xxxx</u>

Total estimated project duration: ~9 weeks.

Deliverables and Benefits

Deliverables

Deliverable	Summary
Fortinet Stack	Fully deployed Fortinet network including FortiGate 70G next-generation firewall, FortiSwitch 148F-FPOE PoE+ managed switch, and four FortiAP 431G Wi-Fi 6E access points, centrally managed in FortiCloud/FortiManager.
VLAN Architecture	Configured VLANs for Corporate, Guest, Printers/Scanners, IoT/Building Systems, and Security Cameras/NVR with inter-VLAN isolation policies enforced by FortiGate.
Conference Room AV	Two fully equipped conference rooms with mounted 75" 4K UHD displays, Microsoft Teams Rooms video conferencing kits, microphones, compute engine, and full cabling.
Secure Device Management	Microsoft Intune and Windows Autopilot integrated with Azure AD (Entra ID) for zero-touch provisioning, BitLocker/FileVault enforcement, patch management, and conditional access.
End-to-End Documents	Complete documentation set including as-built network and cabling diagram, FortiGate configuration exports, VLAN/IP schema, Intune policy pack, conference room wiring diagrams, and post-deployment troubleshooting log.
Staff Training & Handover	Formal training and handover package covering FortiCloud/FortiManager operations, Azure AD/Intune administration, and guest Wi-Fi procedures.
Centralized Management	Integrated management via FortiCloud/FortiManager and Microsoft Intune for unified monitoring, configuration, and remote troubleshooting.
Secure Wi-Fi	Dedicated and isolated guest Wi-Fi network with FortiGate-enforced firewall rules to separate guest and corporate resources.



*Statement Of Work*

Backup & DR	Implementation of Azure Backup/Site Recovery options and documented recovery procedures for business continuity.
Diagram & Runbooks	Comprehensive solutions diagram and deployment runbooks for ongoing operations and rapid issue resolution.

Benefits

Benefit	Solution	Problem
Modern, Secure Infrastructure	Deploy Fortinet FortiGate firewall, FortiSwitch, and FortiAP Wi-Fi 6E to provide strong perimeter security, real-time threat prevention, and segmented internal traffic.	Legacy network infrastructure lacks advanced threat protection, leaving the environment vulnerable to attacks and internal traffic segmentation issues.
Centralized Cloud Management	Manage all network components and devices via FortiCloud/ FortiManager and Microsoft Intune for unified monitoring, policy changes, and rapid remote troubleshooting.	Disparate management systems lead to slow incident response, inconsistent configurations, and higher operational overhead.
Frictionless Onboarding & Offboarding	Use Microsoft Intune and Windows Autopilot for zero-touch laptop deployment and automatic provisioning/de-provisioning of accounts and access.	Manual device setup and user account management cause delays, higher IT workload, and increased risk of forgotten or orphaned accounts.
Isolated & Compliant Guest Access	Implement dedicated VLANs and FortiGate firewall rules to separate guest and IoT traffic from corporate resources.	Guest and IoT devices on the same network as corporate systems create compliance concerns and potential security breaches.
FutureReady & Scalable	Install shielded Cat6a cabling, high PoE+ capacity, and modular design to support higher-density Wi-Fi, IoT devices, and future technology upgrades.	Older cabling and hardware lack capacity for next-generation Wi-Fi, IoT expansion, and evolving network demands, limiting future growth.

Assumptions & Exclusions

- Assumes the 1 Gbps fiber circuit will be live and tested before network installation begins.
- Excludes office furniture, construction, and non-IT electrical work.
- Integrations with third-party SaaS applications beyond Microsoft 365/Entra ID and Intune require separate scoping and approval.



*Statement Of Work*

- Long-term Fortinet subscription renewals (FortiGuard, FortiCare) and Microsoft cloud service consumption are billed directly to the client's accounts.

Licensing & Subscriptions

License / Subscription	Notes	Fees & Release Notes
Fortinet FortiGate 70G – FortiGuard Security & FortiCare Support (1 year or multiyear)	Required (New)	Enables intrusion prevention (IPS), antivirus/ anti-malware, web filtering, VPN, and provides firmware updates, 24/7 support, and hardware replacement.
Fortinet FortiSwitch 148F-FPOE – FortiCare Support License	Required (New)	Covers firmware upgrades, remote support, and hardware replacement for the access switch.
Fortinet FortiAP 431G – FortiCloud Management & FortiCare Support (4 units)	Required (New)	Delivers cloud-based configuration and monitoring, security updates, and hardware replacement.
FortiCloud / FortiManager Cloud Subscription	Required (New)	Centralized cloud management, analytics (FortiView/FortiAnalyzer), and automated configuration backups for FortiGate, FortiSwitch, and FortiAP devices.
Microsoft 365 Business Premium	Required (Existing or New for new employees)	Provides Microsoft 365 apps, email/ Exchange Online, Azure AD Premium P1, and Intune Endpoint Manager for device provisioning and policy enforcement.
Microsoft Intune (Endpoint Manager)	Included with Microsoft 365 Business Premium	Cloud-based device compliance, OS patching, and remote wipe.
Windows Autopilot	Included with Microsoft 365 Business Premium	Zero-touch deployment and automated enrollment of Windows endpoints.
Windows BitLocker / macOS FileVault	Included with operating systems	Full-disk encryption for all laptops, with recovery keys stored in Azure AD.
Azure AD Premium P2	Optional / Recommended	Adds Privileged Identity Management (PIM), risk-based Conditional Access, and automated access reviews for stronger governance.



*Statement Of Work*

Microsoft Sentinel	Optional / Usagebased	Cloud-native SIEM/SOAR for advanced log analytics, security correlation, and automated incident response.
Video Conferencing Platform Licenses (e.g., Microsoft Teams Rooms or Zoom Room licenses)	Required (New or Existing)	Enables multi-participant video conferencing in the two branch-office conference rooms.

Decommission and Degassing

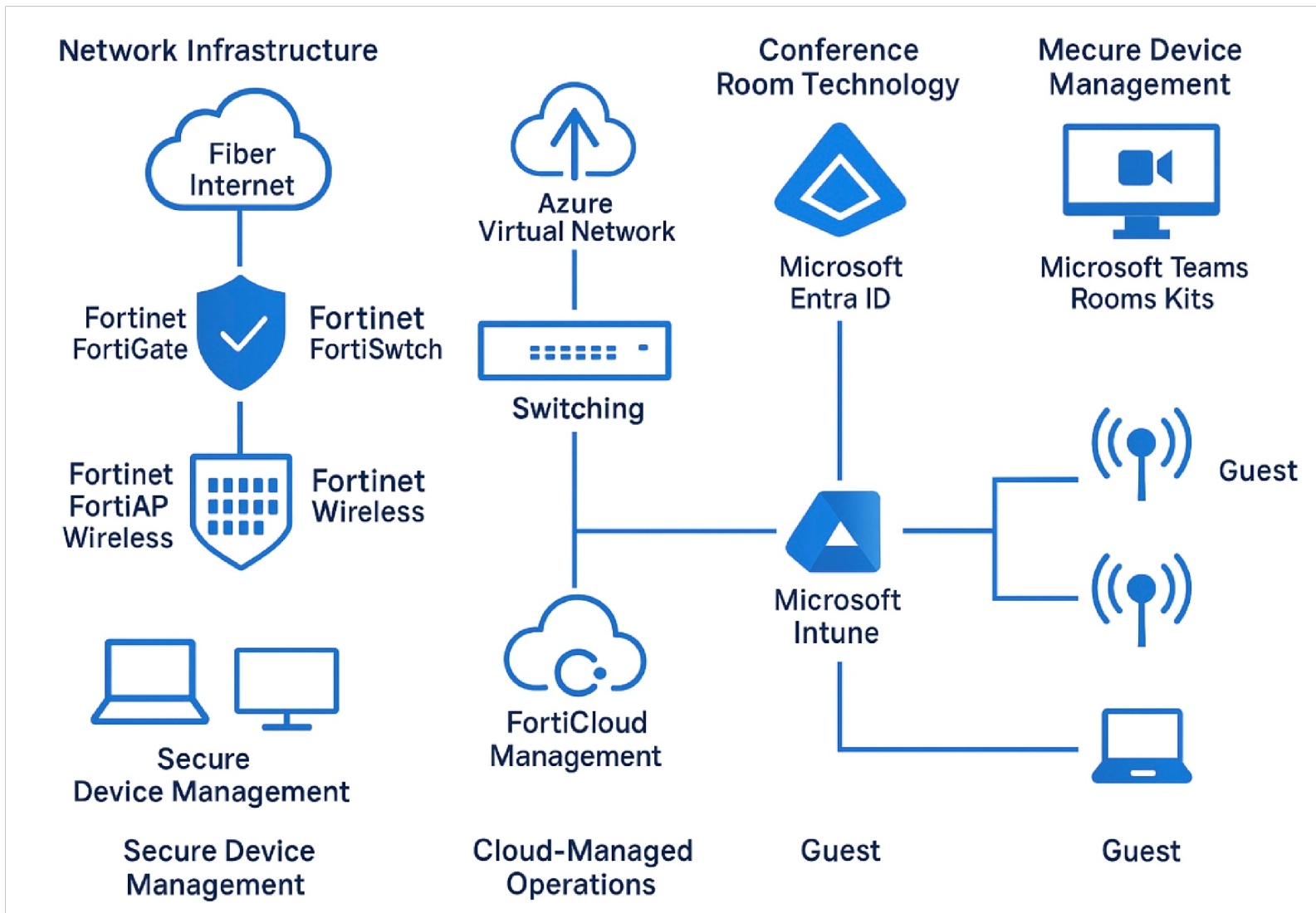
Phase	Action	Notes
Assessment & Inventory	Identify all temporary or construction-phase network connections, test gear, and placeholder configurations used during the build-out.	Confirm no production dependencies remain before removal; ensure 1 Gbps fiber circuit is fully active and tested.
Data & Configuration Backup	Export and securely store FortiGate configuration files, FortiSwitch settings, and FortiAP profiles. Archive Microsoft Intune and Azure AD policy sets.	Ensures rapid restoration if rollback or site relocation is required.
Legacy/ Temporary Network Removal	Remove any temporary network gear, test firewalls, unmanaged switches, or non-production VLANs used during construction.	Document each removal; confirm guest and corporate VLAN isolation remain intact.
Device Deprovisioning	Decommission unused demo or staging laptops and test accounts from Intune and Azure AD.	Maintain compliance by revoking all access tokens and wiping devices before reuse or disposal.
Credential & Key Sanitization	Rotate or revoke any temporary admin credentials, shared secrets, or certificates used during installation and testing.	Store revocation proof and updated credentials in the approved password vault.
Hardware Disposal or Reuse	Recycle, repurpose, or securely store any test or spare hardware not part of the final production design.	Follow e-waste regulations and provide recycling or storage certificates.
Final Verification & Handover	Run full site acceptance tests: VLAN isolation, VPN performance, conditional access enforcement, and conference room QoS verification.	Collect final sign-offs from Redwood Consulting management and deliver as-built documentation and final configuration exports.





PostDeployment Monitoring	Monitor FortiCloud/FortiManager, Microsoft Intune, and Azure AD logs for 30 days after decommissioning temporary resources.	Quickly remediate any unauthorized connection attempts or latent configuration conflicts.
---------------------------	---	---

Solutions Diagram





Statement Of Work

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 2 business 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

Summit Marketing

DKB

Name: _____

Name: _____

Signature: _____

Signature: _____

Date: _____

Date: _____

