Dekalb County School District

Managed Services and Secure & Protect
October 2025 - September 2026

Statement of Work

SOW Delivery Date: 7/7/2025

SOW Expiration Date: 9/5/2025

Submitted By: Monica Davis

(P) 404-316-3565

mdavis@blueally.com

Table of Contents

1.0 Introduction

Statement of Work

This Statement of Work (SOW) is effective as of July 7, 2025, between Dekalb County School District (Client) and BlueAlly Technology Solutions, LLC (Service Provider). The parties agree as follows.

Client:	Dekalb County School District
Client Contact:	Jamal Northington
Project Name:	Managed Services
Statement of Work ID:	BA202569752
Statement of Work Investment Summary:	$148,100
Statement of Work Date:	7/7/2025
Statement of Work Expiry Date: (if not executed by all Parties)	9/5/2025
Service Provider Contact:	Monica Davis

2.0 Project Overview

Service Provider currently provides managed services for Client's Azure and Microsoft 365 environments. Client's Azure tenant currently houses the cloud portion of their ADFS environment and their public facing web site. The purpose of this proposal is to outline details for continued managed services and general support.

Service Provider recommends that we provide managed services for Client's Azure environment, M365 tenant, and related systems. In addition, we are offering a generic support contract for those occasions when you need assistance with specific issues that are not covered under a managed services contract.

2.1. Azure Managed Services (including website)

Service Provider is a full life cycle provider, including managed services for Azure based solutions. In addition to the consulting services to configure this solution, Service Provider recommends ongoing monitoring and management to ensure the system is available when needed, even in the dynamic world of technology.

Managed services can be customized to meet the needs of the client. In the case of Client, we recommend end-to-end managed services for your Azure-based systems.

2.2. Azure Tenant/Environment

Service Provider currently provides managed services for Client's Azure Tenant. We recommend continuing these services. Under this service plan, monthly management tasks and deliverables include:

- Validation and remediation of backup solutions
- Server performance monitoring including memory, disk space, and processors
- Event Log review for critical events
- Monthly patch management
- Monthly Reporting to provide a snapshot of the current state of existing systems under Service Provider's control/visibility
- Quarterly Summary of the overall health of the environment under Service Provider's control/visibility

2.3. Identity / SSO Management

Service Provider currently provides managed services for Client's ADFS and other identity/SSO related systems hosted in Azure. We recommend continuing these services. Under this service plan, monthly management tasks and deliverables include:

- ADFS Services:
  - Onboarding New Relying Party Trusts
  - Replacing expired certificates for Third Party Trusts
  - Third Party Trusts configuration updates
  - ADFS infrastructure configuration changes (spinning up additional servers, decommissioning, etc.)
  - Provide Tier III support on an ad hoc basis
- Monitoring:
  - Proactive Infrastructure Monitoring
  - Proactive health monitoring of ADFS environment (Azure AD Connect health monitoring)
  - Performance tuning
  - Log monitoring
  - Monitoring Alerts, Usage Analytics, Performance, Risks
  - Log monitoring
  - Monitoring Relying Party Trusts
- Reporting:
  - ADFS Usage Reports
  - Infrastructure Reporting (patch, backup, critical events)
  - Monthly reporting of managed environment provided to Client in pdf format
- Maintenance:
  - Infrastructure updates/upgrades
  - ADFS server updates/upgrades
  - Backup planning, policy setup and control
  - Health check + Guidelines to improve infrastructure
- Implementation of Enterprise Apps for SSO
- Migration of supported systems from ADFS Federation to Enterprise Apps

2.4. Website

Service Provider recommends continuing the Azure Managed Services to include the Azure App Service and MySQL Database/server upon which the public website runs. Under this service plan, monthly management tasks and deliverables include:

- Monitor and manage the Azure App Service including Scale-up and Scale-out
- Monitor and manage the MySQL Database Server
- Scheduled patching and updating the MySQL Database Server Virtual Machine
- Monitor backups and site availability
- Report on backup anomalies and site availability
- Security and Access adjustments when onboarding / offboarding staff/employees
- Provide Tier III support on an ad hoc basis
- Monitoring website certificates and coordinating renewal and implementation of new certificates
- Implementation of a Development/Staging site for testing changes
- Moving documents outside of the WordPress structure to Azure Storage to allow of greater flexibility and better performance when scaling-up and scaling-out
- Implementing restrictions on documents that can be downloaded/shared from the website
- Implementing Azure Active Directory integration for authentication for "staff" / "faculty" users
- Performing a semi-annual review of security and implementing approved changes to settings/configuration to improve overall security posture

- Performing a semi-annual review of ManageWP backup configuration to ensure that all new sub-sites are captured and backed-up correctly
- Performing a semi-annual security review/sweep of the website

2.5. Secure and Protect (Microsoft 365 Security)

A focus of Service Provider's Microsoft Infrastructure Team is Microsoft Security. Over the past few years, we have developed several security offerings. Our premier offering is a service we refer to as Secure and Protect.

Microsoft Centric Cyber Security Program

Security Hardening Using the Tools licensed as part of Microsoft 365

+ MAD365 for Identity Breach Protection

Microsoft 365 includes a plethora of security features. Depending on your level of licensing, you have access to some or all of these products – many of which may duplicate functionality you are purchasing through other products. We will work with you to determine which of the Microsoft products you wish to run, assist with implementation (or review and tweaking), and identify areas of duplication for potential cost savings by replacing redundant products.

Once we complete the initial deployment, we will begin the cycle of reviewing and updating key workloads to ensure your environment remains secure and that you are taking advantage of the features that are constantly being added to the Microsoft security products.

Finally, we have included our Identity Breach Protection product, MAD365, as part of Secure and Protect. We have included a detailed description of this product later in this document.

Secure and Protect is a tenant security hardening effort by Service Provider to improve the overall security posture of the Microsoft 365 and Azure Tenants. It consists of a three-phase repeating cycle to maximize your security posture now and over time.

The initial review and implementation of the Secure and Protect workloads will take place over approximately six (6) months. During this time, we will implement all security controls to be enforced.

We will lead a quarterly working session to review the progress to-date and review/revise the implementation and review schedule. Following the initial phase, we will review key workloads on an ongoing basis to ensure they are up to date with the latest features/functionality and in keeping with any updated compliance requirements.

The Microsoft 365 Tenant Security monitoring effort will begin upon implementation of the first security workload. As new workloads or functions are incorporated into M365, we will incorporate them into the offering, always keeping your environment maximally protected.

The following workloads are reviewed and hardened as part of this effort. A complete list of actions performed are outlined in Appendix A: Secure and Protect:

- Azure Active Directory
- Microsoft Purview (Compliance) and Security
- Defender for Cloud Apps
- Defender for Endpoints
- Exchange Online
- Intune (Mobile Application Policies for BYOD)
- OneDrive / SharePoint
- Teams

2.6. MAD365

In 2018, Service Provider worked with Microsoft to co-develop an identity breach detection solution. Our Malicious Activity Detector (MAD365) is built on the security systems you have already licensed with Microsoft 365. It consists of a combination of automated log review and human monitoring. By combining the automation and monitoring service, we put barriers in place to prevent and/or identify breaches before harm occurs. Some of the areas covered include:

- Impossible Travel (login from two distant locations)
- Infrequent Country
- Anonymous IP address
- Multiple failed login attempts
- Creation of forwarding/redirect rule
- Suspicious email sending pattern
- Unusual multiple file download
- Unusual file deletion activities
- Unusual administrative activities

While Microsoft security products built into Microsoft 365 provide you with the information you need to identify (potential) breaches, it is highly unlikely that you have the time required to manually review and cross-reference this information. MAD365 continuously analyzes authentication activity. Our dedicated engineers review the output and report only issues or anomalies to you, giving you the information you need to secure your environment without the “noise” of detailed logs.

2.7. Project Scope

Project Initiation

- Schedule and Lead Project Kickoff
- Request and validate system access
- Develop Project Plan/schedule

Security Hardening

- Service Provider will work with Client to review, implement/update, and monitor Microsoft 365 Security Workloads listed in Appendix A. Service Provider will provide the following services:
    - Perform the initial assessment of Microsoft 365 security posture, including a review of the following:
        - Entra ID (formerly Azure Active Directory)
        - Microsoft Purview (Compliance) and Security
        - Defender for Cloud Apps
        - Defender for Endpoints
        - Exchange Online
        - Intune BYOD (Mobile Application Management)
        - OneDrive / SharePoint
        - On-premises integration with Microsoft 365
        - Teams
    - Review the configuration of the environment against a pre-defined checklist (see Appendix A)

        - Provide the output of the report
        - Work with Client to develop a prioritized timeline/plan
    - Implement agreed-upon changes in “working sessions” or through Client’s standard change control process
    - Provide support for the changes immediately following implementation
- MAD365 Remote Monitoring and Reporting
    - Service Provider will provide remote technical telephone support that focuses on the activities associated with breaches and other attacks on an identity within Client’s Office 365 tenant and Azure environments. Telephone services are offered Monday through Friday between the hours of 8:00 AM and 5:00 PM Eastern time. Support hours beyond the basic offering will be provided within future offerings and/or as a separate contract.
    - Service Provider will provide the following services:
        - Respond to Client’s inquiries via telephone or email of potential threats or events
        - Provide recommendations and guidance on security events and violations
    - Follow Client’s escalation process via telephone/email for any violations that are considered High Risk or Critical.
    - Daily Review of the Microsoft Defender for Cloud Apps logs being Imported into MAD 365 Dashboard Services.
        - Service Provider will collect logs daily from Client’s MDCA and ATA/ATP web portals. The logs would be automatically uploaded and imported into their respective MAD365 dashboard hosted by Service Provider.
    - Remote Technical Support when a breach or other high-risk activities occur.
- Ongoing Security Hardening and Monitoring
    - Re-assess periodically for new security features/offerings from Microsoft and work with Client to implement.
        - Work Client priority on the timeline
        - Implement agreed-upon changes in “working sessions” unless Client prefers the changes to be implemented in a different way
        - Provide support for the changes that were made
    - Monitor the Microsoft 365 Tenant for security events to identify gaps
    - Advise on additional controls and configurations from which Client can benefit
    - Re-assess the security configuration periodically for new security offerings and implement
    - Provide support when requested/needed

2.8. Ad Hoc Support (Block of Hours / Office 365 Admin)

In the past we provided this type service under a separate agreement as a retainer. Based on our experience with Client this past year, we believe a Block of Time contract for 100 hours is the best fit for this need.

Client may require technical support outside their managed services contract. Examples include:

- Additional support staff in the event several employees are out of the office simultaneously
- Ad hoc support for systems not covered under a managed services contract
- Consulting Services related to net new solutions

DESCRIPTION OF SERVICES:

- Phone Support for general consulting and answering technical questions.
- Ad hoc problem resolution as requested
- Azure and Office 365 implementation assistance
- SharePoint Online Support
- Microsoft consulting and planning services as requested

Please refer to Appendix B for Block of Time Terms of Service.

3.0 Project Timeline

During the Project Kickoff meeting, the start and end dates will be discussed and finalized. Working sessions will be scheduled in a minimum of one (1)-hour blocks. Project hour estimates assume remote access for Service Provider engineers. The project timeline and hours may be impacted if remote access is not available for Service Provider engineers.

The Period of Performance for the work as described in this SOW is twelve (12) to thirty-six (36) months from the date of Project Kickoff depending on which option is selected in the "Project Pricing and Invoicing" section. The Period of Performance and the level of effort defined in this SOW are based on the information provided by Client at the time of this SOW; changes to that information will result in a Change Order.

4.0 Communication Plan

Communication is key to the success of any engagement; the following communication plan is designed to ensure that all stakeholders are kept informed of progress. The Service Provider team will communicate via e-mail and telephone.

Task	Frequency	From	To	Purpose
Quarterly Business Reviews	Quarterly	Service Provider	Client Representative	Formal presentation of the project status, findings, issues, and recommendations.

5.0 Responsibilities and Assumptions

5.1 Service Provider Responsibilities

- Keep functional requirements in scope as defined.
- Coordinate meetings and schedule interviews with Client stakeholders, keeping Client's point of contact informed and involved to the degree requested.

5.2 Client Responsibilities

- Assign stakeholders to ensure that all required experts in specific process areas are involved in the requirements phase.
- Establish a single point of contact (SPOC) who is authorized to accept work on behalf of Client.
- Provide information about all related systems, processes, and other required documentation.
- Provide system access for Service Provider engineers as required to successfully complete all services covered in the scope of this SOW.
- Client provides remote access for Service Provider engineers to equipment covered in the scope of this SOW.
- Provide a review of documentation and feedback on requested changes and accepted content.
- Participate in working sessions in accordance with the agreed-upon cadence.
- Approve and accept deliverables.

5.3 Assumptions

- To benefit fully from Secure and Protect (i.e., utilize all of the security workloads listed), Client must be licensed for Microsoft 365 at the E5, G5, or A5 level.
- Client provides assistance and guidance in researching questions and issues pertaining to any business or functional requirement.
- Client functional area SMEs and technical personnel are available for necessary meetings and communication and respond in a timely manner to requests to review and approve the documentation.
- If Client stakeholders request additional functionality beyond the scope of this SOW, then Service Provider will issue a Change Order, and upon Client approval, Service Provider will issue a revised schedule and integrate the Change Order into the project.

6.0 Working Hours and Services Criteria

6.1 Designated Place of Work

Service Provider's designated place of work will be remote. Meetings with Client will be held via web conference.

7.0 Change Management Process

In the event unforeseen factors change this services scope of work and/or impact the term and cost of Service Provider provided services, Client and Service Provider may mutually revise the Agreement and Service Provider shall provide Client with an estimate of the impact of such revisions to the fees, payment terms, completion schedule, and other applicable provisions of the Agreement. If the parties mutually agree to such changes, a written description of the agreed-upon change ("Change Order") shall be prepared, incorporating such changes to the Agreement, and shall be signed by both parties. The terms of a Change Order prevail over those of the Agreement.

8.0 ENGAGEMENT TERMS AND CONDITIONS

8.1 Engagement Contacts

	Service Provider Contact	Client Engagement Contact
Contact name	Monica Davis	Jamal Northington
E-mail address	Mdavis@blueally.com	Jamal_Northington@dekalbschoolsga.org
Phone number	404-316-3565	
Mailing address	3475 Piedmont Rd NE # 900, Atlanta, GA 30305	1701 Mountain Industrial Blvd Stone Mountain GA 30083

8.2 Project Pricing and Invoicing

Azure Managed Services Costs:

- This quote is a fixed-price quote. Invoicing will be performed annually at the beginning of the contract period.
- The cost for this service is $57,600 per annum.

M365 Managed Services (Secure & Protect) Costs:

- This quote is a fixed-price quote. Invoicing will be performed annually at the beginning of the contract period.
- The cost for this service is $72,000 per annum.

Support Hours:

We have included 100 hours of ad hoc support at a discounted rate. NOTE: These hours may be utilized for Premium Services tasks or Support associated with Managed Systems Only. Project Tasks will be quoted and invoiced separately. Please refer to Appendix B for additional information.

Description	Hourly Rate	Total
Block of 100 Hours	$185	$18,500

Summary (Oct 1, 2025 – Sept 30, 2026)

Description	Monthly	Annual
Azure Managed Services	$4,800	$57,600
M365 Managed Services (Sec & Pro)	$6,000	$72,000
Block of Time	Prepaid	$18,500
	TOTAL	$148,100

8.3 Termination

The term of this SOW begins on the SOW execution date and ends upon Client's acceptance of engagement. Service Provider will provide a Certificate of Acceptance document or email to Client for signature to acknowledge the completion of the contract in writing. Client will return the signed acceptance document or an email stating acceptance within ten (10) business days of receipt. If Client fails to respond or notify Service Provider of discrepancies, then Service Provider will perceive the non-response as acceptance.

8.4 Microsoft Partner of Record

Client agrees to designate BlueAlly as its Partner of Record with Microsoft for the following:

- ✓ Azure Subscriptions – those used as part of this project
- ✓ Microsoft/Office 365 – those workloads that are part of this project
- ✓ Intune

Disclosure to Client: Microsoft may pay Service Provider incentives for helping to implement and support Azure, Office 365 and EMS. This does not change Client's licensing, support, and pricing agreements with Microsoft.

8.5 Terms and Conditions of Engagement

Client agrees to purchase from Service Provider those services specified in the SOW attached hereto. In addition to the terms and conditions set forth in the SOW, Client agrees that all services provided by Service Provider to Client will be subject to the following terms and conditions:

1. Billing. Payment for services rendered by Service Provider shall be billed and invoiced by Service Provider on a periodic basis. Client agrees to pay all invoiced amounts within thirty (30) days of the date of invoice. All out-of-pocket expenses incurred by Service Provider in the performance of services to Client shall be billed as incurred. Client shall pay all such expenses as promptly as practicable after receipt thereof. All taxes incurred by Client, resulting from the performance by Service Provider of the services specified in the SOW, shall be the responsibility of Client.

2. No Solicitation. During the term of the services provided by Service Provider to Client and for a period of twelve (12) months thereafter, Client shall refrain from soliciting for hire any current or future Service Provider employee, provided that nothing shall prevent Client from general solicitation for hire of employees through public advertisement.

3. Termination. Client may terminate the transactions contemplated by the SOW and this agreement upon the material breach or non-performance by Service Provider of the terms and conditions set forth in the SOW or this agreement, provided that Service Provider fails to cure such breach or non-performance within thirty (30) days of Service Provider's receipt of notice thereof. Service Provider may terminate the transactions contemplated by the SOW and this agreement upon the material breach by Client of the terms and conditions set forth in the SOW or this Agreement, or the failure by Client to pay any amounts due or to become due under the terms hereof or thereof. Client shall remain liable for payment of all fees and expenses incurred by Client up to the date of termination.

4. Limitation of Liability. Client's sole and exclusive remedy for all claims, damages, losses, costs, fees, expenses, or similar items arising from the transactions contemplated by the SOW, including the provision of services by Service Provider, shall be limited to termination by Client of the services set forth in the SOW in accordance with the terms set forth above. In no event shall Service Provider be liable for any incidental, consequential, or punitive damages, including any damages resulting from the loss of data or its use, lost profits, or claims asserted against Client by a third-party. Service Provider DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

5. Access. Client shall afford Service Provider access to such Client technical matter, data, information, operating supplies, and computer system(s), as may be reasonably required by Service Provider to perform the services set forth in the SOW (including, providing Service Provider with a primary point of contact).

6. Service Provider Personnel. Service Provider retains sole discretion to assign such Service Provider personnel as it deems necessary or appropriate to perform the services set forth in the SOW. Service Provider will provide Client with a primary point of contact for inquiries regarding the services.

7. Confidentiality. Any information (whether written or oral) designated as confidential at any time by either party shall be held in strict confidence by the receiving party and may be used by the receiving party only for the purposes set forth in the SOW and the terms of this agreement. Except as required by law, no confidential information, including the terms of this agreement and the SOW, shall be disclosed by either party without the prior written consent of the party designating the information as confidential. Confidential information shall not include any information, that is in or becomes part of the public domain through no fault of the recipient, is already known to the recipient, has been developed independently, or is received from a third party without similar restriction and without breach of this or a similar agreement. Nothing contained in this agreement or the SOW shall prevent Service Provider from publicizing its business relationship with Client or the nature of the services it provided to Client.

8. Interpretation. In the event of a conflict between the terms and provisions of this agreement and the SOW, any purchase order or other document authorizing the work or services covered by this agreement and the SOW, the provisions of this agreement, and the SOW shall govern.

9.0 ACCEPTANCE AND AUTHORIZATION

The terms and conditions of the Statement of Work apply in full to the services and products provided under this Statement of Work.

IN WITNESS WHEREOF, the parties hereto each acting with proper authority have executed this Statement of Work, under seal.

	BlueAlly Technology Solutions, LLC	**Dekalb County School District**
Signature		
Name	Jason Schroeder	
Title	SVP, Services	
Date		

APPENDIX A: SECURE AND PROTECT

The following table details the minimal security workloads covered by Secure and Protect. As Microsoft adds workloads and functionality, the additions will be incorporated.

Overall Tenant Security Checklist:

Tasks / Effort	Platform
Review Azure AD Reporting	Azure AD
Turn on User Risk Policies	Azure AD
Turn on User Sign-in Policies	Azure AD
Restrict user consent to applications	Azure AD
Do not allow users to grant consent to unmanaged/unreliable applications	Azure AD
Restrict logins by IP / Geo-Location	Azure AD
Enable self-service password reset	Azure AD
Enforce MFA for Admins	Azure AD
Set up Azure AD Break Glass Accounts	Azure AD
Implement Privileged Identity Management for Just-in-Time access	Azure AD
Remove dormant accounts from sensitive groups	Azure AD
Use limited administrative roles	Azure AD
Implement Custom Banned Passwords List and Lockout thresholds	Azure AD
Secure Applications Access using Conditional Access Rules	Azure AD
Ensure all users can complete multi-factor authentication for secure access	Azure AD
Configure Named Locations to allow bypass of conditional access policies	Azure AD
Block Legacy Authentication	Azure AD
Do not expire passwords	Azure AD
Enable password hash sync if hybrid	Azure AD
Configure General Anti-Spam Policies	Compliance & Security
Configure Safe Links	Compliance & Security
Configure Safe Attachments Delivery in block mode	Compliance & Security
Configure DLP (Data Loss Prevention) Rules and notifications	Compliance & Security
Configure Retention Policies	Compliance & Security
Configure General Anti-Phishing Policies	Compliance & Security
Configure user/domain impersonation	Compliance & Security
Configure Impersonation Safety Tips	Compliance & Security
Configure General Anti-Malware Policies	Compliance & Security
Create customized DLP policies for personal data	Compliance & Security
Create DLP Policies for Company Sensitive Information	Compliance & Security
Create DLP Policies for Personally Identifiable Information	Compliance & Security
Configure Sensitivity Labels	Compliance & Security
Apply sensitivity labels to protect sensitive or critical data	Compliance & Security
Configure Microsoft Information Protection Scanner for on-premises file classifications	Compliance & Security
Review Security Recommendations for Azure and remediate	Compliance & Security
Ensure that Auto-labeling data classification policies are set up and used	Compliance & Security
Configure supported app connectors	MDCA
Configure Conditional Access App Controls for apps for session control	MDCA
Enable Azure AD Identity Protection Integration	MDCA
Enable Defender for Identities Integration	MDCA
Configure Unsanctioned Apps to block access using Defender for Endpoints	MDCA
Discover Risky and Non-Compliant Shadow IT Applications	MDCA
Detect anomalous behavior	MDCA
Set automated notifications for new and trending cloud applications in Client organization	MDCA
Notify upon Detection of New OAuth Application	MDCA

Tasks / Effort	Platform
Create a Custom Activity Policy to Discover Suspicious Usage Patterns	MDCA
Email Notifications	MDCA
Microsoft Defender for Endpoints Integration	MDCA
User Enrichment Integration with Azure AD	MDCA
Automatically scan new files for sensitivity labels and content inspection warnings	MDCA
Azure Security Monitoring	MDCA
Install Defender for Endpoints on Servers	MDE
Enable Azure AD Identity Protection Integration	MDE
Enable Tamper Protection	MDE
Configure Device Groups	MDE
Web Content Filtering	MDE
Automatically Resolve Alerts	MDE
Configure Auto-remediation levels	MDE
Use MDE to enforce security configuration settings from MEM	MDE
Automated Investigation	MDE
Live Response	MDE
Live Response for Servers	MDE
Enable EDR in block mode	MDE
Allow of block file	MDE
Show user details	MDE
Office 365 Threat Intelligence connection	MDE
Microsoft Defender for Cloud Apps Integration	MDE
Microsoft Intune connection	MDE
Device discovery	MDE
Email Notifications	MDE
Implement Outbound Spam Policy	Exchange Online
Implement DMARC for outbound mail	Exchange Online
Enable Client Rules Forwarding Block	Exchange Online
Set action to take on high-confidence spam detection	Exchange Online
Ensure that no sender domain allowed for an anti-spam policy	Exchange Online
Spam retention in Quarantine (recommended is 30 days)	Exchange Online
Block users who reached the message limit (300 per day)	Exchange Online
Set up a Sender Policy Framework to prevent spoofing	Exchange Online
Implement BIMI with a logo	Exchange Online
Configure Message Records Management Tags and Policies (for archiving)	Exchange Online
Allow Mailbox Delegation Only When Authorized	Exchange Online
Do Not Override FROM Address Enforcement	Exchange Online
Implement connection filter	Exchange Online
Do not allow Exchange Online calendar details to be shared with external users	Exchange Online
Enable Mailbox Intelligence	Exchange Online
Move messages that are detected as impersonated users by mailbox intelligence	Exchange Online
Quarantine messages that are detected from impersonated domains	Exchange Online
Quarantine messages that are detected from impersonated users	Exchange Online
Set action to take on phishing detection	Exchange Online
Set the email bulk complaint level (BCL) threshold to be 6 or lower	Exchange Online
Configure Application Protection Policies for unmanaged devices	Intune
Configure Application Configuration Policies for unmanaged devices	Intune
Review and Configure OneDrive and SharePoint Sharing configuration	OneDrive/SharePoint
Review Security configuration for OneDrive and SharePoint	OneDrive/SharePoint
Block unmanaged devices from running desktop apps	OneDrive/SharePoint
Block Apps that don't use modern authentication	OneDrive/SharePoint
Enable versioning for document libraries	OneDrive/SharePoint
Configure External Sharing Links to Expire	OneDrive/SharePoint

Tasks / Effort	Platform
Sign out inactive users in SharePoint Online	OneDrive/SharePoint
Allow syncing only on computers joined to specific domains	OneDrive/SharePoint
Review the ADFS environment for security	On-premises
Azure AD Password Protection on on-premises domain controller	On-premises
Configure Microsoft Defender for Identities (formerly Azure ATP)	On-premises
Configure secondary Azure AD Connect server in staging	On-premises
Configure which users are allowed to present in Teams meetings	Teams
Require lobbies to be set up for Teams meetings	Teams
Restrict anonymous users from joining meetings	Teams
Limit external participants from having control in a Teams meeting	Teams
Restrict anonymous users from joining Teams meetings	Teams
Restrict dial-in users from bypassing a meeting lobby	Teams
Only invited users should be automatically admitted to Teams meetings	Teams

Defender for Endpoints (client-specific) checklist:

Tasks / Effort	Platform
Turn on Firewall in macOS	MDE
Turn on Microsoft Defender Antivirus PUA protection in block mode on macOS	MDE
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	MDE
Block Win32 API calls from Office macros	MDE
Block execution of potentially obfuscated scripts	MDE
Block Office applications from injecting code into other processes	MDE
Block executable content from email client and webmail	MDE
Block persistence through WMI event subscription	MDE
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	MDE
Block Office applications from creating executable content	MDE
Block Office communication application from creating child processes	MDE
Block Adobe Reader from creating child processes	MDE
Block all Office applications from creating child processes	MDE
Block process creations originating from PSExec and WMI commands	MDE
Block untrusted and unsigned processes that run from USB	MDE
Block JavaScript or VBScript from launching downloaded executable content	MDE
Block abuse of exploited vulnerable signed drivers	MDE
Enable 'Network Protection'	MDE
Set User Account Control (UAC) to automatically deny elevation requests	MDE
Disable Solicited Remote Assistance	MDE
Disable 'Allow Basic authentication' for WinRM Service	MDE
Disable 'Allow Basic authentication' for WinRM Client	MDE
Set LAN Manager authentication level to 'Send NTLMv2 response only. Refuse LM & NTLM'	MDE
Set default behavior for 'AutoRun' to 'Enabled: Do not execute any autorun commands'	MDE
Enable 'Require additional authentication at startup'	MDE
Disable 'Enumerate administrator accounts on elevation'	MDE
Enable 'Local Security Authority (LSA) protection'	MDE
Turn on Microsoft Defender Application Guard managed mode	MDE
Turn on Microsoft Defender Credential Guard	MDE
Enable scanning of removable drives during a full scan	MDE
Disable Anonymous enumeration of shares	MDE
Disable 'Autoplay' for all drives	MDE
Fix unquoted service path for Windows services	MDE
Enable FileVault Disk Encryption in macOS	MDE

Tasks / Effort	Platform
Set account lockout threshold to 5 or lower in macOS	MDE
Secure Home Folders in macOS	MDE
Set minimum password length to 15 or more characters in macOS	MDE
Set 'Account lockout threshold' to 1-10 invalid login attempts	MDE
Disable JavaScript on Adobe DC	MDE
Ensure the screensaver is set to start in 20 minutes or less in macOS	MDE
Set the screen to lock when screensaver starts in macOS	MDE
Set 'Maximum password age' to '90 or fewer days, but not 0' in macOS	MDE
Set 'Enforce password history' to '24 or more password(s)' in macOS	MDE
Disable JavaScript on Adobe Reader DC	MDE
Disable Flash on Adobe Reader DC	MDE
Enable 'Hide Option to Enable or Disable Updates'	MDE
Disable 'Continue running background apps when Google Chrome is closed'	MDE
Block outdated ActiveX controls for Internet Explorer	MDE
Disable running or installing downloaded software with an invalid signature	MDE
Set 'Interactive logon: Machine inactivity limit' to '1-900 seconds'	MDE
Enable Local Admin password management	MDE
Disable 'Installation and configuration of Network Bridge on your DNS domain network'	MDE
Enable 'Microsoft network client: Digitally sign communications (always)'	MDE
Disable the local storage of passwords and credentials	MDE
Disable IP source routing	MDE
Set IPv6 source routing to the highest protection	MDE
Disable 'Autoplay for non-volume devices'	MDE
Set 'Minimum PIN length for startup' to '6 or more characters'	MDE
Enable 'Apply UAC restrictions to local accounts on network logons'	MDE
Prohibit the use of Internet Connection Sharing on DNS domain network	MDE
Set 'Minimum password age' to '1 or more day(s)'	MDE
Set 'Enforce password history' to '24 or more password(s)'	MDE
Set 'Minimum password length' to '14 or more characters'	MDE
Disable 'Password Manager'	MDE
Set user authentication for remote connections by using Network Level Authentication to 'Enabled'	MDE
Disable merging of local Microsoft Defender Firewall connection rules with group policy firewall rules for the Public profile	MDE
Disable merging of local Microsoft Defender Firewall rules with group policy firewall rules for the Public profile	MDE
Enable Automatic Updates	MDE
Enable Gatekeeper in macOS	MDE
Secure Microsoft Defender firewall private profile	MDE
Secure Microsoft Defender Firewall domain profile	MDE
Secure Microsoft Defender Firewall public profile	MDE
Fix Microsoft Defender for Endpoint sensor data collection in macOS	MDE
Enable 'Block third party cookies'	MDE
Enable 'Require domain users to elevate when setting a network's location'	MDE
Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile	MDE
Disable Microsoft Defender Firewall notifications when programs are blocked for Private profile	MDE
Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile	MDE
Encrypt all BitLocker-supported drives	MDE
Update Microsoft Defender for Endpoint core components	MDE
Fix Microsoft Defender for Endpoint impaired communications in macOS	MDE
Fix Microsoft Defender for Endpoint impaired communications	MDE
Fix Microsoft Defender for Endpoint sensor data collection	MDE

Tasks / Effort	Platform
Update Microsoft Defender Antivirus definitions in macOS	MDE
Turn on Microsoft Defender for Endpoint sensor	MDE
Enable EDR in block mode	MDE
Change service account to avoid cached password in Windows registry	MDE
Change service executable path to a common protected location	MDE
Disable SMBv1 client driver	MDE
Turn on Tamper Protection	MDE
Use advanced protection against ransomware	MDE
Disable 'Configure Offer Remote Assistance'	MDE
Set controlled folder access to enabled or audit mode	MDE
Set 'Maximum password age' to '60 or fewer days, but not 0'	MDE
Update Microsoft Defender Antivirus definitions	MDE
Turn on real-time protection	MDE
Turn on PUA protection in block mode	MDE
Ensure BitLocker drive compatibility	MDE
Fix Windows Defender Antivirus cloud service connectivity	MDE
Turn on Microsoft Defender Antivirus	MDE
Resume BitLocker protection on all drives	MDE
Enable Microsoft Defender Antivirus real-time behavior monitoring	MDE
Enable Microsoft Defender Antivirus scanning of downloaded files and attachments	MDE
Turn on Microsoft Defender Antivirus real-time protection in macOS	MDE
Turn on Microsoft Defender Firewall	MDE
Enable Microsoft Defender Antivirus email scanning	MDE
Set Microsoft Defender SmartScreen Microsoft Edge site and download checking to block or warn	MDE
Set Microsoft Defender SmartScreen app and file checking to block or warn	MDE
Disable 'Store LAN Manager hash value on next password change'	MDE
Disable SMBv1 server	MDE
Enable Microsoft Defender Antivirus cloud-delivered protection in macOS	MDE
Disable the built-in Guest account	MDE
Disable 'Insecure guest logons' in SMB	MDE
Enable 'Safe DLL Search Mode'	MDE
Turn on all system-level Exploit protection settings	MDE
Enable cloud-delivered protection	MDE
Disable the built-in Administrator account	MDE
Set 'Remote Desktop security level' to 'TLS'	MDE
Disable 'Anonymous enumeration of SAM accounts'	MDE
Restrict anonymous access to named pipes and Shares	MDE
Disable 'Always install with elevated privileges'	MDE
Enable System Integrity Protection (SIP) in macOS	MDE
Set 'Reset account lockout counter after' to 15 minutes or more	MDE
Set 'Account lockout duration' to 15 minutes or more	MDE
Disable sending unencrypted passwords to third-party SMB servers	MDE
Enable Explorer Data Execution Prevention (DEP)	MDE
Block Flash activation in Office documents	MDE
Enable 'Limit local account use of blank passwords to console logon only'	MDE
Disable 'WDigest Authentication'	MDE
Enable 'Domain member: Digitally sign secure channel data (when possible)'	MDE
Enable Set 'Domain member: Digitally encrypt secure channel data (when possible)'	MDE
Enable 'Domain member: Digitally encrypt or sign secure channel data (always)'	MDE
Enable 'Domain member: Require strong (Windows 2000 or later) session key'	MDE
Disable 'Network access: Let Everyone permissions apply to anonymous users'	MDE
Disable 'Domain member: Disable machine account password changes'	MDE

Appendix B: Block of Time Terms of Service

Lifecycle of Consulting Hours

All prepaid hours are available for one year from the date of purchase. All remaining unused hours will expire on the anniversary of the purchase date with no available refund to the Client.

Utilization Reporting

Client will be given a detailed monthly invoice of the hours that were consumed during a particular period of time. When reporting on a prepaid pool of hours engagement, the invoice will show the total value of the block that has been purchased, the number of hours that have been used in that period of time, and the funds remaining.

Prepaid Hours Overage

In the case that the Client exceeds the available hours in their prepaid pool, the Client will be given the opportunity to reload their prepaid pool and have the deficit of hours taken out of the reload. In the case that the Client does not choose to reload hours, all overages will be billed at Service Provider's standard hourly rate of $220.00 per hour.

Business Hours Usage

All work performed for the client under this Agreement will occur at a 1:1 ratio for billable hour to actual hours worked. Business hours are defined as 8:00AM to 5:30PM EST, Monday through Friday. Yearly observed holiday schedule shall be provided to Client upon request.

After Hours Usage

Requests that are performed on an emergency basis that occur after normal hours of business (8:00AM to 5:30PM EST, Monday through Friday) are consumed at an hourly rate of 1.5:1 against the existing prepaid pool of hours. This rate does not apply to sufficiently scheduled maintenance windows agreed upon by both Client and Service Provider.

Support Requests

All Client support requests must be issued by sending an email to support@blueally.com.

Location

The location of services to be provided is: remote access

Travel and Material Expenses

In the event the need for travel arises, Client will remain responsible for all expenses related to travel where necessary and all materials required for services. Out-of-pocket expenses are billed at actual. Automobile mileage is billed at the then-current IRS allowable rate. The Service Provider travel expense policy is available upon request.

In order to minimize costs, Service Provider strives to minimize airfare and other travel-related costs by booking travel at least 7 days prior to the scheduled project start date. When projects are rescheduled without seven days advance notice, non-refundable charges will be added to the total out-of-pocket charges.

Assumptions

- Service Provider will provide knowledge transfer to the available Client resource(s)
- Prior to the start of the engagement, Client will provide the engineer (s) assigned to the project with Client contacts, instructions, and login credentials.
- Service Provider is not responsible for delays caused by failures, including but not limited to, failures caused by systems, personnel, or environmental causes or in using incorrect or insufficient data provided by Client.
- Service Provider will not develop applications as a part of this Agreement.
- Service Provider engineers shall not be asked to perform, nor volunteer to perform, engineering and/or consulting tasks that are outside their skill sets and experience. Service Provider consultants have the right to decline a Service request if the request falls outside the area of expertise of a Service Provider staff member.
- This document and price are valid for 60 days from the date of issue and for services delivered within 365 days of that date.
- Service Provider Responsibilities
- Provide professional, knowledgeable, and qualified staff to deliver Services as necessary to complete the requested tasks where applicable.

Client Responsibilities

- If applicable, perform a full working backup of its environment prior to the commencement of the Services. Service Provider is not responsible for lost data.
- Provide a resource dedicated to this project. The extent of the knowledge transfer is dependent upon the availability of this resource. Please note that the time designated for knowledge transfer is throughout the project.
- Supply the necessary administrative usernames and passwords available to the Service Provider consultant.
- Provide Service Provider with detailed and accurate information regarding its current network environment. This information may include the technical configuration of the domain environment.
- Supply Service Provider with a professional workspace and network access to provide the Services.
- Grant access to the building(s) and room(s) as necessary to complete the Services.
- Provide all hardware and/or software and licensing required to perform the Services, including ensuring that all wiring, hardware, and software required to perform the Services are in working order.
- Assign a technical point of contact for Service Provider during the performance of the Services.