Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

Effective April 1st, 2025. These Service Descriptions supersede and replace all prior versions.

SCHEDULE OF SERVICES

THESE DESCRIPTIONS ARE SUBJECT

TO CHANGE ANY TIME WITHOUT

NOTICE.

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of Provider's Security Services is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property right in and to the security software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

REMOTE HELPDESK SUPPORT`

Provider provides unlimited comprehensive end-user support through its Remote Helpdesk Support service. This service is available 24 hours per day, 7 days a week and 365 days per year, except for US federal holidays, ensuring that users receive continuous assistance for their technical issues. Support can be accessed via chat, phone, and email, offering flexibility and convenience for users. The service is subject to the scope, conditions and terms of the service level agreement.

PATCH MANAGEMENT

Patch Management is a service provided targeting both managed Windows computers and managed Windows servers that run supported operating systems. This service focuses on applying OS-related patches that are classified as critical or important. Patch Management is conducted in accordance with the patching and maintenance policy mutually agreed upon by the provider and the client, ensuring that systems are kept secure and up to date. Regular patch cycles are scheduled to minimize disruption, with emergency patches deployed as necessary to address vulnerabilities promptly.

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

• **Failed patch troubleshooting** is included.

• **Client Responsibilities**: Clients must ensure devices remain online and connected to the management platform during scheduled maintenance windows.

• **Exclusions**: Provider is **not responsible** for any issues resulting from vendor-issued patches or compatibility failures.

MANAGED WINDOWS SERVER PATCHING

Provider will perform automated OS patching for systems running a supported Windows Server OS. Patching will be monitored monthly subject to the patch release and patch installation schedule outlined in the client maintenance policy. Troubleshooting of failed patches is included. The provider is not responsible for any software or hardware issues resulting in an installed patch.

REMOTE SERVER MONITORING AND MANAGEMENT

Provider will perform server monitoring and management including, alert monitoring and management of Windows services, periodic reporting and performance tuning, and prioritization of alerts to identify high-priority incidents. Provider will also perform remote remediation services as needed. The Service Fee does not include major hardware / software upgrades or replacements or new server installations.

WINDOWS AND MAC SUPPORT

Provider offers remote support for troubleshooting and user assistance related to Windows and macOS operating systems. Support is provided in accordance with vendor best practices and recommendations to maintain performance and security. This includes support for the operating systems themselves and licensed, supported third-party applications installed on covered devices.

This service applies exclusively to company-owned and managed devices that:

- Are enrolled in the Provider's management platform
- Meet minimum hardware requirements
- Have the Provider's required security and monitoring agents installed

Personal devices are not covered under this service.

In addition to remote support, the Provider delivers comprehensive desktop management, which includes:

- Management of company-owned desktops and laptops
- Remote troubleshooting and remediation
- Firmware updates as required by the manufacturer
- Operating system patching

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

- Limited updates for supported third-party applications

Hardware replacements and new hardware installations are not included in the standard service fee unless explicitly specified in the service order.

DEDICATED ENGINEERS

The provider provides clients with an assigned dedicated engineer who possess expertise and a deep understanding of the client's unique environment and needs. These engineers work closely with clients to ensure that their specific requirements are met, offering personalized support and tailored solutions. This service is designed to foster a strong partnership between the provider and its clients, ensuring that the clients' technology infrastructure is optimized and aligned with their business goals.

MOBILE DEVICE MANAGEMENT

Mobile Device Management (MDM) services are designed to ensure that corporate mobile devices are managed efficiently and securely. This service includes the management of corporate-owned mobile devices, ensuring they are enrolled with Intune and Azure AD, meet minimum hardware and OS specifications, and have the necessary tools installed. The MDM service also covers the setup of new mobile devices, ensuring they are configured according to the client's requirements and security policies.

LINE OF BUSINESS APPLICATION UPDATES

Provider offers a comprehensive service for line of business application updates. This service ensures that all critical business applications are kept up-to-date with the latest features, security patches, and performance improvements. Due to the sensitivity of line of business applications and their impact on interoperability and business workflow, the client is responsible for notifying and requesting from the provider that an application update is deployed for a specific application and working with the provider to coordinate the implementation of these updates in a manner that minimizes disruption to the client's operations.

NEW COMPUTER AND USER SETUPS

This service includes the configuration and deployment of new computers, ensuring that they are set up according to the client's specific requirements and security policies. The service also covers the setup of user accounts, including the configuration of necessary permissions and access controls to ensure that users have the appropriate level of access to the resources they need. Additionally, provider will provide support for the installation of essential software and applications, ensuring that all necessary tools are available and functioning correctly from day one. This service is designed to minimize downtime and ensure a smooth transition for new users, allowing them to be productive as quickly as possible.

IDENTITY AND ACCESS MANAGEMENT

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

Identity and Access Management (IAM) ensures secure and efficient access to corporate systems and data. This service manages user, administrator, and escalated privilege access using a least privilege model to minimize risks. It includes periodic reviews of IT security policies for compliance with industry standards.

The IAM service covers:

- Administration of access permissions based on the client's policy
- Enforcement of least privilege access
- Configuration and management of Multi-Factor Authentication (MFA) for Microsoft 365 and third-party apps
- Regular review of privileged access roles

Key IAM and MFA capabilities include:

- User account provisioning and de-provisioning
- Permissions Changes for Email Accounts, Groups and File Shares
- Modifications to Role Based Access Control

MANAGED CLOUD BACKUP

Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data is backed up via a third-party client-side desktop/server application or via API, encrypted, stored remotely in a Third-Party owned datacenter facility and storage repository. Data files can be restored from the cloud but the server itself cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution. Provider will monitor the status of all scheduled backup jobs, notify Client of storage failures beyond the agreed upon Recovery Time Objective and Recovery Point Objective outlined in the client's backup policy which provider has agreed to or provided , perform corrective actions, and work with third-party to resolve backup failures. Provider will also provide remote administrative services of Data Backup Service as requested by Client. Upon termination of these Services, Provider will have no responsibility for data retention or integrity of backups for the covered systems. Upon service termination, **data retention responsibility shifts to the client**.

DISK ENCRYPTION

Provider will implement disk encryption on corporate-owned devices to protect data from unauthorized access. This service ensures that data stored on devices is encrypted and secure. Disk encryption helps safeguard sensitive information against theft or loss. It provides an additional layer of security by making data unreadable without proper authorization. Encryption keys will be stored automatically within Microsoft Endpoint Manager. Provider makes no guarantees as to the recoverability of encryption keys if lost.

EMAIL ENCRYPTION

Provider will manage native email encryption within the email platform to ensure that emails containing sensitive information are encrypted during transmission. This service helps protect

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

confidential communications from being intercepted or accessed by unauthorized parties. Email encryption ensures that only the intended recipient can read the message. It also helps organizations comply with data protection regulations. Provider will troubleshoot and modify the encryption system configuration to ensure its effectiveness.

EMAIL SECURITY

Provider will implement and manage email security solutions to protect against phishing, spam, and other email-borne threats. This service includes real-time monitoring and filtering of incoming and outgoing emails. Email security solutions help prevent malicious emails from reaching users' inboxes. Provider will regularly update and fine-tune the email security systems to address new and emerging threats. This service ensures the integrity and confidentiality of email communications.

ENDPOINT SECURITY

Provider will manage and secure corporate endpoints, including desktops, laptops, and other managed devices, to mitigate cybersecurity threats. This service includes:

• **Installation, configuration, and continuous updating of endpoint security solutions**, including **antivirus, endpoint detection and response (EDR), host-based intrusion detection (HIDS), and anti-malware protection**.

• **Firewall, Intrusion Prevention, and Gateway Antivirus** to provide real-time protection against network threats, spyware, SQL injections, cross-site scripting, and buffer overflows.

• **Advanced Persistent Threat (APT) Protection** to detect and prevent sophisticated attacks, including ransomware and zero-day threats.

• **Regular security scans and automated remediation of detected malware or security incidents**.

• **URL Filtering** to block known malicious websites and enforce safe browsing policies.

• **Application Control** to restrict or block unauthorized software execution based on business requirements.

Provider will ensure all endpoints comply with the latest security policies and maintain protection through real-time threat detection and response.

MANAGED SINGLE SIGN ON – 3RD PARTY APPS

Provider will implement and manage single sign-on (SSO) solutions natively within Microsoft Entra ID for third-party applications. This service simplifies user access by allowing them to use a single set of credentials to access multiple applications. SSO improves security by reducing the number of passwords users need to remember and manage. It also enhances user

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

productivity by streamlining the login process. Provider will oversee the integration and maintenance of SSO systems to ensure seamless access to third-party apps.

SIMULATED EMAIL PHISHING

Provider will conduct simulated email phishing campaigns to test and improve employee awareness of phishing threats. This service includes sending mock phishing emails to employees and tracking their responses. The results of the simulations will be used to provide targeted training and feedback to employees. Simulated phishing helps organizations identify vulnerabilities and educate employees on recognizing and avoiding phishing attempts. Provider will schedule regular simulations to maintain a high level of security awareness.

ADVANCED EMAIL THREAT PROTECTION

Provider will implement advanced email threat protection solutions to detect and block sophisticated email threats. This service includes real-time scanning and analysis of email content and URL filtering to identify malicious attachments, links, and other threats. Advanced threat protection helps prevent email-based attacks such as ransomware and spear-phishing. Provider will continuously update the threat protection systems to address new and evolving threats. This service ensures the security and integrity of email communications.

SECURITY AWARENESS TRAINING PROGRAM

Provider will offer a security awareness training program to educate employees on best practices for cybersecurity. This service includes regular training sessions and materials to keep employees informed about the latest security threats and their mitigation. Security awareness training aims to reduce the risk of security breaches caused by human error. Provider will deliver ongoing security awareness training and phishing simulations to enhance employee knowledge of cybersecurity threats. This service includes:

- Scheduled and randomized phishing campaigns designed to test and educate employees on recognizing phishing threats.
- Detailed tracking and analytics to assess user responses and identify vulnerabilities.
- Customizable training modules based on phishing simulation outcomes to improve cybersecurity behaviors.
- Automated user risk scoring to measure security awareness levels and ensure continuous improvement.

Provider will implement and manage a managed cybersecurity awareness training platform ordered through a third party on Client's behalf. The program features:

- Enrolling all technology-facing workforce members in the program.
- Access to a curriculum of industry-leading cybersecurity awareness education, customizable to meet the unique needs and regulatory requirements of Client.
- Management reporting and visibility into workforce participation and progress in the training.

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

- Regular campaigns to test each workforce member's ability to recognize and effectively respond to cyberattacks targeting individuals.
- Automated enrollment in remedial training for individual workforce members when appropriate.

DARK WEB MONITORING

Provider will monitor the dark web for any compromised data related to the client. This service includes scanning dark web forums, marketplaces, and other sources for stolen credentials, proprietary information, and other sensitive data using an automated system. If any compromised data is found, the client will be automatically alerted and be provided guidance on mitigation steps. Dark web monitoring helps organizations respond quickly to potential security breaches. Provider will regularly update monitoring techniques to stay ahead of new dark web threats.

WEB CONTENT FILTERING

Provider will implement **web content and DNS filtering** to restrict access to malicious, inappropriate, or non-business-related websites. This service includes:

• **DNS Filtering** to detect and block malicious DNS requests, preventing access to harmful domains.

• **URL and Content Filtering** to control access based on business policies and security needs.

• **Client-Side DNS Filtering** for laptops and remote users to protect devices even when outside the corporate network.

• **Redirection to Safe Pages** for users attempting to access blocked content, reinforcing cybersecurity awareness.

Provider will continuously update filtering policies and monitor effectiveness, ensuring proactive protection against phishing, malware, and other online threats.

M365 SECURE SCORE MANAGEMENT

Provider will manage the Microsoft 365 Secure Score to ensure that the client's Microsoft 365 environment is configured according to best practices. This service includes monitoring the Secure Score dashboard and recommending improvements to enhance security. Regular assessments will be conducted to identify and address security gaps. M365 Secure Score management helps improve the overall security posture of the Microsoft 365 environment. Provider will provide guidance and support to implement the recommended actions.

MANAGED DETECTION AND RESPONSE

IMAGIS

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

Provider delivers **24/7 Managed Detection and Response (MDR)** services, supported by a **Security Operations Center (SOC)**, to **detect, analyze, and respond to security threats in real-time**. This service ensures **continuous monitoring, rapid threat identification, and effective remediation** to minimize security risks and maintain business continuity.

Key Features & Capabilities

• **Continuous Threat Monitoring** – Real-time security monitoring of **networks, endpoints, cloud environments, and user accounts** to detect suspicious activities.

• **Enterprise-Grade Threat Intelligence** – Correlates data from multiple sources to **prioritize and respond** to security incidents effectively.

• **Automated & Analyst-Driven Incident Response** – Combines **machine learning-driven** automation with expert **SOC analysis** for rapid threat investigation and containment.

• **Ransomware Rollback** – Restores compromised files to a **pre-infection state**, minimizing damage from ransomware attacks.

• **Advanced Malware Detection** – Identifies **cryptojacking, ransomware, zero-day exploits, and advanced persistent threats (APTs)**.

• **Detailed Incident Reports & Mitigation Plans** – Provides **actionable insights** and **recommendations** for strengthening security postures.

Endpoint Response Capabilities

Windows & macOS Devices

• **Device Isolation** – If a device is compromised, **network communication is blocked**, preventing lateral movement. Only the security agent remains connected for **continuous monitoring**.

• **Device Un-Isolation** – The SOC can **lift isolation** once the threat is mitigated.

• **Scheduled Task Management** – The SOC can **disable, delete, or restore** malicious scheduled tasks to prevent unauthorized persistence.

Cloud-Based Threat Response

Microsoft 365

• **User Account Disablement** – Immediately disables compromised accounts and revokes access tokens to **prevent further abuse**.

• **External Mail Forwarding Rule Disablement** – Prevents attackers from **redirecting emails** to external domains for **data exfiltration**.

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

• **Malicious Enterprise Application Blocking** – Identifies and **disables suspicious applications** integrated into the Microsoft 365 environment.

Google Workspace

• **Unapproved Country Login Detection** – Detects **logins from unauthorized geographic locations** and flags them for review.

• **Suspicious Login Analysis** – Flags logins using **TOR, risky VPNs, or residential proxies** as potential threats.

• **Suspicious Email Filtering Rule Detection** – Identifies and disables **malicious email filtering rules** set by attackers.

• **External Email Forwarding Prevention** – Blocks newly created **automatic email forwarding rules** that attempt to exfiltrate sensitive data.

• **Google Account Disablement** – Suspicious accounts can be **disabled by the SOC** to prevent unauthorized access.

NETWORK INTRUSION DETECTION

Provider will implement network intrusion detection systems (NIDS) to monitor and detect unauthorized access to the corporate network. This service includes real-time monitoring of network traffic for signs of intrusions and anomalies. NIDS helps identify and respond to potential security breaches before they can cause significant damage. Provider will regularly update the intrusion detection rules and signatures to address new and emerging threats. This service ensures the security and integrity of the corporate network.

VULNERABILITY MANAGEMENT WITH REMEDIATION

Provider will conduct vulnerability assessments and manage remediation efforts to address identified vulnerabilities. This service includes regular scanning of systems and networks to detect security weaknesses. Provider will prioritize and apply necessary patches or fixes to remediate vulnerabilities. Vulnerability management helps organizations stay ahead of potential threats by addressing security gaps. Provider will provide detailed reports and recommendations for improving the overall security posture.

LOG COLLECTION AND STORAGE

Provider will collect and store logs from various systems and devices for compliance purposes. This service includes setting up and managing log collection mechanisms to ensure comprehensive logging. Logs will be stored securely and made available for analysis and auditing. Log collection and storage help organizations meet certain compliance and regulatory requirements where applicable and may be used as part of the forensics analysis after a cyber incident. Provider will ensure that logs collectors are setup and are ingesting data from

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

applicable sources. Retention period of logs varies and is dependent on applicable third-party licensing.

COMPLIANCE AND AUDIT SUPPORT

Provider will support the client in meeting compliance requirements and preparing for audits. This service includes providing documentation and control evidence artifacts, assisting with preparation of formal responses to third-party assessments or questionnaires, and offering guidance on compliance issues. Provider will help identify and address any gaps in the client's compliance posture.

This service includes:

• **Compliance documentation, control evidence, and audit preparation support**.

• **Incident response assistance in the immediate aftermath of a data breach**, working with qualified third parties to support incident response efforts to identify the source and initial mitigation steps.

• **Guidance on regulatory frameworks**, including ISO27001, HIPAA, and SOC2.

Provider supports clients efforts to **maintain compliance, mitigate security risks, and respond effectively to cyber incidents**.

MANAGED LOCATIONS

Provider supports client-owned or leased private office locations by ensuring the stability and integrity of the office network infrastructure. Support is provided remotely whenever possible. If network-level issues cannot be resolved remotely, on-site support will be delivered upon request and subject to the limitations specified in the Order.

On-site support is available only for managed office locations during normal business hours with and is limited to troubleshooting and remediating network-related issues.

INFORMATION SECURITY POLICY DEVELOPMENT

Provider will collaborate with client stakeholders to develop comprehensive information security policy documents tailored to their IT infrastructure. Using proprietary templates aligned with frameworks such as ISO27001, HIPAA, and SOC2, Provider ensures policies reflect the actual configuration and support provided for the IT environment and operations. This alignment helps clients prepare effectively for audits and maintain compliance.

CLOUD MANAGEMENT SERVICES

Provider will manage cloud hosting environments for clients, specifically focusing on Microsoft Azure. This service includes performing cost management analyses to identify potential

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

opportunities for cost savings. Provider will evaluate trends in performance, utilization, and data growth, making informed recommendations to optimize the client's cloud infrastructure.

Support requests will be handled efficiently, acting as an intermediary between the client and the cloud hosting vendor for any issues with the platform, leveraging our partner relationship with Microsoft Azure. This ensures that clients receive prompt and effective resolution for any cloud-related concerns.

In addition, Provider offers architecture advisory services for clients looking to make substantial changes to their cloud environment. This involves working closely with the client's DevOps teams to support their efforts from both an infrastructure and security standpoint, ensuring that any modifications are aligned with best practices and optimize operational efficiency.

Our comprehensive cloud management services help clients maximize the value of their cloud investments while maintaining robust security and operational governance.

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

CLOUD AND HOSTING SERVICES

Third-Party Cloud & SaaS Vendors - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft. Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this software is subject to the applicable third-party cloud or software-as-a-service vendor's agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to be bound by any applicable third-party cloud or software-as-a-service vendor's agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

CYBER TRAINING SERVICES

Provider will implement and managed a managed cybersecurity awareness training platform ordered through a third party on Client's behalf. The program features:

- Enrolling all technology-facing workforce members in the program
- Access to a curriculum of industry-leading cybersecurity awareness education which can be customized to meet the unique needs and regulatory requirements of Client
- Management reporting and visibility into workforce participation and progress in the training
- Regular campaigns to test each workforce member's ability to recognize and effectively respond to cyberattacks which typically target individuals
- Automated enrollment in remedial training for individual workforce members, when appropriate
- Management reporting and visibility into workforce performance on testing campaigns
- Management reporting and visibility into the improvement in workforce awareness and performance over time
- Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals

Imagis, LLC
212-729-7171
info@imagisIT.com
www.imagisIT.com

VOIP AND COLLABORATION SERVICES

Provider will deliver the Voice over Internet Protocol ("VoIP") and associated telephony and collaboration services specified and selected by you on the Order or Proposal. Additional Services may be added only by entering into a new Order including those Services.

The VoIP Services may be provided or delivered by Provider through the use of third-party vendors listed on the Order or Proposal. Use of the VoIP Services are subject to any applicable third-party vendor agreements. Client acknowledges and agrees to be bound by those third-party vendor agreements. Provider shall not be responsible for any third-party vendor service failures when accessing or using the Services. Client agrees to be bound by any applicable third-party vendor's agreements regarding terms and conditions or end user licensing, and Client understands that any applicable agreement regarding terms and conditions or end user licensing is subject to change by any third-party vendor without notice.

Network cabling, conduit, electrical, rack space, and any other required construction or trenching are additional charges are not included with the Service.

**Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.