IMAGIS

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

MANAGED IT SERVICES SERVICE LEVEL AGREEMENT

The following document establishes the service level agreement applicable to services provided by Imagis to the client. It defines acceptable service availability, response times, and performance standards to ensure consistent and reliable support. The document details response time commitments based on issue severity, escalation procedures to address critical incidents, and key performance metrics to measure service effectiveness. By clearly outlining these parameters, this SLA promotes transparency, accountability, and a shared understanding of service expectations between Imagis and the client.

1. SERVICE DESCRIPTION: SERVICE DESK

Engineers will provide support for desktops, laptops, printers, tablets, and mobile phones. This includes remote diagnostic support for hardware issues and resolution support for operating system software and browsers, as well as mainstream productivity software, excluding open-source applications.

Additionally, tasks such as restarting desktop-side services, adding or disabling users on a domain, modifying user email settings, and addressing other similar issues.

1.1 HOURS OF OPERATION

Live phone support, email ticket support, and online chat support are available 24/7, all year round, except on Federal Holidays, when best-effort support will be provided, and these times will not be included in the calculation of SLA metrics.

The following schedule defines business hours:

Day	Time
Sunday	N/A
Monday	9 am – 5 pm EST
Tuesday	9 am – 5 pm EST
Wednesday	9 am – 5 pm EST
Thursday	9 am – 5 pm EST
Friday	9 am – 5 pm EST
Saturday	N/A

1.2 SERVICE LEVEL OBJECTIVES

Monthly metric targets are calculated averaging the speed to answer across all lines of support for the month. The blended target goal for initial response time and speed to answer is 80%.

The response times listed below apply to all service requests regardless of priority:

Method Used to Create Service Request	Average Initial Response Time	Goal Reach Rate as %
Phone	90 Seconds	80%
Chat	30 Seconds	80%
Email during Business Hours	15 Minutes	80%
Email after Business Hours	Next Business Day	80%

Please note that email responses to tickets submitted after hours will be provided on the next business day. If support requests during this time are critical and require an urgent response, the client end-user must engage in support via a phone call. If there is an existing ticket for a request that requires an urgent response, we advise calling the service desk and referencing the service ticket number.

Once a service desk engineer has responded to the ticket, a priority is set to track the request through to completion.

TICKET PRIORITIES

Ticket priority is set by determining Severity and Impact criteria as defined in the tables below.

Criteria	Description
Severity – Low	One user or a small group of users is affected
Severity – Medium	Departments or large group of users are affected
Severity – High	Whole company is affected
Impact – Low	More of an irritation than a stoppage
Impact – Medium	Business is degraded, but there is a reasonable workaround
Impact - High	Critical business processes are stopped

Service ticket priorities are determined by the following criteria:

	High Severity	Medium Severity	Low Severity
High Impact	Priority 1	Priority 2	Priority 2
Medium Impact	Priority 2	Priority 3	Priority 3
Low Impact	Priority 3	Priority 3	Priority 4

Time to In Progress is defined as the total amount of time between the initial response and the time that an engineer begins to work on the actual service request. This does not include the time that a ticket is in a waiting status such as Waiting Vendor or Waiting Client Response.

The table below defines the service level targets for the response time required to initiate action on a ticket.

Ticket Priority	Time to In Progress	Goal %
Priority 1 - Emergency	.5 Hours	80%
Priority 2 - Quick	1 Hour	80%
Priority 3 - Normal	2 Hours	80%
Priority 4 - Next Visit	4 Hours	80%

1.3 SCOPE OF SERVICES

The following scope of services is included as part of the service desk:

GENERAL SUPPORT

- General support for Windows, including "how-to" assistance
- General support for Mac OSX, including "how-to" assistance
- Assistance with Google apps and web applications
- Installation and usage support for PC/Mac productivity applications
- How-to assistance for standard Microsoft Office Applications

- General support for tablets and mobile devices
- Support for local printer/scanner usage

TROUBLESHOOTING

- Troubleshooting error messages (OS or application)
- Troubleshooting slow computer performance
- Troubleshooting Outlook Email client issues
- Detection and removal of suspected viruses
- Troubleshooting Microsoft Edge and Google Chrome web browsers
- Resolving remote access issues, including Azure VPN, Meraki VPN, Citrix Cloud, Azure Virtual Desktop, Windows 365, and Remote Desktop Services

EMAIL AND CLOUD SUPPORT

- Backup and email file recovery from Managed Microsoft 365 Tenant or Managed Google Workspace store, following established guidelines
- Cloud Email support, including adding/disabling users and troubleshooting errors
- Managing distribution lists in email portals
- Adding or modifying Microsoft 365 Groups or Entra ID Security Groups

NETWORK AND USER MANAGEMENT

- Support for network printers and scanners (excluding server configuration or installations)
- Managing user accounts on domains such as Active Directory Domain Services, Google Workspace, or Entra ID tenants
- Password resets and service resets

TICKET HANDLING

Imagis will document all support activities, time entries, and notes within the service ticketing system. Clients can request access to the service ticket portal, where they can monitor their tickets, review activity notes, and provide additional information.
Furthermore, clients may request access to MyGlue, a secure web application that reflects our documentation for the client organization.

1.4 RESPONSIBILITIES

Clients are responsible for ensuring that the service desk has all of the required information and that all preliminary steps have been taken to enable support services.

In order to maintain consistent and quality support experience, clients are expected to:

- Provide up-to-date user lists
- Provide up-to-date information for all supported end users and contact information

- Provide the names and contact information for employees with whom we may interact with and will update with any new Client contacts as they change
- Provide timely notifications for terminated employees at least 48 hours in advance
- Ensure all standard and non-standard change requests are submitted by an authorized contact as documented
- Notify of changes to authorized personnel and complete an updated authorized contact sheet in a timely manner
- Work with third-party vendors if their support or escalation is required to resolve an issue.
- Provide Admin access credentials for all supported systems and applications.
- Notify Imagis of any quality incidents or questions about escalation reported by the Client or its stakeholders within 48 business hours of the incident
- Share Quality Feedback/Survey results with Imagis
- Engage a reputable third-party for certified data destruction and recycling of hardware
- Provide wiring and floor plans for managed locations
- Ensure that all client owned hardware is under active manufacturer warranty
- Ensure that all line of business applications and third-party software is procured legally and has an active vendor support contract in place

1.5 SERVICE EXCLUSIONS

Change requests or enhancements not explicitly listed in the scope of services will be considered out of scope and may incur additional charges. This includes support for outdated software and hardware, personal devices, and network re-architecting or redesigning. Such requests will be billed separately under a block hour agreement.
How-to based requests will be handled on a best-effort basis for these systems. Recommendations for third-party vendors or products may be made if best-effort work is not applicable.

The following services are outside the scope of our offerings:

OUT-OF-DATE SOFTWARE AND HARDWARE

Imagis will not offer support or troubleshooting for outdated software or hardware that is not under the manufacturer's warranty. All client software and hardware should have valid manufacturer support and warranty. Clients are responsible for ensuring that all systems are current and have valid licensing.

PRINTERS

Imagis is not responsible for managing printer hardware, which includes handling physical device malfunctions, ink and toner replacement, accessories installation and troubleshooting, print and scan reporting, and hardware maintenance. For these types of issues, it is highly recommended to engage a print management service, particularly for commercial grade multi-function copiers and printer hardware. The printer vendor should be contacted as hardware support falls under OEM and Manufacturer/Vendor support agreements.

PERSONAL COMPUTERS OR DEVICES ARE NOT SUPPORTED.

Only devices owned or leased by the client and explicitly stated in writing (including the serial number) as fully managed, secured, and enrolled by the organization will be treated as work machines. Imagis will not be liable for any issues arising from personal devices, including compliance, security, or legal concerns. Support for personal machines is limited to ad-hoc remote sessions with user permission, focusing on access to cloud-based data and apps. Hardware issues on personal devices will not be addressed, and support for is limited to cloud data and and web based application access subject to compatibility.

FORCE MAJEURE EVENTS

The service level agreement does not cover Scheduled Downtime, Client-side Downtime, Startup Period or when outages or issues occur due to a force majeure event. Any such instances will be removed from the calculation and measurement of service level objectives.

Force majeure events include, but are not limited to:

- significant failure of a part of the power grid
- failure of the Internet, natural disaster or weather event
- fire, explosions
- physical access limitations, acts or orders of government
- war, riot, insurrection, epidemic, strikes or labor action, or terrorism.

CUSTOM SOFTWARE DEVELOPMENT

Imagis does not offer custom software development services as part of its standard offerings. Clients requiring custom software or application development will need to engage with specialized developers or third-party vendors.

UNSUPPORTED APPLICATIONS AND SYSTEMS

Support for applications and systems that have reached end-of-life or are no longer supported by their respective vendors is not included within the scope of services. Clients are encouraged to upgrade to supported versions or seek alternative solutions.

2. SERVICE DESCRIPTION: MANAGED LOCATIONS

Imagis provides managed location services that encompass comprehensive network troubleshooting. This service includes diagnosing and resolving network issues remotely, and if remote resolution is not feasible, addressing them onsite.

2.1 HOURS OF OPERATION

Managed location support is available Monday to Friday, 9 am to 5 pm, for urgent network related issues with business impact.

Day	Time
Sunday	N/A
Monday	9 am – 5 pm EST
Tuesday	9 am – 5 pm EST
Wednesday	9 am – 5 pm EST
Thursday	9 am – 5 pm EST
Friday	9 am – 5 pm EST
Saturday	N/A

2.2 SERVICE LEVEL OBJECTIVES

SCHEDULING AND NOTICE PERIODS

Priority - Request	Notice Period	Time to Respond from Notice
1 – Service Incident Dispatch	1 Day	Situational
2 – On-Site Engineer Dispatch	5 Days	5 Days
3 - General	N/A	See table below

- **General Requests:** A notice period must be provided in advance to ensure timely processing and scheduling of requests. Details regarding the notice period will be specified based on the nature of the service requested.
- **On-Site Engineer Dispatch Requests:** Scheduling on-site engineer dispatch requests at least 5 days in advance, excluding high-priority (P1) events. This ensures adequate preparation and resource allocation for effective issue resolution.
- **Service Incidents Dispatching for High Priority (P1) events:** An onsite field engineer will be dispatched to troubleshoot any core network related issues pertaining to the managed network equipment (excluding ISP outages) at the discretion of the service manager and only upon determining that the incident cannot be resolved remotely. Dispatching for incidents is subject to resource availability in the geographic area of the location.

The table below defines the service level targets for the response time required to initiate action on a ticket for managed locations requiring remote service support.

Ticket Priority	Time to In Progress	Goal %
Priority 1 - Emergency	.5 Hours	80%
Priority 2 - Quick	1 Hour	80%
Priority 3 - Normal	2 Hours	80%
Priority 4 - Next Visit	4 Hours	80%

2.3 SCOPE OF SERVICES

The scope of service for managed location tasks includes:

- **Managed Switch:** Comprehensive management of network switches including configuration changes and troubleshooting to ensure optimal performance and reliability of network infrastructure and failover mechanisms.
- **Managed Firewall:** Proactive management of network firewall devices to safeguard network security through regular updates, rule management, threat monitoring, and incident response.
- **Managed UPS: Configuration and remote troubleshooting** of Uninterruptible Power Supply (UPS) systems to ensure continuous power availability and protection against power disturbances.
- **Managed Wireless:** Deployment, troubleshooting and management of wireless networks, ensuring robust and secure connectivity for all devices within the managed locations.

- **Managed VPN Connectivity:** Establishment, troubleshooting and management of secure Virtual Private Network (VPN) connections (P2S and S2S) to facilitate safe remote access to network resources or privacy network services through approved vendors.
- **ISP Escalation Support:** Liaise with Internet Service Providers (ISPs) to address and resolve connectivity issues, ensuring minimal disruption to network services.

- Facilitating and supporting Internet Service Providers (ISPs) changes.
- Reporting ISP outages and coordinating repair requests with the vendor only if they have a business impact for the client.

2.4 RESPONSIBILITIES

Clients should ensure the physical premises are prepared for on-site engineers. This includes providing clear access to network equipment, ensuring that the necessary power and network connections are available, and maintaining a safe working environment.

- Clients should also designate a point of contact who can assist the service desk and on-site engineers with any site-specific requirements or questions that may arise during the service visit.
- Clients must promptly report any issues or incidents pertaining to network equipment to facilitate timely troubleshooting and resolution. This proactive communication helps minimize downtime and ensures the smooth operation of the managed network services.
- For any changes in network architecture or upgrades that may impact Imagis managed services, clients are expected to inform Imagis in advance. Collaborating on these changes helps in planning and executing the necessary adjustments without disrupting ongoing operations.

QUALIFYING CONDITIONS FOR ONSITE SUPPORT

To qualify for onsite support for network troubleshooting, clients must ensure the following conditions are met:

- The physical network must be set up by a licensed low voltage specialist.
- Wiring maps and diagrams must be provided and readily available onsite.
- All patch network connections and ports must have undergone a certified fluke test.
- The network must be wired with Cat5e or better wiring.
- All mounted access points must be physically accessible in a safe manner
- A network rack must be present onsite in a locked cabinet
- All network wires must be visually labeled inside the network rack.

NOTICE PERIOD FOR CERTIFICATES OF INSURANCE (COI)

In certain instances, clients may request a certificate of insurance (COI) for on-site work to be performed. A certificate of insurance (COI) is a document issued by an insurance company or broker that verifies the existence of an insurance policy and summarizes its key aspects and conditions. For example, a standard COI lists the policyholder’s name, the policy’s effective date, the type of coverage, policy limits, and other pertinent details.

Please note that COIs are not a standard requirement for Imagis’ services, as packaging, loading, or transporting equipment is not handled by Imagis or any of its third-party providers. Requests for COIs are not standard, and any efforts to address such requests are made purely out of goodwill. Any COI provided by the team will be a standard certificate, and additional documentation is not necessary for the work provided.

Should a COI be mandatory in a specific case, requests must be submitted to Imagis **at least 10 business days** prior to the scheduled work date to ensure sufficient processing time.

2.5 SERVICE EXCLUSIONS

Change requests or enhancements not explicitly listed in the scope of services will be considered out of scope and may incur additional charges. This includes support for outdated software and hardware, personal devices, and network re-architecting or redesigning. Such requests will be billed separately under a block hour agreement.
How-to based requests will be handled on a best-effort basis for these systems. Recommendations for third-party vendors or products may be made if best-effort work is not applicable.

The following services are outside the scope of our offerings:

WIRING TASKS.

This involves the physical installation and organization of network cables and hardware connections within a facility. It encompasses running wires through walls, setting up connection points, and ensuring proper signal transmission.

UPTIME MONITORING FOR STATIC IPS

Uptime monitoring for static IPs**,** which can be managed automatically using alerts. This entails ensuring that a specific IP address is consistently reachable over the internet. Firewall solutions provide automated tools and notifications to handle these tasks without manual intervention.

NETWORK RE-ARCHITECTURE OR REDESIGN.

This includes comprehensive changes to an existing network’s structure or creating a new design from scratch to improve performance, scalability, or security. Such projects often require detailed planning, assessment, and implementation efforts.

VPN UPTIME MONITORING.

This pertains to ensuring that Virtual Private Network (VPN) connections remain active and reliable. The process typically involves checking the connectivity status and performance of VPN links, but it falls beyond our service capabilities.

3. SERVICE DESCRIPTION: SERVER MANAGEMENT

Imagis will provide server support services in the form of Server Management, defined as responding to issues within an end client environment related to performance and availability to bring the operating system and or environment back to a steady operational state. This includes issue remediation concerning network, server, storage, and application support in accordance with this agreement.

3.1 HOURS OF OPERATION

Server Monitoring operates 24x7x365 and will perform all the services outlined as In Scope. All other activities operate during normal business hours.

3.2 SERVICE LEVEL OBJECTIVES

RESPONSE TIMES

Server Management Response times are measured from when the alert is generated and logged in the ticketing system.

Priority	Initial Investigation	Time to In Progress	Goal

P1 – Critical	15 Minutes	30 Minutes	90%
P2 – Major	30 Minutes	1 Hour	90%
P3 – Intermediate	1.5 Hours	4 Hours	90%
P4 – General Issue	6 Hours	24 Hours	90%

PRIORITY MATRIX

Priorities for monitored alerts are set based on the following criteria:

PRIORITY 1: BUSINESS CRITICAL INFRASTRUCTURE PROBLEM

- Outage to all or a significant part of Business System
- Considered “Network Down / Server Down” condition
- Represents a complete loss of service or a significant feature that is completely unavailable, and no workaround exists
- Limited to most important applications, devices and services that are required for day-to-day business operations
- Critical applications could be database, email, accounting software or other applications that are relied upon to conduct normal business operations

PRIORITY 2: DEGRADED SERVICE INVOLVING A MAJOR NETWORKING / SERVER PROBLEM.

- Either “Network / Server Down” condition or severe degradation of network performance
- Applications / Systems Errors in Event Viewer logs
- Applications / Systems Logs providing numerous warnings / error combination
- Hardware Errors (which may require replaced hardware)
- Multiple failed login attempts

PRIORITY 3: INTERMITTENT SERVICE.

- Non-Critical Error in Application/Server/Network
- Includes intermittent issues and reduced quality of service. A workaround may be available
- Hardware warnings
- Applications / Systems Logs providing numerous warnings
- Sporadic Failed Logins
- Impaired networking / Server performance in small area
- Most Client services remain functional but may not be operating to full potential

PRIORITY 4: GENERAL ISSUE.

- Proactive Monitoring: investigating warnings to resolution before issues arise
- Little or no impact on Partner operations, also included are administrative support issues

3.3 SCOPE OF SERVICES

The NOC will perform the following monitoring and remediation activities for the clients' covered devices and applications:

SUPPORTED OS VERSIONS

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

MANAGED PATCHING

- Scheduled Monthly OS Patching of Windows Servers
- Scheduled Monthly OS Patching of Windows Workstations
- Monthly Reporting available upon request

BACKUP AND DISASTER RECOVERY:

- Backup and DR configuration
- Daily monitoring of backup and DR systems
- Disaster recovery and backup restore activities
- Troubleshooting of failed backups and disaster recovery systems managed by Imagis

WINDOWS SERVER CONFIGURATION

- Initial setup and configuration of Windows Servers
- Configuration of Active Directory, DNS, and DHCP
- Group Policy Management
- File and Print Services configuration
- Network configuration and management
- Security configuration and hardening
- Performance tuning and optimization
- Monitoring and alerting setup
- Remote Desktop Services configuration
- High availability and clustering setup

24X7X365 MONITORING

Continuous monitoring of servers, workstations, and network devices to identify and respond to alerts promptly.

ALERT MANAGEMENT

Identification, verification, response, and tracking of alerts. A ticket is created for each alert based on acceptable thresholds.

EVENT AND ERROR MANAGEMENT

Handling events and errors from identification to resolution, including the management of severe or critical incidents.

SERVER MONITORING

Monitoring is performed in real-time, provided that the monitoring agent is running and there is internet access at the site. We monitor Windows server services, system resources, Microsoft Event Viewer, and Windows Services.

If HTTP/HTTPS is not available, we will be notified, as this is a requirement for the monitoring agent to function. Please note that specific protocols such as ICMP (pings), IMAP, and SSH are not monitored.

The data retention period for monitored devices is 3 months.

PRIORITY RESPONSE MODEL

A tiered response model designed to prioritize and address critical NOC events and performance issues immediately.
⍰

ALERTING AND MONITORING

Imagis will perform monitoring of standard alert thresholds described below. Changes to any of these thresholds can be made upon client request.

WINDOWS SERVER MONITORING ACTIVITY / PROCESS MONITORING

Process monitoring consists of an ongoing check to ensure that core systems processes are operating within predefined / agreed upon performance parameters. The core operating systems processes that are monitored include but is not limited to:

- Process Count to alert when a process is not running or is running an inappropriate number of instances
- % CPU Utilized to alert for those exceeding or approaching the threshold
- % Memory Utilized to alert for those exceeding or approaching the threshold
- Windows® Processes Monitored Operating system services configured to start automatically at startup

SYSTEM RESOURCE MONITORING

System Resource Monitoring consists of an ongoing check for constrained resources that persist over a period, which may indicate a performance issue. Monitored activity that may require attention and intervention to maintain identified thresholds includes but is not limited to:

- Disk Utilization
- Disk Space o Shared Memory Utilization
- CPU Bottleneck
- CPU Idle
- Blocked I/O
- Paging Activity
- Process Utilization
- Disk I/O
- Disk Queue (length / timeout)

- Available Memory
- Memory Utilization

MICROSOFT EVENT VIEWER

Microsoft event viewer is comprised of monitoring in real time for error conditions outside the normal condition's levels. System error messages that are monitored include but is not limited to:

- Critical event log errors
- File system full
- Failed login, Invalid login attempts by listed service accounts
- SCSI errors, Hardware or cooling system warnings and errors
- Ethernet Shutdown, System reboots

WINDOWS SERVICE MONITORING

Windows Service Monitoring is comprised of monitoring real time for the following:

- Service up time
- System event log files
- Service stop / start / restarts

3.4 RESPONSIBILITIES

Clients are responsible for ensuring all preliminary steps have been taken to enable support services:

- **Standard Operating Procedures:** Client will provide complete standard operating procedures and processes for any systems already in place. This includes preferred incident, problem, and change management resolution processes and escalation information needed.
- **Change Notification:** Client will inform the NOC team of changes relative to the monitoring operation, including but not limited to emergency maintenance and/or planned outages in a timely fashion. Lack of proper notification in a timely manner will excuse NOC from their service levels until the changes can be incorporated into the environment and staff can be trained.
- **New Technology Introductions:** The introduction of a client approved technology, which will alter the technical skill requirements of the staff, may require a change order to ensure that staff have the technical training to adequately perform their job function.
- **Imagis Personnel Notification:** Client will promptly notify Imagis of all Imagis personnel activities which require the attention of Imagis.
- **Vendor Support Contracts:** Client will ensure that vendor support contracts are in place for equipment and software supported by this agreement which continually generates an irregular level of alerts. If a vendor support contract is not in place Imagis reserves the right to
    - remove the item from being monitored
    - reduce the processes being monitored to include only those actionable
    - c) increase the price to reflect the increased number of alerts from the device or application.
- **Access Authorization:** Client will be responsible for authorizing all user requests for access rights and privileges.
- **Remote Access Rights:** Client will provide Imagis with remote access to Client systems as required to deliver services identified in this SOW. When given access through remote facilities to any Server or

Client computer or electronic data processing system to provide the managed services as described in this scope of work, Imagis will limit such access to activities related to those outlined.

- **Software Access Rights:** Client will provide Admin access rights to all software
- **Access Limitations:** Client will provide admin rights to Imagis only.
- **Documentation Notification:** If client makes any administrative level changes in any of the supported systems, client must notify Imagis in advance to have this change documented.
- **Software Licensing:** Client will ensure that all Client Client's software will include a valid license agreement between the Client and the Client's software original licensor. If providing managed desktop service(s) involving Client's software as set forth in this SOW, Imagis will comply with the terms contained in the applicable Client software license agreement for Client software provided, including those terms that govern:
- Rights granted or denied to third parties, whether in the form of a sublicense, to copy and distribute the Client software and,
    - Usage or duplication of the Client software in the creation of any image that may be required in the performance of the managed desktop service(s) if Client makes the terms of such Client software license available to Client.
- **Equipment Maintenance:** Client will continue to own and maintain all associated Client-owned tools and equipment.

In addition to the foregoing obligation, except as permitted in the Client software license agreement and this SOW, Imagis will not copy, modify, decompile, reverse engineer, or disassemble the Client software.

3.5 SERVICE EXCLUSIONS

Change requests or enhancements not explicitly listed in the scope of services will be considered out of scope and may incur additional charges. This includes support for outdated software and hardware, personal devices, and network re-architecting or redesigning. Such requests will be billed separately under a block hour agreement.
How-to based requests will be handled on a best-effort basis for these systems. Recommendations for third-party vendors or products may be made if best-effort work is not applicable.

The following services are outside the scope of our offerings:

- Change requests or enhancements not explicitly listed in the scope of services
- Support for outdated server software and hardware
- Upgrading line of business applications from one major version to another
- Network re-architecting or redesigning to support application or vendor requirements
- Creation, modification, or support for personal server-based applications
- Detailed how-to requests related to server management
- Recommendations for non-approved third-party server vendors or products
- Expanding storage for servers
- Upgrading virtual machine SKUs in Azure
- Installing or upgrading database software
- Major OS Upgrades

4. SERVICE DESCRIPTION: SECURITY (SOC) SERVICES

In a modern technology environment, a shared responsibility exists between the end-client and the various vendors involved in delivering IT capabilities to client organizations. Imagis provides a comprehensive offering of proactive, defensive measures to minimize the risk of cyber incidents.

Imagis and its partners may assist a client in the Identification of a cyber security incident. The client is responsible for ensuring their own information security program includes the appropriate policies and procedures as it relates to incident response and business continuity. As an IT Managed Service provider, Imagis will review and confirm acceptance of such governing documents in writing.

4.1 HOURS OF OPERATION

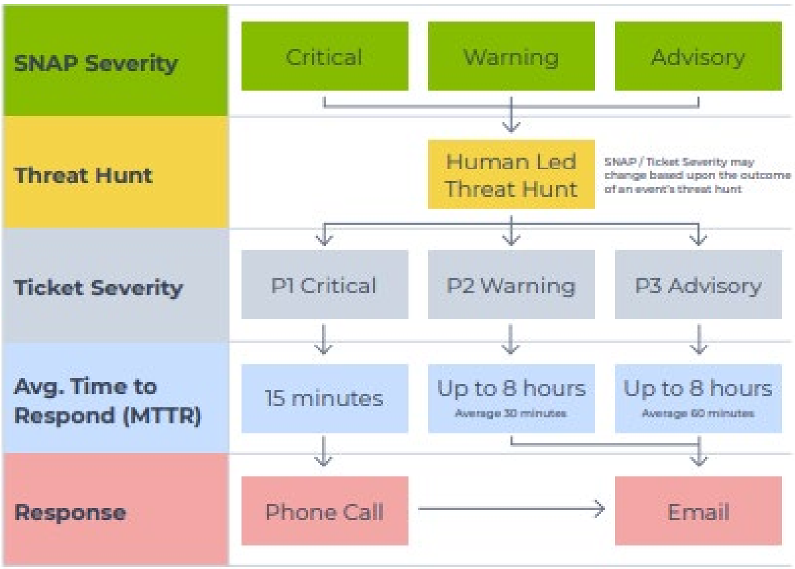
Our Imagis SOC team can be reached 24/7/365 via the phone number or email address below. Your team will always be able to reach a live security analyst regarding an incident.

4.2 SERVICE LEVEL OBJECTIVES

The Imagis SOC follows our SLO. The malicious behavior the Imagis SOC hunts for does not always materialize in a way that we can ensure a set, promised reaction time. Imagis SOC's MDR technology, SNAP-Defense, detects malicious behavior and alerts the Imagis SOC. This alert triggers an investigation and the need for threat hunting. Our SLO guides our Imagis SOC when responding to alerts and incidents.

It includes the following:

- For critical alerts, the Tier 1 analyst must conduct initial alert triage, investigation, and threat hunting tactics within 15 minutes.
- If an alert is deemed a false-positive, the Tier 1 analyst can escalate to the senior team (Tier 2 and Tier 3 analysts), suggesting suppression or resolution.
- If an alert is deemed a true positive, the Tier 1 analyst will escalate the alert as an incident to the senior team. For critical alerts, the senior team has an additional 15 minutes from the time an incident was created to investigate, threat hunt, and respond to contain the threat(s).



TICKET PRIORITIES

Priority	Severity	Definition	*MTTR	Example
1	**Critical**	Malicious event that we responded to or needs customer action	15 min	We see an infected device trying to laterally spread on the network and have detained the machine
2	**Warning**	An event we need more information or verification on	Up to 8 hours	We saw a suspicious process run but did not see any malicious events
3	**Advisory**	A non-malicious event that requires actions	Up to 8 hours	The following device does not have a SNAP agent and performed a privileged action or had an A/V event we are unable to fully investigate

* Mean Time to Respond

4.3 SCOPE OF SERVICES

MANAGED DETECTION AND RESPONSE (MDR)

Imagis SOC MDR analysts will triage all alerts and the involved devices, reviewing created processes, network connections, and currently running processes.

Further investigation of other data may occur depending on analysis during the triaging phase. Imagis SOC will reach out to the client to verify suspicious activity and tools to ensure they are known and authorized. If malicious activity is observed, the Imagis SOC will isolate impacted machines and mitigate the threat.

The client is called after the threat has been mitigated, will be informed of the incident, and provided follow-up recommendations. The Imagis SOC will provide an IR Report containing the timeline, devices involved, accounts involved, processes observed, indicators of compromise, and post-incident actions for Imagis to take.

The Imagis SOC is responsible for triaging and investigating all alerts triggered within SNAP-Defense. The Imagis SOC is staffed 24/7/365 to fulfill this requirement. These alerts will be escalated and resolved according to their findings.

Combining leading Managed Detection and Response with the integration of third-party endpoint security solutions enables our capabilities to surpass visibility. We also quickly and effectively remediate attacks by ingesting the solution’s alerts and device metadata, triaging threats, and closing the gap on detection. When malicious activity is triggered from a third-party solution, Imagis SOC can respond immediately.

Windows Devices

- Device Isolation: The device is not able to communicate to the network and nothing is able to communicate to it. The only exception to this is the agent required to retain SNAP-Defense connectivity, allowing the Imagis SOC to monitor the isolated device during an active incident.
- **Device Un-Isolate:** Device isolation can be lifted after isolation.
- **Scheduled Tasks:** The SOC can disable, delete, and restore Scheduled Tasks if deemed malicious.

Mac Devices

- **Device Isolation:** The device is not able to communicate to the network and nothing is able to communicate to it. The only exception to this is the agent required to retain SNAP-Defense connectivity, allowing the Imagis SOC to monitor the isolated device during an active incident.
- **Device Un-Isolate:** Device isolation can be lifted after isolation.

SNAP DEFENSE AGENTS

As a primary component of Imagis' MDR service, it detects advanced cyberthreats in real time and offers live asset visibility and awareness. Imagis utilizes a lightweight software agent (referred to as the SNAP agent) deployed to compatible endpoints. It has live network mapping, visualization, and actionable alerts. Additionally, SNAP-Defense provides an active response capability, allowing our security analysts to respond to cyberattacks around the clock.

MDR AGENT DATA COLLECTION

When a third-party AV/EDR solution is set up, the IMAGIS SOC Imagis SOC will review and investigate alerts produced by the tool. If an alert is resolved by the Imagis SOC in SNAP-Defense, there is no action required for the client. If an alert is escalated to the client, it will include remediation guidance.

The SNAP agent collects system metadata, which is sent to Imagis SOC's cloud for processing. The following types of metadata are collected by the SNAP agent:

- System Event Logs
- Running Processes
- Services
- User Account Information
- Network Interfaces
- Hostnames
- IP Addresses
- Scheduled Tasks
- ARP (Address Resolution Protocol)
- Network Connections (Processes)
- Network Share

BLOCK RULES

Notifications for rules in Curated Block Rules and Custom Block Rules can be enabled so that when a blocked or monitored application tries to execute, the partner receives a notification via email, and within their events portal.

All applications blocked through the Curated Block Rules list will create an alert for the Imagis SOC. The Imagis SOC will always contact the partner via email and may additionally call them if malicious activity is uncovered during the threat hunting process, as well as if there are loud or noisy false positives.

Categories within the Curated Block Rules list include:

- RMM
- Reconnaissance
- Remote Access
- Ransomware Operator Tools
- Pen testing
- Defense Evasion
- Lateral Movement
- Credential Access
- Exfiltration
- C2

RANSOMWARE RESPONSE

Ransomware Response is an automated functionality built into the SNAP agent, delivering a last line of defense against ransomware. If ransomware behavior is detected on the system, Ransomware Response will suspend the malicious process and alert the Imagis SOC team.

Capabilities include automatic suspension of the parent process executing ransomware and the manual ability for the Imagis SOC to resume execution of parent process. This allows Imagis SOC to stop drive-by click-based attacks that occur within seconds.

CLOUD RESPONSE OPERATIONS

Cloud Response extends MDR into Microsoft 365 and Google Workspace environments. Imagis SOC provides active monitoring and unified response across cloud services, including all associated applications, data, and settings. Cloud Response allows the 24/7 SOC to view contextual data within the cloud environment and respond immediately to anomalous behavior. Custom policies can be set up to implement cyber hygiene processes across all users and monitor events through custom notifications.

Microsoft 365 Through Cloud Response

- Disable User Account: An abused user account can be disabled and have all associated tokens expired to prevent further abuse.
- Disable External Mail Forward Rule: A rule forwarding a user's emails to an external source can be disabled by the SOC to minimize damage.
- Disable Enterprise Application: If an Enterprise Application is determined to be malicious, it can be disabled.

Google Workspace Through Cloud Response

- Login from Unapproved Country: A user signs in from a country not on the approved list.
- Suspicious Login: A login is flagged as suspicious by our analytics engine. This could be due to successful logins from TOR, risky countries, malicious VPN usage, or anomalous residential proxy usage.
- Suspicious Email Filtering Rule Created: An email filter rule that is flagged as suspicious by our analytics engine.
- External Email Forwarding Rule Created: A new email forward rule is created that sends mail to a mailbox outside your organization.
- Ability to disable a Google Account

4.4 RESPONSIBILITIES

CLIENT RESPONSIBILITIES

The client is responsible for the following actions:

- Notify Imagis of approved countries for their end users.
- Maintain updated contact information for the Imagis SOC in Business Continuity and Incident Response policies.
- Review and audit mandatory and selected notifications.
- Perform post-incident actions and recommendations to restore business operations and reduce future risk.

- Clients must notify Imagis of any planned international travel using the travel notice template provided by Imagis **at least 48 hours in advance of planned travel**. This notice should include all countries you will visit or pass through if you intend to use a laptop or mobile device that accesses organizational resources. It is important to list each destination to ensure appropriate security measures are in place.
- The client must keep their Approved Countries list up to date. If it is not, they may be potentially unnecessary account disablements.

Note: Setting up approved countries does not mean it limits what countries a Microsoft 365 user can log into from. It only designates which alerts will be sent out via an automated email or Imagis SOC alert.

IMAGIS SOC RESPONSIBILITIES

The setup and configuration of Cloud Response is Imagis' responsibility. This includes connecting the Microsoft 365 tenant, selecting authorized countries, adjusting policies to best practice recommendations, and configuring alerts. Cloud Response will send automated notifications to the Imagis team based on the preferences set up for activity verification. The Imagis SOC team will be alerted to and will investigate logins from proxies, Tor, suspicious user agents, and/or risky countries. Consideration of these factors, along with previous user activity, previously detected events, and geopolitical research may result in the SOC taking action and disabling the account.

The SOC will follow up with an Incident Response (IR) Report containing the timeline, devices involved, accounts involved, processes observed, indicators of compromise, and post-incident actions for Imagis to take. If the only suspicious indicator is the use of a VPN, a notification will be sent to the customer regardless of their notification settings for the first-time usage from a user.

Incident response Reports

After the Imagis SOC identifies, responds to, and stops an attack, the related client will be sent an **Incident Response (IR) report** via the email in the contact profile. IR Reports are not created for any false positives or zero-impact security alerts.

The IR Report will include the following details:

- A summary
- Specific times of events
- Devices* and accounts involved
- Binary names*
- Commands seen*
- Installed security products*
- Indicators of compromise
- Ticket information
- Post-incident actions

*These items are included on MDR IR reports, not Cloud Response IR reports. The client can expect a detailed IR report within twenty-four (24) hours after the Imagis SOC responds to a threat.

The Imagis SOC is responsible for identifying malicious activity, responding to attacks, and providing relevant information to the client. Therefore, each report will include post-incident remediation actions.

4.5 SERVICE EXCLUSIONS

Change requests or enhancements not explicitly listed in the scope of services will be considered out of scope and may incur additional charges. This includes support for outdated software and hardware, personal devices, and network re-architecting or redesigning. Such requests will be billed separately under a block hour agreement.
How-to based requests will be handled on a best-effort basis for these systems. Recommendations for third-party vendors or products may be made if best-effort work is not applicable.

The following services are outside the scope of our offerings:

ALERTING

The Imagis SOC is not alerted to user sign-in activity if the country is whitelisted.

The geolocation information in Cloud Response alerts may not match up to similar reporting from another tool. For example, you may see a different IP address location in an event produced by Cloud Response compared to an event produced by Microsoft Identity Protection. This is expected at times due to the geolocation service. Therefore, these events should always be reviewed by the partner to ensure the sign-in activity is expected and from a legitimate use.

5. SERVICE DESCRIPTION: VULNERABILITY MANAGEMENT

5.1 HOURS OF OPERATION

- Vulnerability scanning is performed on managed endpoints daily once every 24 hours.
- Remediation services are a combination of automatic remediation for patches and fixes that can be auto applied through the vulnerability management solution as well as manual remediation performed by an Imagis engineer.
- Manual remediation occurs once per calendar month.

5.2 SERVICE LEVEL OBJECTIVES

Ticket Priority	Time to In Progress	Goal %
Priority 1 - Critical	15 days	80%
Priority 2 - High	30 days	80%
Priority 3 - Medium	60 days	80%
Priority 4 – Low, no information	N/A	N/A

Note: These objectives apply solely if a fix is available from the software provider. Vulnerabilities may reappear with a lower CVSS score following the acquisition of further intelligence, which depends on the CVSS database, the vulnerability scanning tool, and the exploitability of the vulnerability.

PRIORITY/SEVERITY RATINGS

In the effort to quickly remediate security vulnerabilities, findings should be prioritized based on the severity level.

Priority Level

Critical

- **CVSS Score:** Critical patches where the patched vulnerability has a CVSS score of 9.0 or higher. They can be readily compromised with publicly available malware or exploits.
- **Definition:** Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allow remote code execution, financial theft, unauthorized access to/extraction of sensitive data, etc.
- **Examples:** Vulnerabilities that result in Remote Code Execution such as Vertical Authentication bypass, SSRF, XXE, SQL Injection, User authentication bypass.

High

- CVSS Score: High-severity patches where the patched vulnerability has a CVSS score of 7.0-8.9.
- Definition: Vulnerabilities that depend on known public impact malware or exploit available.
- Examples: Lateral authentication affects the security of the bypass, Stored XSS, platform including the some CSRF processes it supports.

Medium

- CVSS Score: Medium-severity patches where the patched vulnerability has a CVSS score of 6.0-6.9.
- Definition: Vulnerabilities that have little or no impact on multiple users and can be user interaction to mitigated within an extended trigger time frame.
- Examples: Reflective XSS, Direct object reference, URL Redirect, some CSRF depending on impact.

Low

- CVSS Score: Low-severity patches where the patched vulnerability has a CVSS score of 4.0 to 5.9.
- Definition: Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. Issues that affect singular users and require interaction or significant prerequisites (MitM) to trigger.
- Examples: Common flaws, Debug information, Mixed Content

Informational

- CVSS Score: Information patches where the patched vulnerability has a CVSS score lower Issues that do not affect than 4.0.
- Definition: These are users but are considered risks but bugs in the system that cannot be exploited but reference might be important as an information for the reference information state and configuration of an asset.
- Examples: Minor bugs or functionality issues

In the case a severity priority or rating level is updated after the initial finding was already created, or due to partial remediation, the assignee can upgrade or downgrade level to match the CVSS severity rating.

5.3 SCOPE OF SERVICES

Our comprehensive Vulnerability Management solution includes the following scope of services:

- Daily External and Internal Vulnerability Scanning to identify and prioritize potential threats and weaknesses in your network.
- Prioritization and classification of vulnerabilities based on their CVSS scores, allowing us to focus our efforts on the most critical vulnerabilities first.
- Remediation of known vulnerabilities with available patches, following your organization's policies and procedures to minimize the risk of exploitation by malicious actors.
- Monthly Reporting, providing a clear and concise overview of identified vulnerabilities, remediation progress, and any recommendations for further improvement.

Remediation Services May Include the following:

- Patching Operating Systems to address known vulnerabilities and reduce the risk of exploitation by malicious actors.
- Patching 3rd party software, ensuring that all software applications are updated with the latest security patches to minimize vulnerabilities and improve your overall security posture.
- Configuration or policy changes for Azure, Intune, scripts, and Network devices, to address any misconfigurations or vulnerabilities that may exist in your systems.

Reporting a finding

- Upon identification of vulnerability (including vulnerability in software, OS patching level or process) a ticket is created in automated way.
- The description of the findings should include further details, without confidential information and a link to the source.
- The finding will be given the same urgency and priority level as defined in scanning solution.

Resolving a finding

- The finding should be assigned to a specific member of Engineering team
- A change request should be created and approved in accordance with the Change Management policy if resolving a finding requires configuration changes
- Remediation actions will be taken in accordance with internal documentation and patching policy (above) for most common use cases or as the Engineering team sees fit to resolve in a timely and secure manner.
- The finding may be resolved by:
- Providing a valid fix/mitigation
- Determining as a false positive
- Documenting an approved exception

Closing a Finding

- The assignee should provide a valid resolution (as defined in previous section) and add a comment to the ticket connected to the finding

Apart from the vulnerabilities discovered by the vulnerability scanning system, the Engineering team might identify vulnerabilities during regular security and configuration checks of internal systems. In that case the same steps from the policy apply, and it should be properly tracked in a ticketing system, remediated, and closed.

Exceptions

- An exception may be requested when a viable or direct fix to a vulnerability is not available. For example, a version of the patch contains the fix that is opening other issues or instability to the system or operating system
- An alternative solution must be in place to address the original vulnerability such that the risk is mitigated. The compensating control may be technical or process or a combination of both
- False Positives arise when the vulnerability scanning solution identifies the endpoint as vulnerable, when it is not. This can occur because of the software version numbers or some applications updated the issue without updating the version so the scanning solution can not recognize it.
- Exception must be recorded in the ticket and internal documentation
- Each exception must be reviewed and approved by the Cloud Operations Security Manager

Assets are counted as any device with an agent, or a device discovered/scanned with an IP address (may include printers, servers, workstations, switches, access points, firewalls, etc….). External scans would count as one asset per public IP address.

5.4 RESPONSIBILITIES

CLIENT RESPONSIBILITIES

Remediation may include manual work on the workstation or server and can cause downtime, which must be approved by the client. The client is responsible for:

- Coordinating and approving any necessary downtime associated with remediation efforts. This ensures that any disruption to business operations is minimized and adequately planned for.
- Participating in updating or removing vulnerable software. This involves collaborating with Imagis engineers to identify and implement suitable alternatives if necessary.
- Ensuring that any software acquired or utilized does not contain known unfixable vulnerabilities or is not at the end-of-life/end-of-support stage, where upgrades and patches are no longer being released. This requires staying informed about the software lifecycle and making prudent decisions regarding software procurement and usage.

IMAGIS RESPONSIBILITIES

- **Monitor the findings:** Continuously scan and monitor the network and systems for any newly discovered vulnerabilities. This includes regular updates and enhancements to the monitoring tools and methodologies to ensure up-to-date threat detection.
- **Prioritize and categorize vulnerabilities:** Assess all identified vulnerabilities based on their severity, potential impact, and exploitability. Use threat intelligence and the CVSS (Common Vulnerability Scoring System) to prioritize vulnerabilities that need immediate attention and categorization into high, medium, or low-risk levels.
- **Act on remediating the fixable vulnerabilities:** Work collaboratively with the client to implement remediation measures for vulnerabilities that have available fixes. This process involves applying patches, updating configurations, and, if necessary, performing manual interventions. Ensure that any actions taken are thoroughly documented and communicated with the client to minimize disruption and downtime.

5.5 SERVICE EXCLUSIONS

Change requests or enhancements not explicitly listed in the scope of services will be considered out of scope and may incur additional charges. This includes support for outdated software and hardware, personal devices, and network re-architecting or redesigning. Such requests will be billed separately under a block hour agreement.
How-to based requests will be handled on a best-effort basis for these systems. Recommendations for third-party vendors or products may be made if best-effort work is not applicable.

The following services are outside the scope of our offerings:

HARDWARE UPGRADES

The scope of services does not include the physical upgrading or replacement of client hardware such as servers, workstations, or networking equipment. While Imagis can provide recommendations and guidance on necessary hardware upgrades, the actual procurement, installation, and configuration of new hardware must be managed and executed by the client or a third-party vendor. Additionally, any downtime associated with hardware changes will need to be coordinated and approved by the client.

DISCLOSURE OF THREAT INTELLIGENCE SOURCES

Imagis utilizes a variety of proprietary and third-party threat intelligence sources to prioritize and categorize vulnerabilities. Disclosure of these sources is not included within the scope of services provided. While Imagis ensures the efficacy and reliability of the threat intelligence used, the specific sources and methodologies employed will remain confidential to protect the integrity of our threat detection and mitigation processes.

CONFIGURATION CHANGES

Configuration changes that are out of scope include, but are not limited to, software code modifications, application-specific settings alterations, or adjustments to assets not managed by Imagis, such as personal printers, home Wi-Fi networks, and other non-corporate devices.

OUT-OF-SCOPE CHANGE REQUESTS

Change requests or enhancements not explicitly listed in the scope of services will be considered out of scope and may incur additional charges. This includes support for outdated software and hardware, personal devices, and network re-architecting or redesigning. Such requests will be billed separately under a block hour agreement.

6. GENERAL CLIENT RESPONSIBILITIES

STANDARD OPERATING PROCEDURES

Client will provide complete standard operating procedures and processes for any systems already in place. This includes preferred incident, problem, and change management resolution processes and escalation information needed.

NOTIFICATION OF CHANGES

Client will inform the Imagis team of changes relative to the monitoring operation, including but not limited to emergency maintenance and/or planned outages in a timely fashion. Lack of proper notification in a timely manner will excuse NOC from their service levels until the changes can be incorporated into the environment and staff can be trained.

NEW TECHNOLOGY INTRODUCTION

The introduction of a client-approved new technology, which will alter the staff's technical skill requirements, may require a change to ensure that staff have the technical training to adequately perform their job function.

NOTIFICATION OF PERSONNEL ACTIVITIES

Client will promptly notify Imagis of all Imagis personnel activities which require the attention of Imagis.

VENDOR SUPPORT CONTRACTS

Client will ensure that vendor support contracts are in place for equipment and software supported by this agreement which continually generates an irregular level of alerts. If a vendor support contract is not in place, Imagis reserves the right to:

- Remove the item from being monitored
- Reduce the processes being monitored to include only those actionable
- Increase the price to reflect the increased number of alerts from the device or application

USER ACCESS RIGHTS AND PRIVILEGES

Client will be responsible for authorizing all user requests for access rights and privileges.

REMOTE ACCESS

Client will provide Imagis with remote access to Client systems as required to deliver services identified in this Service. When given access through remote facilities to any Server or Client computer or electronic data processing system to provide the managed services as described in this Service, Imagis will limit such access to activities related to those outlined in the Order.

7. REPORTING AND REMEDIES

REPORTING

Upon client's written request, Imagis shall make available to client service reports that illustrate the response times for service requests generated during a specific period. If the service level objectives are not met for a given month, Imagis will provide a report to the client describing the timeframe and the reason (if known) in which the uptime requirement was not met.

REMEDIES

If Imagis fails to meet the service level objectives outlined within this agreement, then, upon written request from the client, Imagis may issue a credit, as the sole and exclusive remedy under this agreement, in an amount equal to the percentage of the service fee by which the service level objective was not met within a 30 day period.

Example: If Imagis met a 75% average response time for last month with a target response time objective of 80%, credit would be issued for a 5% difference.

Remedies under this section shall apply only to the following fees:

- Managed Services User and Managed Server fees related to the services covered by this agreement.

Said remedies shall not apply to, and no credits will be issued for:

- Licensing

- Subscriptions
- Hardware
- Cloud hosting, or Cloud management fees.
- Managed Locations
- Security (SOC) Services
- Vulnerability Management

Credits are issued at the sole discretion of Imagis. Any such credits must be requested **no later than 30 days after the month of service** during which Imagis has failed to meet the service level objectives. Account credit will automatically be applied to future invoices and may not be redeemed for cash. No credit issuance may exceed 100% of the monthly charges for any affected services.

8. FEEDBACK MECHANISMS AND QUALITY ASSURANCE

At Imagis, we value our clients' feedback as it helps us continuously improve our services. We have established several mechanisms to ensure that your feedback is heard and acted upon promptly:

CLIENT SATISFACTION SURVEYS

After the resolution of each service request, clients will receive a satisfaction survey. This survey allows clients to rate their experience and provide comments on the service received. The feedback from these surveys is reviewed daily by our Service Manager and Client Success Manager to identify areas for improvement and to address any concerns.

QUALITY ASSURANCE AUDITS

All service interactions are logged, and support calls may be recorded for quality assurance purposes, stored for up to 90 days. The Service Manager will perform the following activities to ensure service quality and continuity:

- Review ticket surveys daily, actioning items that require follow-up or remediation
- Randomly pull a sampling of call recordings and service tickets
- Investigate and measure any reporting quality incidents
- Review SLA performance results
- Ensure each reported incident adheres to process and protocol including
    - Ticket notation requirements
    - Ticket handling procedures
    - Appropriate usage of support tools
    - Overall customer service experience

MONTHLY REPORTING

Upon client request, Imagis will provide monthly service desk reports that show data and trends of the previous month’s ticket data. The dedicated Client Success Manager is available to review the reports with the client upon request.

Monthly reports include information on the following:

- SLA Adherence
- Time to Response
- Time to in Progress
- Time to Resolution
- Breakdown of tickets by type, subtype, and item

- Counts of tickets submitted by each user
- Number of opened and closed support tickets
- Count of tickets submitted afterhours
- Assets with expired warranties
- Warranty expirations within the next 6 months

9. KEY TERMS & DEFINITIONS

- **Service Provider** – The company (Imagis) responsible for delivering the agreed-upon services.
- **Client** – The entity receiving services under this agreement.
- **Service Availability** – The percentage of time services are operational and accessible to the client.
- **Response Time** – The timeframe within which the service provider acknowledges a reported issue.
- **Resolution Time** – The timeframe within which the service provider aims to resolve an issue.
- **Incident** – Any event that disrupts normal service operations, requiring intervention.
- **Severity Levels** – A classification system for incidents (e.g., Critical, High, Medium, Low) based on impact and urgency.
- **Escalation Procedure** – The process for escalating unresolved issues to higher support levels or management.
- **Service Request** – A non-incident request for assistance, such as account setup or system access changes.
- **Business Hours** – The designated hours during which standard support services are provided.
- **Key Performance Indicators (KPIs)** – Metrics used to measure service effectiveness, such as uptime and response times.
- **Escalation Point of Contact** – The designated personnel or team responsible for handling escalated issues.
- **Service Credits** – Compensation (if applicable) for failure to meet service level commitments.
- **Planned Maintenance** – Scheduled maintenance that may temporarily impact service availability, communicated in advance.
- **Scheduled Downtime: Defined as maintenance hours documented in the client's Maintenance Policy document or downtime scheduled and approved in writing by the client via email or service ticket request.**
- **Unplanned Downtime** – Any unexpected service outage that affects availability.
- **Client-Side Downtime: Any downtime caused by the client's actions, omissions or any third-party agent acting on the client's behalf.**
- **Startup Period:** The first thirty (30) days after any services have been provisioned may have unanticipated down or delays to the initial necessary onboarding activities.
- **Initial Response Time** is defined as the total time from when the service request is created until an engineer is assigned to the ticket.
- **Service Exclusions:** This term lists the services that are outside the scope of the agreement
- **Priority Response Model:** This term describes a tiered response model designed to prioritize and address critical NOC events
- **Force Majeure Event:** An unforeseen and unavoidable circumstance that prevents one or both parties from fulfilling their contractual obligations. In the context of an SLA, it includes events beyond reasonable control, including but not limited to:
  - **Natural Disasters** – Earthquakes, floods, hurricanes, or other extreme weather events.
  - **Government Actions** – Laws, regulations, or restrictions that impact service delivery.

- **Acts of War or Terrorism** – Conflicts, hostilities, or cyberattacks affecting operations.
- **Labor Strikes or Industrial Disruptions** – Widespread workforce disruptions beyond the provider's control.
- **Power or Utility Failures** – Extended outages not caused by the service provider.
- **Pandemics or Public Health Emergencies** – Events causing widespread business disruptions.