IT Eagle Eye

Managed Services Description

This Agreement between IT Eagle Eye and the Client for Managed Security Services was developed based on the following dependencies and assumptions, which if not accurate or adhered to, may require a change in the scope of services. Any change in service or fees will be mutually agreed to in writing by both parties.

1. Service Provision
    a. IT Eagle Eye shall not begin to provide the Services as described in the Order Form until Client has returned a signed Order Form. If a new payment account is being utilized for the purchase, a Payment Authorization Form is also required prior to the start of the Services.
    b. The Service Level Agreements (SLA) for the Managed Security Services described herein, which are incorporated into this Agreement and include commitments with respect to certain availability of those Managed Security Services are set forth at https://iteagleeye.com/legal/terms-of-service. To the extent that there are any inconsistencies between this Service Description and the SLA posted for the Services hereunder, the Service Descriptions posted in this document will apply.
    c. ITEE Managed Services provide a fully managed service with 24/7/365 security monitoring, health and availability monitoring, backup and restore, configuration management, vulnerability management, change management, and incident management where applicable.
2. Scope of Services
    a. Device Management
        i. Unless otherwise agreed upon in accordance with the Co-Management Clause of this Agreement, ITEE shall be the sole manager of the Device covered by the Service. Device refers to any computer equipment, hypervisor, virtual machine, cloud server, virtual appliance, or accepted security device whose enrollment under a Managed Security Service plan has been accepted by ITEE.
    b. Co-Management
        i. Co-Management is available as an account level option It may be added by Client election and payment of an additional fee. The co-management fee applies to all services under the client account.
        ii. Configuration item availability (Service Level Agreement) is not applicable.
        iii. Configuration Item configuration and policy changes to be completed by ITEE can only be made by raising a Request for Change (RFC) via the Account Management Center.
        iv. Access to configuration items must be limited in accordance with the Remote Access clause of this agreement.

v. Client must notify ITEE in advance of changes being made, to include scheduling and scope of changes being made, to avoid 'lost transaction' or collision of change work.
vi. Any changes done by the Client without prior notification to the change may cause initiation of an incident investigation. All time utilized for this investigation will be billed to Client as Service Credits. A minimum charge of twenty (20) Service Credits will apply per incident. If Co-Management Service has not been enabled on the account, Service Credits included in the Services may not be used.
vii. All modifications made by the Client must be recorded in the Account Management Center by entering a Notification of Change (NFC).
viii. Upon completion of a configuration or policy change, the Client must provide a report or status from their internal change management process to verify all completed changes to configuration item(s).
ix. Client must make changes to configuration items such that there is a clear audit trail indicating the party responsible for the change, the date of the change, and your change control identification.
x. Any change made by the Client must be made in such a way as to provide the possibility of rolling back to the previous version. Failure to do this may render it impossible to recover the previous settings and data if problems occur. Client accepts full liability, damage, and loss from configuration changes.
xi. Any changes that impact the service administration must be agreed upon in writing by ITEE prior to implementation.
xii. All work resulting from Client changes to configurations or policies will be billed as Service Credits. The minimum amount billed per incident is twenty (20) Service Credits. If Co-Management Service has not been enabled on the account, Service Credits included in the Services may not be used.
xiii. The Co-Management election may only be changed on an annual basis with a minimum of thirty (30) days of notice prior to the anniversary date of the election.

c. Standard Maintenance
i. ITEE will perform Standard Maintenance during a scheduled maintenance period. Unless otherwise requested by the Client and accepted by ITEE in writing, the maintenance period will last from 7:00 PM EDT to 9:00 PM EDT or from 7:00 AM EDT to 9:00 AM EDT daily. The elected maintenance period will be identified on the Order Form.
ii. Standard Maintenance, including security patches, updates, and requested changes will be done without specific notification by ITEE to the Client when the maintenance is done during the maintenance window and any expected outage or limitation is expected to last less than five (5) minutes.
iii. When Standard Maintenance is scheduled and access or performance of the Device is expected to be limited for more than five (5) minutes, ITEE will send notification to the Client of the upcoming maintenance work and any related Service interruptions and their anticipated durations.

d. Emergency Maintenance
    i. During cases of Emergency Maintenance, ITEE will use its best efforts to minimize the duration of any disruption to the Service. Emergency Maintenance means any non-scheduled, non-standard maintenance required by ITEE.
    ii. ITEE is relieved of its obligations under the applicable Service Level Agreement for the duration of any Emergency Maintenance and the Client expressly excludes ITEE for any liability, loss, or damage suffered during Emergency Maintenance.
    iii. In cases of Emergency Maintenance, ITEE will endeavor to provide the Client with as much notice as is reasonably practicable in the circumstances. Client acknowledges that in order to minimize Service disruption, no prior notice may be provided.
e. Configuration Management
    i. Change Control
        1. All change requests and change request approvals must be submitted to ITEE directly by authorized users in the Account Management Center.
        2. A history of all change requests is retained including the requestor, request time and date, and change requested. The date and time of the requested change implementation is also recorded.
        3. When a Managed Security Service includes a Compliance election, ITEE will also record the request approver, time of approval, and up to two additional custom details upon Client request.
        4. Change Control records are kept for a minimum of 60 days following the termination of the Service. Additional retention times may be available as a plan upgrade upon request.
        5. Requests for Changes may be cancelled with no penalty up to four (4) hours before any scheduled changes are committed to occur. Cancellations that are less than four (4) hours before the scheduled change will be charged a service fee in the amount of 25% of the estimated Service Credits to complete the change. Reversals to changes that are in progress or completed must be entered as a new Request for Change.
        6. Records are available to be sent to Client upon request and payment of a records fee.
    ii. Configuration Item Control
        1. Managed configuration includes continuous system evaluation against defined configuration standards. This includes checks for installed applications, configuration settings, and configuration files.
        2. ITEE will maintain a Record of Entitlements for each applicable Device and use this Record as a basis for configuration enforcement.
        3. Additional software configuration checks are available when Managed DevOps Security Service is used in conjunction with Device that is covered under a Managed Technology Security Service.

iii. Compliance Control
    1. When Compliance Services is included in a Managed Technology plan, the Service is extended to include robust monitoring to enforce compliance standards for multiple regulations and standards, including ISO 27000, HIPAA, PCI, and NIST using automated tools.
    2. Ongoing monitoring prevents compliance drift and provides automated remediation routines to enforce approved security policies on Devices covered under the Service.
    3. Event driven automation enforces compliance policies and creates incidents for further investigation by an ITEE SOC Engineer.

f. Patch Management
    i. ITEE monitors Original Equipment Manufacturer (OEM) published patches, security hotfixes, and version updates (Patches) associated with covered configuration items. Patches are reviewed for applicability to covered systems.
    ii. When applicable, any covered Patches that do not involve a major version update, will be installed automatically as a part of Standard Maintenance.
    iii. An unlimited number of qualified and applicable software patches and minor version upgrades for covered configuration items is included in all security management plans.
    iv. Patches are identified through monitoring of OEM provided mailing lists, security watch lists, and daily review of conglomerate security news sites. In addition, weekly direct checks of OEM repositories for published Patches are performed.
    v. Patches are reviewed and applied to covered Devices according on the following scheduled based on their plan type.

PLAN TYPE	CRITICAL PATCH	STANDARD PATCH
Standard	7 Days	30 Days
Compliance	72 Hours	14 Days
Development	14 Days	30 Days

    vi. Patches are determined to be Critical when their CVSS score is ranked high or above for a covered Device. Devices that do not have compensating security measures or protect sensitive data are prioritized for Patch application. When the security vulnerability is not exploitable due to other security measures or configuration, then a Critical Patch may be downgraded to a Standard Patch.
    vii. In the event that a Patch is not available within 30 days for an identified security vulnerability, ITEE may recommend additional compensating controls be applied to mitigate security risk. Application of compensating controls will be completed as a Request with Client Approval. Client acknowledges that the recommendations of ITEE are to reduce the risk of exploitation and may not fully remove the risk associated with any known vulnerability.

viii. Patches may be applied to covered Devices through direct manual interaction or through automated processes. Automated updates are scheduled, pushed, and verified using the itee-controller software package when applicable.
ix. Patch installation is verified on a weekly basis on all covered Devices.
x. Any Patch that is suspected to contain breaking changes is handled in accordance with Version Management.

g. Incident Management
   i. Incident Management refers to the detection and handling of monitored events. Events refer to any systematic detection or correlation of one or more logs that that identify activities of interest on a Device included in the Service.
   ii. Incidents are managed based on the ITIL best practices for Incident Management. Throughout the entire Incident Management Lifecycle, the priority is to minimize negative impact and restore normal operating functions.
      1. Logging: Incidents may be generated by the health and availability monitoring, the ITEE SOC, or by direct submission of an incident request by the Client.
         a. Client may submit a request to ITEE via email or ticket submission in the Account Management Center.
         b. Email submissions must come from an email address on file for an authorized contact.
         c. Emergency incidents may only be submitted by ticket in the Account Management Portal.
      2. Prioritization: After an incident has been logged, the ITEE SOC will triage the incident to assess the priority. Priority will be designated as Emergency, Standard, or Low, depending on the service impact of the request. Client may submit an incident request with a designated priority, but ITEE retains the right to downgrade the priority based the assessed impact. Incidents are then assigned to an appropriate SOC engineer for further investigation and analysis.
      3. Investigation: Incidents will be worked on according to priority and availability. An initial assessment of the incident will be completed to determine if a solution can be enacted to resolve the incident or if further communication and investigation is warranted. When a resolution requires only steps that can be completed without a Change Control process and may be implemented in less than one hour, Client authorizes ITEE to proceed without notification in order to expedite incident resolution. Client acknowledges that this ability to promptly remediate incidents prior to communication is essential to reduce the negative impact of incidents and authorizes ITEE to take such action.
      4. Communication: A SOC Engineer will communicate with the Client concerning the results of the analysis and any steps that have been or will be taken to resolve the incident. Further information may be requested from the Client in order to complete the investigation of the

incident. Client is responsible for answering all questions and requests in a timely manner in order to resolve the incident. ITEE bears no liability and the SLA does not apply if Client fails to respond promptly to these requests.

5. Resolution: Once a potential solution to the event has been identified and provided to the client, the remediation of the event will take place immediately or as scheduled with the Client. Steps requiring change control will be undergo the required approval process unless the event has been designated as an Emergency.
6. Review: Client will be informed of the incident resolved status. It is the responsibility of Client to review and test the solution.
    a. Incidents that are related to a security breach are reported on a Security Incident Report. This report will be available to the Client within 15 business days of the incident in the Account Management Center.
    b. If the incident is determined to be a Request or Project, it will be charged to the client under the applicable billing process.
7. Closure: Following Client confirmation of the resolution, the incident will be closed. If Client fails to respond or provide further notice of ongoing issues, the incident may be automatically marked as closed after a period of forty eight (48) hours.

iii. Incidents that involve Third Party Providers are not covered under the Service. Any incident that is caused by a change or loss in functionality of a Third Party Provider will be billed to the Client as a Request or as a Professional Services Engagement, in the sole discretion of ITEE, based on the necessary time to complete any incident remediation activities, including assessment, analysis, implementation, and monitoring of the event. Professional Services Engagement refers to any requested or required work to be completed by ITEE that is not covered under a Managed Security Service. Professional Services Engagements are not eligible to use Service Credits that are included with Managed Security Services.

h. Request Management
    i. Request Management refers to the flexible model for managing and executing the moving, adding, changing, and removing of hardware and software configuration on a device. It also includes technical requests for information, advice, or access, including by not limited to, requests concerning performance, configuration, or other aspects of configuration items.
    ii. Requests must be able to be performed remotely. If an on-site task is required to complete a Request, additional charges will apply.
    iii. A Request that takes more than two (2) hours to complete by an appropriately skilled engineer may, at the sole discretion of ITEE, be classified as a separately billable Professional Services Engagement. The time to complete may be the time to perform necessary task(s) on a single device or the cumulative time to

perform the same necessary task(s) on multiple devices. These engagements will not be considered a Request and the SLA under the Service is not applicable.

iv. Requests must relate directly Devices supported under a Managed Security Service. Any work that is requested for an asset that is not covered under the Service will be billed as a Professional Services Engagement and no SLA is applicable.

v. Standard Requests may be raised by the Client via the Account Management Center or via email to customersupport@iteagleeye.com. Emergency Requests may only be raised via the Account Management Center.

vi. ITEE will managed the execution of Requests by authorized representatives. Requests are administered through a service credit system where Service Credits are purchased in advance and then deducted in the execution of Requests. If Client exhausts the number of Service Credits included in the Service(s), Client shall be obliged to purchase additional Service Credits at the then-current applicable rate.

vii. Requests will be completed in accordance with the applicable SLA.

viii. Requests that must be completed within a shorter time period than provided by the SLA will be executed based on availability. If any Request that must be completed outside of business hours or within a time period that is less than what is provided for in the SLA, the Request will be considered a Rushed Request. For these Rushed Requests, an uplift factor is applied vs standard charges. The applicable uplift factor is based on the table below. Client's designation of a Request as an Emergency or urgent constitutes authorization of the applicable uplift factor. ITEE shall incur no liability from the inability to accommodate a Rushed Request.

SERVICE WINDOW	UPLIFT FACTOR
Weekday Business Hours (Rushed)	1.5x Standard Charges Apply
Weekday Non-Business Hours	1.5x Standard Charges Apply
Weekend and Public Holidays	2x Standard Charges Apply

Business Hours are Monday through Friday 9:00am – 4:00pm Eastern Daylight Time. For Rushed Requests during the work week, Service Credits will be deducted at a rate of one and a half (1.5) times the standard rate. For Rushed Requests during the Weekend or Holidays, Service Credits will be deducted at a rate of two (2) times the standard rate. A list of observed public holidays is available at https://iteagleeye.com/legal/observed-holidays.

i. Problem Management

i. Problem means the cause or potential cause of one or more Security Incidents. Problem Management refers to the detection and handling of Problems. ITEE follows ITIL best practice guidelines for the identification and handling of problems.

ii. Problem Management is divided into three distinct phases.
    1. Problem Identification
        a. A proactive approach to the identification of problems is used to attempt to detect problems before they cause a Security Incident.
        b. Problem identification activities include:
            i. Trend Analysis of Incident Records
            ii. Detection of Duplicate or Recurring Issues
            iii. Analysis of Manufacturer Information
            iv. Analysis of Internal Observations
            v. Periodic Account Review
        c. Identified Problems are logged and may be viewed by the Client in the Account Management Center.
        d. ITEE utilizes best efforts and industry standards to identify Problems. Client acknowledges that all Problems may not be detected. ITEE bears no liability for Problems that are undetected.
    2. Problem Control
        a. Once a Problem has been identified, it undergoes a Problem control process which analyzes the Problem to better understand and document the potential impact of the Problem as well as possible workarounds and solutions.
        b. Each Problem will be classified by impact. The classification is determined by the presence or absence of a security risk, the exploitability of any security risk, and the potential impact on critical or production networks.
            i. The Info classification denotes a Problem that does not constitute a security concern or impact normal production capabilities. Problems in this category are often related to optimization or suggested improvements. These may be determined to not be a Problem based on Client preferences.
            ii. The Low classification indicates a Problem that may impact performance but has low impact and no associated security concerns.
            iii. The Medium classification indicates a Problem that may have impact on production performance or decreased security. The impact on production environments is judged to cause some noticeable change to speed or responsiveness but should not result in an outage. The security decrease, if any, has a limited exploitation window but has not been fully mitigated. This severity

level may also refer to the potential for critical outages in development or internal networks.

iv. The High classification indicates a Problem that may have devastating effects on production environments.

v. The Critical classification indicates a Problem that potentially has an active exploitable security risk.

c. ITEE will analyze the Problem and suggest changes to resolve or place and effective workaround to mitigate the Problem. ITEE accepts no liability if no known solution or workaround is discovered.

3. Error Control

a. This phase consists of ongoing monitoring for errors or Problems following remediation activities. Any errors or outstanding risk that is noted will be reassessed periodically.

b. When a permanent solution has not been implemented, the error control phase also includes periodic re-assessment of risk or impact level given the mediations in place. Suggested remediation activities may be revised to further mitigate risk or achieve a permanent solution.

iii. Problems, Impact Ratings, and Suggested Remediation Activities will be documented in the Account Management Portal. It is the responsibility of the Client to review these problems and request remediation activities be implemented, including any necessary change control approvals.

iv. Remediation activities will be classified and billed as a Professional Services Engagement. They are not subject to the SLA under the Service. Scheduling is subject to availability.

v. Impact ratings are applied as a convenience for the Client based the opinion of an industry expert. ITEE bears no liability for the misclassification of Problem impact.

vi. ITEE accepts no liability for the failure of the Client to review Problems, approve and request remediation, or schedule remediation activities.

vii. Client acknowledges that the recommendations of ITEE are based on industry standard best practices and may not fully mitigate any risk.

j. Version Management

i. Version Management provides a Professional Services Engagement to plan, schedule, and control the insertion of updated device operating systems or major asset configurations on covered Devices.

1. Devices that are on a Managed Security Service Plan that does not include a minimum of thirty-six (36) months are not eligible for this benefit.

2. A Device must have completed a minimum of twelve (12) months on the Managed Security Service Plan in order to qualify to schedule the first Version Management Professional Services Engagement.

3. Eligibility for the subsequent Version Management Professional Services Engagement will be available twelve (12) months following the previous Version Management Professional Services Engagement.
4. This benefit is only available while the Device is covered under the Service. Failure to schedule the Version Management Professional Services Engagement constitutes a waiver of the benefit. No refunds or other compensation will be provided.
5. All included updates will be completed as provided in the Version Management Plan. Subsequent updates constitute a separate engagement and will be billed, according to their designation, as a Request or Professional Services Engagement.
6. Failure of Client to provide necessary feedback, information, or access to complete an agreed upon Version Management Plan within thirty (30) days of a request by ITEE will constitute a waiver of the benefit for the given period.

ii. Only major version updates only are governed by this policy. Minor version updates are handled under Standard Maintenance.
    1. Minor Updates or dot releases may be reclassified as a Major Update for installation purposes if they contain changes that may cause incompatibility or removal of support.

iii. If a system hardware upgrade is required to comply with current manufacturers specifications, such upgrades are not provided as a part of Version Management. ITEE will provide Client with an estimate or quote for any hardware upgrades, licensing changes, or cloud migration necessary to deploy the updated versions.

iv. In addition to system software, some client software updates may be included in this project if the change is from one supported version to another supported version for covered software. Other commercial software may be included at ITEE discretion upon Client request. Covered software includes:
    1. Database Services (MySQL, MariaDB, PostgreSQL)
    2. Programming Languages (PHP, NodeJS, Java, Python)

v. When available, ITEE will apply Version Management changes to a Development Device that is covered under a Managed Security Service prior to the application of changes to a Production Device. Client accepts full liability, damage, and loss from any changes made for the Version Management Professional Services Engagement.

vi. Emergency Requests are not included in the benefit and will be billed to the Client.

vii. Client is responsible for compatibility and functional testing on all Devices within a Review Period of five (5) days of the completion of changes. Any changes requested after the Review Period will be handled as Requests or Projects. During this period Standard Requests related to the Project are covered under this benefit.

viii. Client is required to provide all information, access, testing and feedback in accordance with the agreed upon plan. Failure to meet this requirement constitutes a waiver of the benefit for the given period. Any additional time required to complete the Version Management Professional Services Engagement will be billed to Client.

k. DevOps Management
   i. DevOps Management provides support for custom software applications through the use of serverless containers. The service includes options for code management through approved third party providers or a private Git repository.
   ii. Upon Client request, file integrity monitoring can be enabled on a covered Device for software that is enrolled in a DevOps Management Plan.
   iii. ITEE is not liable for the contents of the code repository and cannot be held liable for unauthorized access. Client is solely responsible for granting access to the repository and the contents of the repository.

l. Performance and Capacity Monitoring
   i. Devices covered under the Services will be monitored for resource utilization and performance. Monitored items include CPU Utilization, Disk IO, Disk Space Usage, Memory Utilization, Page Load Speed, and SWAP Utilization.
   ii. For each Client, the usage limits that denote high utilization and the accompanying length of time required for notification is recorded in the chart below. Client may request adjustments to these limits. ITEE will accommodate changes to capacity limits when possible. Additional Services or Fees may apply. ITEE, in its sole discretion, may increase these limits on a Device to reflect normal usage if normal operations for the Device is determined to be close to these recommended limits.

MONITORED ITEM	ALERT LIMITS	DURATION
CPU Utilization	>1.5 times Load Average Per CPU	5 Min
Disk IO	>20ms Read/Write Delay	15 Min
Disk Space Utilization	<10% Partition Capacity	NA
Memory Utilization	>90% Average Usage	5 Min
Page Load Speed	>2 Second Load Time	1 Min
SWAP Utilization	>80% Average Utilization	5 Min

   iii. Detection of resource usage or performance meeting critical limits will result in the initiation of an Incident and will be handled according to the Incident Management Section of this Agreement.
   iv. Annual review of resource utilization will be performed by ITEE and any suggested changes will be reported to the Client and recorded as described in the Problem Management section of this agreement. Suggestions for changes in capacity will be based on industry knowledge, best practices, and previous growth trajectory.

m. Backups
    i. Managed Services include configuration and monitoring of daily backups of covered Devices. Backups may be configured to work with cloud, on-premise, and hybrid environments.
    ii. Bandwidth and storage costs are the responsibility of the Client and are not included in the Service.
    iii. If the Client requires backups to remain in their own environment, they may use this benefit with the IT Eagle Eye Cloud Backup Virtual Appliance (HCB). HCB is not included in the Service and must be purchased separately. Purchase and use of the HCB does not entitle the Client to configuration, management, or monitoring for the HCB. A Managed Service with included Backup Configuration must be selected for this Service. If a Managed Service is not purchased, the Client retains all responsibility for configuration, operation, and management.
    iv. ITEE cannot be held liable for any loss or deletion of your data or damage to computer systems for any reason.
    v. ITEE recommends backups of data are completed from another independent geographical region. Redundant backup solutions will further reduce the chances of data loss. ITEE is not liable for Client's acceptance or rejection of these recommendations.
n. Disaster Recovery
    i. After data loss or hardware failure, Disaster Recovery Services are available as an option for Managed Devices when Backups are available for restoration.
    ii. Disaster Recovery is charged to the Client as a number of Service Credits. The minimum number of Service Credits that will be charged for a Disaster Recovery process is 200 Credits. Additional Service Credits may be charged when the recovery time is extended due to complexity, third party provider issues, or other Client factors.
    iii. ITEE is not liable for any lost data or data that cannot be retrieved. It is the responsibility of the Client to ensure appropriate business continuity plans are in place to prevent unacceptable loss.
    iv. Disaster Recovery Testing or Business Continuity Testing may be requested by the Client. These tests are not subject to the SLA and are scheduled based on availability. The test will be billed to the Client as a Disaster Recovery.
o. Firewall Management
    i. Device Firewall Management is included in the Managed Technology Service. This management may be applied to any of the firewall types listed below. One firewall per covered Device is included in the Service. Additional firewall types may be covered, at the discretion of ITEE, for an additional fee.

MANUFACTURER	PRODUCT	TYPE
IT Eagle Eye	NextGen Cloud Firewall	Virtual Appliance
IT Eagle Eye	OnDevice Firewall	Not Applicable
Amazon Web Services	EC2 Cloud Firewall	Not Applicable

ii. Firewall management includes configuration, monitoring, and rule management of the firewall. The service is limited to firewalls that directly cover only one Device.
iii. The IT Eagle Eye NextGen Firewall Virtual Appliance is not included in the service and must be purchased separately for use.
iv. It the OnDevice Firewall is chosen, ITEE will install and configure the firewall on the Managed Device in accordance with the Transition Activities described in this Agreement.

3. Sites
    a. All Services are performed remotely and not at a Client Site. Client may request that ITEE perform a Service at a Client Site, and ITEE may, at its discretion, agree to do so. The Service will be performed at an additional fee or fees that will be invoiced and charged to the Client.
    b. ITEE may at its sole discretion utilize resources temporarily or permanently located in any ITEE location for the delivery of Services.
4. Remote Access
    a. At minimum, all administrative access to the Device must be limited by a Privileged IP Address Firewall Allow Rule or a Virtual Private Network.
    b. Where administrative access to the Device is not able to be limited by IP Address, the Client must provide a compliant secure virtual private network (VPN) tunnel to enable ITEE to securely access the Device. This restriction refers to direct administrative access and web interfaces or backends that allow privileged access. Client may elect to purchase a Managed VPN plan from ITEE for this purpose.
    c. Physical Devices with Out of Band (OOB) Management access are required to be protected from any external network access by a secure VPN due to the sensitivity of the interface.
    d. Hybrid Networks are required to be connected by VPN to ensure the security of data in motion. Client may elect to purchase a Managed VPN plan from ITEE for this purpose.
    e. ITEE requires a secure remote connection in accordance with the requirements in this Agreement in order to be able to perform the Service.
    f. ITEE requires datacenter or cloud logins with administrative access in order to facilitate analysis and diagnosis of network or device disturbances and to receive certain monitoring data. ITEE does not accept any liability, damage, or loss due to Client's failure to provide this access with sufficient permissions to perform the Service.
    g. ITEE is relieved of its obligations under this Agreement and the applicable Service Level Agreement where the required administrative access is limited or unavailable due to any circumstances.
    h. Client expressly excludes ITEE from any liability, loss, or damage when the Client fails to limit administrative access according to this Agreement or to provide ITEE with the required secure remote access. Client accepts full liability for any requested changes that result in divergence from this policy.
5. Client Obligations

a. Client's primary point of contact, as identified to ITEE, or a designee, must be available to IT Eagle Eye during the entire engagement. The representative must have sufficient authority to schedule testing and address any issues that may arise. Notification or contact with this designated point of contact is considered sufficient for the purposes of any required notifications sent by ITEE to Client.
b. Client agrees to promptly notify ITEE of any change in the authorization, contact information, or employment status of any authorized persons. ITEE shall incur no liability resulting from Client's failure to provide such notification.
c. Client is responsible for compatibility, user acceptance testing, and functional testing within a production environment. You must ensure all configuration items are connected to the Internet to enable delivery of automated signature updates from the configuration item's manufacturer.
d. Client shall obtain all consents and authorizations from any third parties necessary for IT Eagle Eye to perform the Services, including without limitation, third party datacenters, co-locations, and hosts. For the avoidance of doubt, IT Eagle Eye will not execute agreements with any such third parties.
e. Client will be solely responsible for any unauthorized acts or omissions that occur as a result of Client's access to or use of the Services and Client agrees to indemnify and hold ITEE harmless from such acts or omissions.
f. Client shall not distribute, reproduce, duplicate, copy, sell, resell, or exploit the Services for any purpose or for the benefit of any third party.
g. Client shall install and maintain any physical hardware delivered by ITEE in an appropriate environment, with adequate power and environmental controls comparable to those generally considered appropriate for business computing equipment.
h. Client shall not move any Device delivered by ITEE to another network location unless it obtains approval in writing, in advance of such move from ITEE.
i. Client shall provide ITEE with at least ten (10) business days' notice prior to taking any action that may affect the Intellectual Property of ITEE.
j. Client agrees to make configuration changes to routers, firewalls, and other network devices upon request by ITEE as required to enable communication between the Client's Network or Device and the ITEE Security Operations Center. ITEE shall not be responsible for any damages in connection with such remote access.

6. Client Equipment
   a. Client must ensure that any Client equipment, network, or systems connected to any ITEE Equipment, network, or systems or used in the Services is technically compatible, connected and used in accordance with any instructions and safety and security procedures applicable to the use of such Client equipment and as directed by ITEE.
   b. If any Client equipment, network, or systems does not comply with the requirements set forth by ITEE in this Agreement or otherwise, Client must advise ITEE within four (4) hours of determination and upon notice from ITEE, disconnect such Client equipment, network, or systems and where applicable, direct ITEE to do the same, the cost of which will be borne by Client.

c. ITEE will not be liable for any failure to meet any Service Level Agreement or other obligations set out in this Agreement if the failure is caused by Client's breach of its obligations.
d. ITEE gives no warranty in respect of the interoperability between ITEE Equipment, network, or systems and any Client equipment, network, or systems.

7. Service Credits
   a. Service Credits must be purchased as a minimum number of one (1) Credit Pack bundle (50 Service Credits). No credit will be provided if there are remaining unused Service Credits at the end of the Billing Term. Credit Pack bundles may be billed separately or included in future scheduled invoices.
   b. For simple Requests, the number of Service Credits deducted per Request is based on a predefined list of standard tasks according to the complexity of the task. Standard task complexity and the associated Service Credit charge is as shown:

COMPLEXITY / TYPE	SERVICE CREDITS
Small	20 Credits
Medium	50 Credits
Standard	75 Credits
Large	125 Credits

   c. For complex and non-standard tasks, the number of Service Credits deducted will be based on the time to complete the task.
      i. Sixty (60) Service Credits per hour will be deducted for tasks performed by a standard SOC Engineer.
      ii. Seventy Five (75) Service Credits per hour will be deducted for tasks performed by Specialty or Advanced Engineers.
      iii. Time will be calculated in minimum increments of fifteen (15) minutes.
      iv. All Service Credit amounts will be rounded up to the nearest whole number.
   d. Service Credit Usage Logs and Service Credit Balance is available in the Account Management Portal. Client holds the responsibility to view and track the use of Service Credits. It may take up to forty eight (48) business hours for logged credit use information to appear in the Account Management Portal.
   e. Client may request an estimate of the number of Service Credits required to fulfill a Request prior to submitting a Request. Client accepts all responsibility to request and review Service Credit Usage and estimates prior to submitting a Request. Submission of a Request indicates Client's authorization to be charged for the number of Service Credits determined by ITEE for that Request.

8. ProService Management
   a. ProService Management provides an ongoing reserve of Service Credits that may be applied to Requests and Professional Service Engagements. When possible, Service Credits that have limited use are used prior to the use of Service Credits from ProService Management.

b. ProService Management Service Credits (PMSC) are available from the first day of a given month and expire on the last day of the same month. Failure to use some or all of the available PMSC constitutes a waiver of the benefit for that period. No refunds or other compensation will be provided.

9. Other Dependencies
    a. Device Change Fee
        i. Each Managed Security Service Plan refers to a single Device that is identified on the Order Form. Change of the Device for a subscribed Service Plan may be completed upon Client request and payment of the Device Change Fee.
        ii. Change requests are not subject to the SLA and will be scheduled based on availability.
        iii. Device changes do not include migration of any data or applications.
        iv. If Exit Transition Activities must be performed on the Device that is being removed from the Service, those Activities will be billed in accordance with this Agreement. Exit Activities are not covered by the Device Change Fee.
    b. Development Network
        i. Services are available for Development Networks at a reduced rate. Election of a Development Service Plan signifies the Client's warranty that the Device is used only in a development environment.
        ii. Performance Monitoring does not apply to Development Service Plans and no Service Credits are included with the Service.
        iii. The number of Development Service Plans may not exceed the number of Managed Technology Security Service Plans.
        iv. Devices on a Development Service Plan may only be used on internal networks for the purpose of testing of products and services. Devices may not be publicly accessible. Internal administrative use does not meet the requirements for Development Service Plans.
        v. In the event that ITEE determines that a Device is publicly accessible, a Development Service Plan will be immediately converted to a Managed Technology Plan. This designation may be made retroactively. Client acknowledges that this reduction in rates is provided as a courtesy to the Client and agrees to pay the difference in Fees in the event that the Device is no longer eligible for the Development Service Plan.
    c. Cloud Plans
        i. When a Managed Security Plan covers a Cluster or Database Group, the following definitions will be used:
            1. A Cluster is a single Auto-Scaling Group that contains a single workload. Determination of what constitutes a single workload is done in the sole discretion of ITEE.
            2. A Database Group is a single database instance that is configured for either vertical or horizontal scaling of resources.
        ii. Cloud Plans are billed hourly, according to use. They are subject to a minimum charge fee of fifteen days per month.

iii. Cloud Plans include support for horizontal scaling via Auto-Scaling Groups and vertical or horizontal scaling for Database Groups. Security Group Management and Access Management such as IAM is also included in the service.

d. SSL Management
   i. Managed Security Service Plans include configuration and maintenance of one Let's Encrypt SSL certificate per covered Device. Alternate types of SSL may be substituted for an additional fee.

10. SLA Exclusions
    a. ITEE will not be liable for Service Level Agreement defaults resulting from one or more of the following events:
       i. Any exclusions stated elsewhere in this Agreement;
       ii. The absence of a patch, repair, policy, configuration, or maintenance change recommended by ITEE but not approved by Client;
       iii. Scheduled downtime in respect of ITEE equipment, including the standard maintenance period of Tuesdays from 7:00pm EDT to 8:00pm EDT or any other scheduled or emergency downtime;
       iv. Changes made by Client to covered Configuration Item where Client has not notified ITEE in accordance with this Agreement;
       v. Unavailability of access to a Site or Device;
       vi. Damage or delay arising from Client failing to carry out an action or contractual obligation required by ITEE in order for it to render the Services in a timely manner and/or in accordance with the agreed Service Level Agreement;
       vii. Time taken for any third party vendor to respond;
       viii. Damage to equipment or software used to render the Services and which are within Client environment due to abnormal operation conditions or changes made by Client;
       ix. Modifications, repairs, or replacements, or attempted modifications, repairs, or replacements no performed by ITEE or not approved by ITEE in writing prior to being performed by any other Party, including the Client;
       x. Restoration of any lost data from any products or devices connected to covered Devices or to the Service without ITEE knowledge and written consent;
       xi. Products where Client has failed to license such products and such license is a prerequisite of the Manufacturer or where such license is no longer current or valid or when such products have been purchased outside of acceptable purchasing norms;
       xii. Data provided by Client is inaccurate or not up-to-date; or
       xiii. A virus, worm, distributed denial of services, or any other malicious activity.

11. End of Life
    a. End of Life (EOL) Devices may be allowed on the Service on a case by case basis. ITEE must approve any Device with hardware or software that is End of Life prior to Service Delivery.
    b. It is the sole responsibility of the Client to inform ITEE of any device with an EOL status.

c. Due to the added complexity and risk in administering the Services, an additional uplift Fee in the amount of twenty five (25) percent will be added to any Managed Service that is applied to an EOL Device. If additional Services are required to mitigate the risk posed by an EOL Device, these Services are not included and will be billed separately.
d. If ITEE, in its sole discretion, is unable to continue to effectively provide the Service for a Device or Software, ITEE may remove the EOL Device from the Service following 90 days written notice to the Client. Upon removal, ITEE must make a pro rata adjustment of the Service Fees.

12. Transition Activities
    a. Objectives
        i. During any transition, the primary objective is to ensure that both organizations enter the transition with a clear understanding of the goals and activities of the transition.
        ii. Transition activities are planned to provide the minimal business disruption that is reasonably possible during the transition of a Managed Service through the following points:
            1. Determination of a realistic transition timeframe;
            2. Establish an operational baseline for the global managed services delivery organization that will be responsible for delivering the service post-transition;
            3. Facilitation and conclusion of the contracting process;
            4. Development of a sound business relationship;
            5. Alignment of expectations and service delivery capabilities and constraints;
            6. Development of understanding regarding the Client's business and how to deliver reliable, stable, and excellent service.
        iii. Transition plans will be completed using ITEE derived methodologies and templates.
    b. Dependencies
        i. Transition plans are designed to occur over a ten (10) week period. This period is further divided into three phases as described below.
            1. Due Diligence: The standard length of this period is two (2) weeks. During the Due Diligence period, ITEE will collect information to gain a better understanding of the Client's network and any special needs. The list of covered Devices will be validated prior to Service initiation. A Network Discovery will be performed. This knowledge will be used to schedule and plan the Service Migration Period for each newly covered Device.
                a. It is the Client's responsibility during this period to provide the necessary access to networks, devices, and premises, including any third party providers, that is required in order to perform the Service.

b. A Record of Entitlement for each Device will be created to govern Configuration Management. It is the Client's responsibility to review all Records of Entitlements in a timely manner and provide feedback if any changes are required.
c. Risks and problems with covered Devices that are identified during the Due Diligence period will be documented for the Client.
d. Any required work done to resolve problems prior to Service Migration is not included in the Service and is not subject to the Service SLA and will be billed separately to the Client. Delays in Service Initiation due to unresolved problems on the Device will not change the Service Effective Date.
e. The Due Diligence period is extended to four (4) weeks for the Managed Technology Security Service with Compliance.

2. Service Migration: The standard length of this period is four (4) weeks. During the Service Migration period, ITEE will transition each covered Device into the Service. This transition will include installation of any required software and necessary changes to configurations or access required in order to perform the Service. When applicable, ITEE will apply additional security features or Hardening to the Device.
3. Service Optimization: The standard length of this period is four (4) weeks. During this period, ITEE has begun to monitor and maintain the device. Based on this knowledge and feedback from the Client, Device and Service Optimizations will be applied.
    a. The Service Optimization period is extended to eight (8) weeks for the Managed Intrusion Detection Security Service.
    b. The Service Optimization period is extended to twelve (12) weeks for the Managed Web Application Firewall Service.

ii. The Transition Period will begin on the Service Effective Date listed on the Order Form. Alternate start dates for the Transition Period may be selected if agreed upon in writing by ITEE and the Client. Election of alternate start dates will not change the Service Effective Date.
iii. Depending on the complexity of the environment, at the discretion of ITEE, the Due Diligence period may be lengthened, shortened, or eliminated and the Service Migration Period may be lengthened or shortened based on prior work and knowledge of the Client.
iv. Managed Devices must be Healthy and Tuned prior to acceptance of management responsibility.
    1. Healthy means that the Device must not have any known hardware or software issues or bugs affecting the operation or management of the Device.

2. Tuned means that the Device must be specified, designed, and configured correctly and it must not have any software that is unlicensed or no longer supported by the manufacturer.
    a. Devices with unsupported EOL software may be allowed on a Managed Service at the discretion of ITEE with written consent and additional fees and restrictions as described in the End of Life section of this Agreement.

v. Transition Activities will be performed during the business day. Additional Fees may apply for work that is required to be performed outside of standard business hours.
vi. If covered Devices are found to have additional requirements, numbers, or other changes during the Transition Period, additional Service Fees may apply.
vii. Any travel costs and fees incurred during the Transition will be charged to the Client separately and in addition to the Service Fees.
viii. Migration and integration services are not included in the Services. All migration and integration services will be billed to the Client as a separate Professional Services Engagement.

c. Exit Activities
    i. During the Exit Period, ITEE will provide reasonable assistance, acting in a manner consistent with Good Industry Practice, for the Transition of Client data and/or domain names following the termination of this Agreement provided that the termination occurred for reasons other than the unresolved material breach of the Client. Such assistance shall be treated and charged for as a separate Professional Services Engagement.
    ii. An Exit Period starts on a date mutually agreed upon between ITEE and then Client.
    iii. Throughout the Exit Period, ITEE will continue to perform the Services as agreed upon in this Agreement and maintain the SLA specified in respect of the Services.
    iv. During the Exit Period, ITEE shall be paid all applicable Service Fees.