SecureIT Service Description

The following managed services are defined as SecureIT on the order if agreed to by the Customer. DivergeIT shall provide Information Security Monitoring & Remediation for the Customer's IT systems, computers, users, servers, and networks. In addition to the terms set forth in this agreement, the Services are subject to the DivergeIT Terms and Conditions and Additional Rates are located at www.DivergeIT.com/agreements, unless there are DivergeIT Terms and Conditions attached hereto or there is a signed master agreement with DivergeIT governing such products and services.

- **Essential:** DivergeIT shall provide a fundamental level of security management and are typically reactive in nature.

Technical Support (MS)	Security Support	Supported Systems/Devices
Agent Deployment Platform Integration Device level incident mgmt.	Endpoint Vulnerability Management Basic Endpoint Protection service & mgmt. DNS Filtering Service & management OS Patch Management 3rd party Patch Management	Windows Devices Apple Devices

- **Advanced:** DivergeIT shall provide all the services in the basic tier but adds a layer of proactive security measures that are characteristic of MDR. This includes advanced threat detection using AI and machine learning technologies, proactive threat hunting, Company level incident response, forensic analysis, and remediation.

Technical Support (MS)	Security Support	Supported Systems/Devices
Agent Deployment Platform Integration Device level incident mgnt	SecureIT Essential + Managed Detection and Response(MDR) Active Endpoint and Cloud Remediation Security Operations Center (SOC) Threat Intelligence Extended Detection and Response(XDR) vCISO - Cyber insurance Support Computer Security Incident (CSIRT) Reporting	Google Sec Command Center Microsoft Defender for Endpoint Carbon Black Sentinel One

- **Maximum:** DivergeIT shall provide a more comprehensive level of security management, including proactive and advanced measures. This more advanced offerings include Security Information and Event Management (SIEM), Security Orchestration, Automation & Response (SOAR), & Compliance identification & adherence.

Technical Support (MS)	Security Support	Supported Systems/Devices
Device Security Deployment Platform Integration Company level incident mgnt	SecureIT MDR + Log Management Advanced Security Monitoring Advanced Vulnerability Management vCISO Cyber Risk Management vCISO Audit Support Tabletop Exercises Red Team Teaming	Microsoft Devices & Cloud Google Cloud Meraki Devices Apple Devices Ubuntu Devices

- **Compliance:** DivergeIT shall provide a more comprehensive level of compliance management, including compliance platform integration and advisory services to maintain compliance. This offering includes a Compliance Management Platform(CMP), security advisor control compliance activities, employee onboarding, vendor risk management,

Technical Support (MS)	Security Support	Supported Systems/Devices
Platform Integration	Compliance Management Platform(CMP) Security Framework Requirement Activities Penetration Testing Advanced Compliance Integration and Monitoring	Microsoft Devices & Cloud Google Cloud Meraki Devices Apple Devices Ubuntu Devices Supported 3rd Party App Integrations

Service Not Included

The following are a list of Services & Costs not covered under this Agreement and can be performed at the sole discretion of DivergeIT:

1. The cost of any Customer owned parts, equipment, or shipping charges of any kind.
2. The cost of any Customer owned Software, Licensing, or Software Renewal or Upgrade Fees of any kind.
3. The cost of any 3rd Party Vendor or Manufacturer Support or Incident Fees of any kind for Customer owned systems or equipment.
4. The cost and Service to bring Customer's environment up to qualify for service.
5. The cost and Service to replace of any network devices, computers, and servers due to the Manufactures End of Life not resulting from systems failure.
6. The cost and Service resulting from the Customer's alteration or modification of hardware, software and/or systems other than that authorized by DivergeIT.
7. The cost and Service to upgrade Major Versions of Applications software or Operating Systems.
8. The Installation, configuration, and deployment of any new applications whether acquired from DivergeIT or any other source.

SERVICE QUALIFICATIONS

- Computers require the Defender for Endpoint P2 EDR software, or alternative compatible EDR software.
- DivergeIT has integration and remediation access to the endpoints and cloud systems
- DivergeIT has internal point of contact to review and approve escalated security actions and remediations as needed.
- Customer agrees that all Devices shall be covered under Security licensing to allow for adequate management and monitoring.
- Customer warrants that all software is genuine, currently licensed, and vendor supported. Should any security system, policy or licensing the foregoing provisions, such security system, policy, and/or licensing shall be excluded from further service unless Customer remedies the issue.
- Customer agrees to pay any third-party vendor support charges required to resolve any issues.

SERVICE REQUESTS METHODS, HOURS & TARGETS

Service Request Methods may change from time to time, and when they do Customer will be notified in writing of the change. Failure to use current Service Request Methods as defined or by written notice at a later date may cause delayed service response and resolution times. Any subsequent delays in service response and resolution time due to failure to use current Service Request Methods shall not constitute a material breach of this Agreement. Each request will be assigned a Service Request number for tracking.

Support of the Customer's Information Technology Systems will be provided to the Customer by DivergeIT in the included services hours and as needed hours indicated below, excluding the holidays. DivergeIT will respond to Customer's Service Requests in accordance with the Service Targets and will use its best efforts to respond within a reasonable time after hours and on holidays. Additional Services, meaning Service Outside of Included Service Hours, requested by Customer shall incur additional charges.

The following Holiday schedule observed by DivergeIT and can be located at the OPM.Gov website. Exceptions include only Columbus Day and Martin Luther King Day where DivergeIT continues to provide regular services. If a Holiday is recognized on a Thursday, the Friday following will be included.

SecureIT+ PLAN				
Monitoring Hours	24/7 x 365 Days a year			
Security Operations Center Hours	Monday – Friday 8am-5pm PST			
	Response	Plan	Resolution	Service Requests methods
Service Targets	90%	80%	70%	Email: help@divergeit.com Portal: http://portal.divergeit.com Instant Message: Desktop Support Portal Phone: (310) 765-7205
Critical	15 Minutes	30 Minutes	60 Minutes	
Important	15 Minutes	30 Minutes	120 Minutes	
Normal	15 Minutes	30 Minutes	240 Minutes	
Scheduled	60 Minutes	4 Hours	N/A	
Outside Control	N/A	N/A	N/A	
CSAT Target	90%			

DEFINITIONS

1. Computer: A Computer is a machine that has our remote management & monitoring software (Agent) installed and a compatible Endpoint Detection and Response package installed on it. Computer counts for services are captured once per month and the computer has been turned on at least once that month.
2. Managed Detection: DivergeIT shall provide Security Operations services to monitor all supported computers that are installed with the DivergeIT agent and compatible Endpoint Detection and Response (EDR), for Indications of Compromise (IOC). DivergeIT will log all confirmed threats in the DivergeIT incident management system.
3. Managed Response: DivergeIT will provide reactive remediation of any detected immediate threats that are logged within the incident management system. DivergeIT will define rules of engagement to avoid disruption of critical systems. DivergeIT will continuously improve playbooks for detection, automation and resolving endpoint compromise. DivergeIT agrees to obtain Customer's authorization to engage third party vendors prior to incurring any additional charges.
4. CSIRT: DivergeIT shall provide your Computer Security Incident Response Team processes and will perform initial security incident triage for all threats identified via detection and or report by Customer. DivergeIT will provide a CSIRT report for any confirmed security breach investigated. There are Incident Response Resources available to remediate large scale impact upon request at an additional charge.
5. Threat Intelligence Service: DivergeIT provides the up-to-date Intelligence continually analyzes telemetry and performs backward-looking analysis of your data (retrospective threat hunts) to ensure that your environment is monitored for new and existing threats.
6. Security Policy Audits: DivergeIT will annually review and upgrade Customers baseline security policies for DivergeIT Security bundles and Computer Security Suite software for the following systems: Email, File, Endpoints, Mobile & Internet Browsing systems.
7. Vulnerability management: DivergeIT will monitor critical 3rd party security application availability and patch as needed. DivergeIT will also monitor for critical OS & Application security settings and modify the settings as needed.
8. Incident: a detected threat that requires validation and investigation.
9. Incident Response: A Qualified Service Engineer has been assigned to Incident.
10. Incident Plan: A Qualified Service Engineer has started or scheduled work on the incident.
11. Incident Resolution: The Incident has been resolved.
12. Incident Impact High: The ability to work has stopped.
13. Incident Impact Medium: The ability to work can continue with workaround.
14. Incident Impact Low: The ability to work can continue.
15. Incident Severity High: All users at the Customer are affected.
16. Incident Severity Medium: More than one user at the Customer is affected.

17. Incident Severity Low: One user at the Customer is affected.
18. Incident Priority 1 (Critical): Incidents that are High Impact, High & Medium Severity.
19. Incident Priority 2 (Important): Incidents that are either High Impact & Low Severity or Medium Impact, High & Medium Severity.
20. Incident Priority 3 (Normal): Incidents that are either Medium Impact & Low Severity or Low Impact, High, Medium & Low Severity.
21. Incident Priority 4 (Scheduled): Incidents that are scheduled for future resolution.
22. Incident Priority 5 (Outside Control): Incidents that are outside of DivergeIT's control.
23. CSAT Formula: The Average Percent Positive Reviews minus the Average Percent Negative Reviews equals the Net CSAT Score for any given period.
24. CSAT Response: The number total number of times an individual response to the customer service request divided by the total number of individual service requests.