MASTER SUBSCRIPTION SERVICES AGREEMENT

This Master Subscription Services Agreement (this "Agreement") is made this __ day of _____, 20__ ("Effective Date"), between the undersigned customer ("Customer") and ePlus Technology, inc. ("ePlus").

1.0   SERVICES.

1.1   Ordering.   ePlus provides managed services and related subscription service offerings ("Services").   Customer may purchase Services through an order form as set forth at Exhibit A ("Order Form") or a statement of work ("SOW") for customized Services.

1.2   Service Descriptions.   Services identified on an Order Form are provided in accordance with the applicable service description document as updated from time to time by ePlus (the "Service Description").   Service levels described in the Service Description are contingent on coverage.   ePlus will make updated Service Descriptions available to Customer electronically.   Service levels will not materially diminish without a mutually agreed change order.

1.3   Affiliate Services.   Customer may purchase Services from an ePlus affiliate by executing an Order Form or SOW between Customer and the affiliate (an "Affiliate Order").   For purposes of an Affiliate Order, references in this Agreement to "ePlus" shall mean the applicable affiliate.   ePlus Technology, inc. may invoice on such affiliate's behalf, but the affiliate shall be solely responsible for the content and performance of the Services under the Affiliate Order.

1.4   Initial Assessment.   ePlus intends to conduct an assessment of Customer's IT environment in connection with the Services, and Customer agrees to cooperate in such assessment.

1.5   ePlus System Maintenance.   ePlus at times will perform routine or emergency system maintenance, which may impact monitoring and other Services.   ePlus will provide as much advance notice as practical to Customer, including estimated impact and duration of Service outage.

1.6   ePlus Personnel.   ePlus personnel who work on Customer's premises will have the requisite experience and qualifications and be required by ePlus to comply with Customer's reasonable workplace rules, provided that such personnel will not be subject to special background check or similar requirements that may delay onboarding.

2.0   ONBOARDING AND COOPERATION.

2.1   Customer Resources and Information.   Customer acknowledges that for ePlus to perform the Services, Customer must make certain personnel or other requested resources available to ePlus in a timely manner.   Failure to do so may prevent ePlus from onboarding or providing the full benefits of the Services.   Customer must furnish the required information for onboarding within thirty (30) days of the Order Form date to ensure timely commencement of Services.   If such required information and cooperation is not provided within sixty (60) days after execution of the applicable Order Form or SOW, ePlus may begin monthly billing under this Agreement, and Customer agrees to pay the invoiced amounts.   However, ePlus will use all commercially reasonable efforts to provide such support as practical until onboarding is complete.

2.2   VPN Access and Monitoring Devices.   Customer agrees that ePlus may install a VPN router and/or hardware necessary for the performance of monitoring responsibilities as outlined in an applicable Service Description.   Customer must provide network connectivity for such devices.   The benefits of certain Service offerings are dependent on data collection devices or programs deployed in Customer's environment. Customer acknowledges that failure to enable such deployment will result in forgoing the related value added deliverables.

2.3   Compliance and Back Ups.   Customer is responsible for its content, material and data made available or transmitted in connection with the Services and for its compliance with federal, state and local laws and acceptable use policies of any third-party vendors.   Additional Customer responsibilities are listed in the Service Descriptions.   Customer must back-up and protect all data against loss, damage, or destruction.

2.4   Customer Hardware Maintenance.   Unless covered by ePlus' Enhanced Maintenance Support ("EMS"), Customer is responsible for support and maintenance of devices in its environment.   ePlus may adjust or discontinue Services with thirty (30) day notice on devices not under maintenance.

3.0   CHANGES/RECONCILIATIONS.

3.1   Quarterly True-Ups.   Contractual true-up meetings will be held quarterly to account for device-count fluctuations (adds/removes/changes). Based on the true-up, a new bill of materials will be created for the updated device count and associated pricing. Periodic recurring charges will be adjusted in accordance with the true-up and reflected in subsequent invoices, provided that such recurring charges shall not decrease by more than fifteen percent (15%) total in a Service Term Year.   A Service Term Year is a consecutive twelve (12) month period from the first date of the Service Term.

3.2   Additional Services.   Customer may add Services or adjust Service levels through a new Order Form, notification or change order, and billing will be adjusted accordingly. Hardware, software, and manufacturer maintenance and support may be purchased under a separate written agreement.

4.0 TERM AND TERMINATION.

4.1 Term. This Agreement shall continue from the Effective Date until terminated by either party on thirty (30) days notice, but no such termination shall affect an outstanding SOW or Order Form. The term of each Service ordered under this Agreement (the "Service Term") shall be indicated in the Order Form or SOW.

4.2 Termination for Default. Either party may terminate a SOW or Order Form in the event of the other party's material breach which is not cured after written notice of forty-five (45) days, or fifteen (15) days in the case of nonpayment. If the breach is of such a nature that a reasonable person could not cure it within such period, the breaching party shall commence to cure within such period, then diligently prosecute such cure to completion.

4.3 Termination Fee. The parties agree that ePlus will be substantially damaged in amounts that will be difficult or impossible to determine if Customer terminates a Service early. Therefore, except in the event of an uncured default by ePlus pursuant to Section 4.2, in the event of early termination of a Service Term with or without ePlus' consent, including any default by Customer in its obligation to make payment after notice, Customer shall pay a termination fee to ePlus. The amount of the termination fee shall be as agreed in the applicable Order Form or SOW. If no such fee is provided there, then the termination fee shall be equal to the amount of all non-recurring and recurring charges set forth in the Order Form or SOW which would otherwise be due through the end of the Service Term, including applicable taxes and fees. The parties agree that the termination fee is reasonable as liquidated damages for such occurrences. It is further understood and agreed that the payment of liquidated damages is in lieu of actual damages. Customer hereby waives any defense as to the validity of any liquidated damages stated in this Agreement, an Order Form or a SOW on the grounds that such liquidated damages are void as penalties or are not reasonably related to actual damages. The termination fee shall be paid in good funds within ten (10) business days of the effective date of the applicable termination.

4.4 Termination for Lack of Funds. The parties acknowledge that pursuant to NRS 244.320 and NRS 354.626, if Customer's governing body does not appropriate funds for the purposes specified in this Agreement, or the Customer's governing body has, in its discretion, determined to amend previous appropriated funds or budgeted amounts to eliminate or reduce funding for the purposes of this Agreement, this Agreement will be terminated without penalty, charge, or sanction, provided that (i) Customer shall have used its best efforts to obtain the funding, and (ii) Customer represents are warrants that it has sufficient funding appropriated and budgeted to meet its obligations during the initial fiscal year of each Order Form and SOW.

5.0 PRICING AND PAYMENT. Pricing is set forth in the Order Form or SOW, subject to adjustment in accordance with Section 3.1. Unless otherwise agreed in writing, payment for both recurring and non-recurring Services is due within thirty (30) days of the date of ePlus' invoice. Customer agrees to pay a late payment charge of one percent (1%) per month. Customer will pay or reimburse ePlus for all taxes due under this Agreement and ePlus will remit those amounts to the appropriate taxing authority. If Services require travel to a Customer-designated site, ePlus will be entitled to reimbursement for actual, reasonable travel and living expenses.

6.0 CONFIDENTIALITY. "Confidential Information" is information or material disclosed by a party ("Discloser") to the other (Recipient") in connection with this Agreement that is either (a) marked or identified in writing as confidential, or (b) relates to the processes, technology, plans, or methodologies used by ePlus or its suppliers to provide the Services. Recipient shall not disclose Confidential Information to any third party until three (3) years after the end of the applicable Service Term. Confidential Information does not include information that: (i) is or becomes publicly available without breach of this Agreement; (ii) is in Recipient's possession at the time of receipt or becomes available from a third party without breach of confidentiality obligation; or (iii) is independently developed by or for Recipient without access to Confidential Information, as evidenced by written records. This section shall not prohibit ePlus from disclosing information required by its suppliers or subcontractors in connection with this Agreement. Customer acknowledges that ePlus or its employees and subcontractors may provide similar services to others and use or disclose to others general knowledge, skill and experience developed over the years, including under this Agreement. Recipient may disclose Confidential Information pursuant to a legal requirement or court order after first notifying Discloser. Discloser may seek to obtain a protective order limiting the scope of disclosure. This Agreement is subject to any applicable public records laws, including NRS Chapter 239.

7.0 OWNERSHIP. Unless indicated in the SOW or Service Description, Services do not involve deliverables. Hardware and software provided in connection with the Services remain ePlus property. On expiration or discontinuation of Services Customer must arrange for safe return at its expense of all hardware and software to ePlus within fourteen (14) days. Customer agrees to pay for any item not returned on time at its then-current market replacement value.

8.0 WARRANTY AND DISCLAIMERS. During the Service Term ePlus will provide the Services using reasonable care and skill in accordance with the Service Description or SOW. ePlus does not warrant that Services will be uninterrupted or error-free. ePlus makes no warranties with respect to hardware, software or maintenance, support or services created or licensed by third parties except that if applicable ePlus will pass through all third party warranties to Customer. To the extent Services include managed security services or assessments, no guaranty is made by ePlus or its third party providers that such Services will detect all security weaknesses, potential security problems, vulnerabilities or potential breaches. ePlus does not guarantee that recommendations or actions undertaken during the Agreement will completely address all issues identified or not identified. EPLUS DISCLAIMS ALL OTHER WARRANTIES RELATING TO THIS AGREEMENT OR THE SERVICES INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF FITNESS FOR PARTICULAR PURPOSE,

MERCHANTABILITY, TITLE, NON-INFRINGEMENT, OR OTHERWISE. Customer will not waive and intends to assert any and all available NRS Chapter 41 liability limitations in all cases.

9.0 INDEMNIFICATION. If a third party brings an action alleging that Services infringe on a U.S. patent or copyright, ePlus will defend and pay damages finally awarded against Customer or included in a settlement, provided Customer promptly notifies ePlus in writing of the claim, furnishes requested information, and allows ePlus to control defense and settlement. ePlus may modify or replace a Service with a comparable non-infringing one or at its option discontinue the Service and provide a credit for the remainder of any pre-paid unexpired term. ePlus will not be liable in connection with a claim based on a Service performed by a third party such as a manufacturer or licensor,but will reasonably assist Customer in working with the third party provider to resolve such claims. In respects to any acts, errors or omissions in the performance of ePlus services, ePlus agrees to indemnify and hold harmless Customer, its officers, agents, employees, and volunteers from and against any and all claims, demands, defense costs, or liability to the extent caused by ePlus' negligent acts, errors or omissions in the performance of ePlus' services under the terms of this agreement.

ePlus agrees to release, defend, indemnify, and hold harmless the Customer for claims, losses, penalties and damages and reasonable attorneys' fees and costs arising out of ePlus', or its subcontractor's, unauthorized use, disclosure, access or acquisition (whether on their own or through a third-party) of Customer's Confidential Information. ePlus acknowledges and agrees that it will inform all of its principals, officers, employees, agents and subcontractors assigned to perform the Services for the Customer under this Agreement of the obligations contained herein. ePlus agrees to assume all liability and shall bear all costs, losses and damages resulting from a breach of this Agreement by any of its principals, officers, employees, agents and subcontractors.

ePlus further agrees to defend Customer and assume all costs, expenses and liabilities of any nature to which Customer may be subjected as a result of any claim, demand, action or cause of action arising out of the negligent acts, errors or omissions of ePlus or its Sub-contractors in the performance of ePlus' services under the Agreement.

10.0 INSURANCE.
10.1 By ePlus. Unless expressly waived in writing by Customer, ePlus, as an independent contractor and not an employee of Customer, must obtain and maintain policies of insurance in amounts specified in this Agreement and pay all taxes and fees incident hereunto. Customer shall have no liability except as specified in this Agreement. ePlus shall, at ePlus's sole expense, procure, maintain and keep in force the following insurance conforming to the minimum requirements specified below. Unless specifically specified herein or otherwise agreed to by Customer, the required insurance shall be in effect prior to the commencement of work by ePlus.

10.2 Form of Coverage. Any insurance or self-insurance available to Customer shall be excess of and non-contributing with any insurance required from ePlus. ePlus's insurance policies shall apply on a primary basis. Until the termination of this Agreement, ePlus shall provide Customer with renewal or replacement evidence of insurance upon expiration or replacement of the required insurance.

10.2.1 Additional Insured. By endorsement to all liability policies (including Professional Liability and Network Security & Privacy Liability), except Worker's Compensation, evidenced by ePlus, Customer, its officers, employees, and any other Indemnitees included under this Agreement shall be included as additional insureds for all liability arising from the Agreement. Additional insured status shall apply until the expiration of time within which a claimant can bring suit per applicable law.

10.2.2 Waiver of Subrogation. Each liability insurance policy (including Professional Liability & Network Security/Privacy Liability), unless otherwise specified below, shall provide that the insurance company waives all right of recovery by way of subrogation against Customer, its officers, employees in connection with damage covered by any policy.

10.2.3 Approved Insurers. Each insurance policy shall be (i) issued by licensed and admitted insurance companies authorized to do business in the State of Nevada or that meet any applicable state and federal laws and regulations for non-admitted insurance placements and acceptable to Customer. and (ii) currently rated by A.M. Best as "A-, VII" or better.

10.3 Policies Required.

10.3.1 Workers' Compensation and Employer's Liability Insurance. ePlus shall provide proof of worker's compensation insurance meeting the statutory requirements of the State of Nevada, including but not limited to NRS 616B.627 and NRS 617.210 or provide proof that compliance with the provisions of Nevada Revised Statutes, Chapters 616A-D and all other related chapters is not required. Employer's Liability limits shall not be less than $1,000,000 each accident for bodily injury by accident and $1,000,000 each employee for bodily injury by disease.
ePlus waives all rights against Customer, its officials, officers, employees, volunteers and agents, for recovery of damages to the extent these damages are covered by the workers compensation and employer's liability or commercial umbrella liability insurance obtained by Tenant pursuant to this agreement. ePlus shall obtain an endorsement equivalent to WC 00 03 13 to effect this waiver.

10.3.2 Commercial General Liability Insurance.
ePlus shall procure and maintain, during the term of this Agreement, occurrence commercial general liability, and, if necessary, commercial umbrella insurance, for limits of not less than Two Million Dollars ($2,000,000) for bodily injury and property damage per occurrence. and Four Million Dollars ($4,000,000) general aggregate. If such CGL insurance contains a general aggregate limit, it shall apply separately to this location or project. Coverage shall be written on an occurrence form at least as broad as an unmodified ISO occurrence form CG 00 01

04 13 (or a substitute form providing coverage at least as broad) and shall cover liability arising from premises, operations, independent contractors, products and completed operations, personal and advertising injury, civil lawsuits, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).

10.3.2.1 Additional Insured. Customer, its officials, officers, volunteers, employees and any other Indemnitees included under this Agreement shall be included as insureds under the CGL, using ISO additional insured endorsement CG 20 10 07/04 or CG 20 26 07/04 or a substitute providing equivalent coverage, and under the commercial umbrella, if any. ePlus shall also include additional insured coverage for its products and completed operations exposures, if applicable to this Agreement. This insurance shall apply as primary insurance with respect to any other insurance or self-insurance programs afforded to Customer or any other Indemnitees under this Agreement.

10.3.2.2 Waiver of Subrogation. ePlus waives all rights against Customer, its agents, officers, directors and employees and any other Indemnitees listed in this this Agreement for recovery of damages to the extent these damages are covered by the commercial general liability or commercial umbrella liability insurance maintained pursuant to this agreement. ePlus's insurer shall endorse CGL policy to waive subrogation against Customer with respect to any loss paid under the policy.

10.3.3   Professional Liability/Errors & Omissions Insured. ePlus shall maintain professional liability insurance applying to liability for a professional, error, act, or omission arising out of the scope of the ePlus's services provided under this Agreement. Limits shall be not less than Ten Million Dollars $10,000,000 each claim and annual aggregate. ePlus shall maintain professional liability insurance during the term of this Agreement.

Technology Services Requirements: If ePlus is providing technology services, including but not limited to software, hardware, networking, information security, information technology consulting and training, cloud computing, telecommunications services, data processing, data and application hosting, provision of managed services, programming, mobile services and web applications, coverage shall be included for errors, omissions, or negligent acts in the performance or failure to perform technological services for others.

10.3.4   Business Automobile Liability Insurance.
ePlus shall procure and maintain, during the term of this Agreement, business automobile liability insurance in the amount of not less than One Million Dollars ($1,000,000) per occurrence for bodily injury and property damage. Such insurance shall cover liability arising out of any auto, including owned, non-owned and hired vehicles. Business auto coverage shall be written on any of the unmodified ISO forms (CA 00 01, CA 00 05, CA 00 12, CA 00 25), or a substitute form providing coverage at least as broad. If necessary, the policy shall be endorsed to provide contractual liability coverage equivalent to that provided in the 1990 and later editions of CA 00 01.
If ePlus does not have any owned or leased automobiles, Customer may agree to accept Hired & Non-Owned Auto

Liability Coverage included under the Contractor's Commercial General Liability.

10.3.4.1 Waiver of Subrogation. ePlus waives all rights against Customer, its agents, officers, directors and employees and any other Indemnitees listed in the Indemnification section of this Agreement for recovery of damages to the extent these damages are covered by the business auto liability or commercial umbrella liability insurance obtained by ePlus pursuant to this agreement.

10.3.5   Network Security and Privacy Liability.
ePlus shall maintain network security and privacy liability insurance insuring against loss resulting from (1) privacy breaches [liability arising from the loss or disclosure of confidential information] (2) system breach (3) denial or loss of service (4) introduction, implantation, or spread of malicious software code (5) unauthorized access to or use of computer systems and (6) system failure. Coverage shall be provided with a limit of not less than Ten Million dollars ($10,000,000) per claim and annual aggregate.

10.4 Evidence of Insurance.
Prior to the start of any Work, ePlus must provide the following documents to Customer, Attention: Risk Management, 1001 E. Ninth St., Building D, Reno, NV 89512.

10.4.1   Certificate of Insurance. Prior to the commencement of any work or services under this Agreement and thereafter upon renewal or replacement of each required coverage, ePlus shall provide a Certificate of Insurance form to Customer to evidence the insurance policies and coverage required of ePlus. Customer reserves the right to require copies of all required insurance policies, including all Subcontractor policies, at any time. Copies of policy forms or endorsements confirming required additional insured, waiver of subrogation and notice of cancellation provisions are required to be provided upon request.

10.4.2   Additional Insured Endorsements. If ePlus does not have a blanket additional insured clause, an original Additional Insured Endorsement, signed by an authorized insurance company representative, must be submitted to Customer, by attachment to the Certificate of Insurance, to evidence the endorsement of Customer as additional insured.

10.4.3   Policy Cancelation Notification. ePlus or its insurers shall provide at least thirty (30) days' prior written notice to Customer prior to the cancellation or non-renewal of any insurance required under this Agreement. An exception may be included to provide at least ten (10) days' written notice if cancellation is due to non-payment of premium. ePlus shall be responsible to provide prior written notice to Customer as soon as practicable upon receipt of any notice of cancellation, non-renewal, reduction in required limits or other material change in the insurance required under this Agreement.

Other Conditions. Failure to maintain the required insurance may result in termination of this Agreement at Customer's option. If ePlus fails to maintain the required insurance as set forth herein, Customer shall have the right, but not the obligation, to purchase said insurance at ePlus's expense.

Any waiver of ePlus's obligation to furnish such certificate or maintain such insurance must be in writing and signed by an authorized representative of Customer. Failure of Customer to demand such certificate or other evidence of full compliance with these insurance requirements or failure of Customer to identify a deficiency from evidence that is provided shall not be construed as a waiver of ePlus's obligation to maintain such insurance, or as a waiver as to the enforcement of any of these provisions at a later date.

By requiring insurance herein, Customer does not represent that coverage and limits will necessarily be adequate to protect ePlus, and such coverage and limits shall not be deemed as a limitation on ePlus's liability under the indemnities granted to Customer in this Agreement. The insurance requirements of this Agreement shall be in addition to and not in lieu of any other remedy available to Customer under this Agreement or otherwise. Customer reserves the right to request and review a copy of any required insurance policy or endorsement to assure compliance with these requirements.

If ePlus's liability policies do not contain the standard ISO separation of insureds condition, or a substantially similar clause, they shall be endorsed to provide cross-liability coverage.

11.0 LIMITATION OF LIABILITY. THE TOTAL AGGREGATE LIABILITY OF EPLUS AND ITS THIRD PARTY SERVICE PROVIDERS ARISING OUT OF OR CONNECTED WITH THIS AGREEMENT, IF ANY, NOT EXCEED TEN MILLION DOLLARS ($10,000,000). Except for payments owed, no action arising out of this Agreement may be initiated more than one year after the cause of action accrued. Each party acknowledges that the limitations of liability in this Agreement are a reasonable allocation of risk and that without such allocation ePlus would not be able to provide the Services at the prices charged. These limitations of liability shall apply notwithstanding any failure of essential purpose of any limited remedy.

12.0 GENERAL.

12.1 Notices. Notices under this Agreement shall be in writing, sent by nationally recognized overnight carrier, and deemed given on receipt at the party's address below (or another address designated by such party by written notice). Notices to ePlus must be addressed to the General Counsel's attention with copy to VP Contracts at the same address.

12.2 Law and Disputes. The laws of the State of Nevada shall govern this Agreement. Venue is proper in state and Federal courts located in Washoe County, Nevada. If legal action must be brought due to Customer's non-payment, ePlus shall be entitled to recover the costs of such action, including reasonable attorneys' fees. The parties waive, to the extent permitted by law, all rights to a jury trial.

12.3 Force Majeure. If a party is unable to perform under this Agreement due to power failure, internet outage, natural disaster, war, terrorism, insurrection, riot, strike, unavailability of personnel due to injury, sickness, death or termination of employment, or other cause beyond the party's reasonable control (a "Force Majeure Event"), such party shall notify the other and take action to resume performance as soon as reasonably possible. Upon such notice, all obligations under this Agreement shall be suspended for the duration of the Force Majeure Event.

12.4 Entire Agreement. This Agreement, together with properly executed Order Forms and SOWs, is the entire agreement between the parties and supersedes all representations, oral or written, made by either party prior to, or contemporaneous with, the date of execution. Terms in or referenced by Customer's purchase orders shall have no effect, nor shall course of dealing or custom. If a provision of this Agreement is held unenforceable under applicable law, the remaining provisions shall not be affected. The relationship created between the parties shall be of independent contractors entering into an agreement.

12.5 Assignment. Neither party shall sell, assign, or transfer any of its rights or obligations under this Agreement without the other party's prior written consent, provided that ePlus may assign all or part of its rights to receive payment but none of its obligations.

12.6 Survival. Sections 4, 6, 7, 8, 9, 10, and 11 shall survive any expiration or termination of this Agreement.

EACH PARTY has caused this Agreement to be signed by its authorized representative.

CUSTOMER: Washoe County, Nevada

By: _____

Print: _____

Title: _____

Date: _____

Address: _____

_____

ePlus Technology, inc.

By: _____

Print: _____

Title: _____

Date: _____

13595 Dulles Technology Drive

Herndon, VA 20171

This Order Form is entered into between ePlus Technology, inc. and the Customer indicated below, pursuant to the Master Subscription Services Agreement ("Agreement") between the parties.

CUSTOMER NAME: WASHOE COUNTY, NEVADA
SERVICE OFFERING: 24x7 SECURITY MONTIORING & ALERTING WITH SIEM SAAS and 1 YEAR LOG RETENTION
SERVICE TERM (check <u>one</u>): _____5 YEARS

START DATE (check <u>one</u>):

  ___X___   **On Signature**. The Service Term begins on the date of the last signature on this Order Form.

  _____   **On Completion of Onboarding**. Customer agrees to furnish ePlus written or electronic acknowledgment of the commencement of services, in a form requested by ePlus. Initial set up fees will apply prior to completion of onboarding as indicated below. Onboarding is dependent on customer's cooperation and is subject to the requirements set forth in the Agreement, which may include ePlus' right to commence the Service Term and periodic invoicing in the event of Customer's failure to cooperate.

  _____   **Other Date**: _____.

1   Services Overview

1.1 Services Summary

ePlus, utilizing its subcontractor ProSOC, Inc dba Proficio ("Proficio"), will utilize the ProSOC Cloud-based Security Operations Center (SOC)-as-a-Service to collect security log data from Customer for monitoring, analysis, and alerting by security analysts. Customer staff will be alerted on significant actionable events prioritized as Very High Priority and provided access to the ProSOC fully managed SIEM-as-a-Service portal for detailed investigation, reporting, operational dashboards, and incident case management.

1.2   Devices Supported

The Log Sources in Scope for this SOW for log collection, 24x7 Security Monitoring and Alerting, and SIEM-as-a-Service are included in the table below:

Log Source	Qty
Large NG Firewall – HA Pair	2
Medium NG Firewall – HA Pair	1
Small Firewall - Single	39
SMB Firewall - Single	39
Category A - Network Device, Security Server, OS Server, Application Server, Web Server, Database	27
Endpoints Agents	7,100

Firewalls, NGFWs, IDS, and WAFs are categorized as Large, Medium, Small, and SMB by their bandwidth and functionality. Devices with less than 100Mbps are considered SMB, from 101Mbps to 1Gbps of bandwidth are considered small, from 1 Gbps to 5 Gbps are considered medium, and devices supporting 5Gbps to 10 Gbps are considered large. Any chassis-based FW/ NGFW with multiple 10Gbps interfaces is a special price. If customer is only using 500MB of a possible 2GB throughput device, Device should be sized as 2GB

Below is the initial list of log sources that will be collected and included in the scope. Any changes will have to be within the same license model or require a change order:

Large NG FW – HA Pair
- o PA5220 – Qty 2

Medium NG Firewall – HA Pair
- o PA3260 – Qty 1

Small Firewall – Single
- o ForcePoint N51 – Qty 4
- o ForcePoint 321 – Qty 34
- o ForcePoint 331 – Qty 1

SMB Firewall – Single
- o ForcePoint 110 – Qty 39

Category A
- o Domain Controller (3 domains with 3 in one, 2 in each of the others) – Qty 7
- o URL Filter Server (MacAffee Proxy Servers) – Qty 5
- o Windows Server (File Servers) – Qty 5
- o Unix/Linux Server (ERP - SAP) – Qty 4
- o VPN concentrator (Pulse Secure) – Qty 1
- o Cloud Application (O365) – Qty 1
- o Authentication Server (DUO) – Qty 1
- o MS-Exchange Server (Exchange on Prem – Relay) – Qty 1
- o Email Gateway / Filter (Mimecast) – Qty 1
- o A/V Server (MacAffee) – Qty 1

Endpoint Agents
- o Office 365 Endpoints – Qty 3100
- o Macaffee Endpoints – Qty 4000

1.3 Data Collection

Proficio ProSOC collects event data at the Customer premise via a technology called a ProSOC Collector Security Appliance. The Collector may be deployed as a software based Virtual Appliance or (optionally if purchased) a hardware appliance to collect event data from security & network devices, databases, and applications. The ProSOC Collector will normalize, aggregate, encrypt, and securely transmit the event data to Proficio ProSOC SIEM for processing.

1.4 Asset, Prioritization, and Policy Modeling

Proficio security engineers will work with Customer during the onboarding process to collect and model extended Asset, Security Zone, Prioritization, and Policy information to optimize the Proficio use case library to suit the Customer's unique requirements. The

Proficio 'Service On-Boarding Package' documentation to be completed by Customer, with the assistance of Proficio, will provide the basis for security information and event management process handling.

1.5   Threat Intelligence Profiler

The ProSOC services includes the Proficio Threat Intelligence Profiler reputation service that compiles bad actors, malware servers, malware beacon hosts, command and control servers, and other malicious activity sources aggregated from trusted security groups into a list that ProSOC SIEM correlates with ingress and egress network traffic and pattern rules to discover active threats. These threats include discoveries like:

1.5.1 Malware infected devices

1.5.2 Dark Web Activity

1.5.3 Attack patterns from known abusive hosts directed at the organization

1.5.4 Public facing services open for attack

1.5.5 Applications in use directing traffic to suspicious hosts

1.6   ProView Plus Portal

The Services include a secure web-based ProView Plus portal with Executive Dashboards and ThreatInsight scoring. ProView Plus portal's executive dashboards empower Customer's team with a high-level overview of its security posture and the ability to filter security alerts and review device behavior. Proficio's ThreatInsight score leverages advanced analytics to expose Customer's threat blind spots and provide timely intelligent recommendations to improve Customer's security posture.

During the Term, Customer is granted 5 ProView Plus account(s). No license or transfer of rights is granted or implied, other than access during the Term for Customer's internal purposes. Customer agrees that Proficio shall own all content within ProView Plus.

1.7   Endpoint Incident Investigation, Response, and Remediation Services

Endpoint Monitoring Services

Proficio's Endpoint Monitoring Services provides 24x7 monitoring and alerting, log collection of Endpoint Anti-Virus or Detection/Protection logs for monitoring, cross-event correlation, event validation and alerting for Windows, Mac and Linux desktops, laptops and servers. Events from CUSTOMERS anti-virus or endpoint management server are integrated into the ProSOC SIEM where our library of advanced use cases accurately detect and correlate endpoint events. Each correlated event is investigated by our highly trained SOC analysts who will validate threats using tools such as VirusTotal, Google and other resources to gather additional threat intelligence to enrich the alert with details and provide recommendations for remediation. Includes one (1) year endpoint security agent aggregated central management server log retention.

2   Services Delivery Tasks

Proficio follows a thorough and methodical approach to implementing security management and monitoring services for new Customers. The process starts with understanding and documenting a Customer's network and policies and continues through to training and service execution. The Proficio onboarding process is thoroughly documented to streamline implementation and ensure services start quickly and effectively without disrupting the Customer's internal team.

A dedicated Proficio consultant will act as the Customer's primary point of contact for all implementation, testing and transition activities prior to service delivery. The consultant will work with the Customer team to create an onboarding plan customized to Customer's needs. During the onboarding process, the goal is to understand and document network topology, security objectives, contacts and escalation policies. Via meetings with key stakeholders, the consultant will classify information assets and user information to determine priorities for security posture, alert notification, escalation, compliance and cyber security.

The final phase of the process includes providing users access and training to the ProSOC portal, kick-off meeting(s), and the creation of the Customer's first ticket.

a. Service Onboarding

Service onboarding begins after the 'Service On-boarding Package' document is completed by Customer. If this Statement of Work becomes effective during Proficio's peak periods of service (such as end of quarter), Customer's Onboarding may be delayed but will be initiated as soon as practical based on Proficio's resource availability. The Service On- boarding Package documents the data sources for data collection, assets, zones, policies, contacts, and other information required for service delivery.

Tasks

i. Proficio resources are available 45 days from the "kickoff" call with Customer. If delays caused by Customer occur, Customer understands that Proficio's dedicated resources may be released to service other Customers and may need to be rescheduled to be available to service Customer.
ii. Event Source Data Collection

Proficio requires a central event source data collection system called a ProSOC Collector installed in the Customer environment to collect log and active list event data. The ProSOC Collector may be a software Virtual Appliance of a physical appliance. The ProSOC Collector has multiple modules in the appliance called Connectors that parse device specific logs into a Common Event Format, as well as preform filtering and aggregation of the log data. The ProSOC Collector encrypts the logs and established a secure connection to the ProSOC data center to transmit the log data.

One or more of the following Connector options will be implemented and configured at the Customer location by Proficio with the assistance of the Customer.

1. Connectors in the ProSOC Collector Appliance Software Virtual Machine on a Customer provided Server (shared or dedicated)
2. Connectors in a ProSOC Collector Appliance hardware server (if purchased)
3. Directly on individual event source system
    iii. Configure Base Content which includes applicable dashboards, reports, active channels, and correlation rules that support the ProSOC monitoring service. Baseline Events and Tune Content
    iv. Configure Customer Access Rights and Escalation Procedures to Portal
    v. Create Customer Knowledge Base in SOC Management System
    vi. ProView Portal Training (Maximum of 3 training sessions of no more than 2 hours each)
    vii. Create Initial Ticket or Case

b. Security Monitoring, Alert Notification, and SIEM

This table below provides the list of Services provided by Proficio to Customer in accordance with pricing – specifically for items listed in section 1.1-1.7

Security Monitoring, Alerting, and Reporting

Services
Log Collection and Retention

350+ Device Types and Applications Supported
Distributed Log Collection via Proficio Collector on Customer Virtual Machine or Proficio Appliance (if ordered)
No Agents Required (optional if desired)
365 Day Log Retention
Advanced SIEM and Correlation
Industry leading SIEM and Correlation Engine and Portal
Asset modeling & prioritization
Security zone modeling & correlation
User level tracking & analysis
Multiple methods of correlation including Cross-Device, Pattern, and Session correlation
Reputation Service Threat Feeds Correlated to Traffic
Collection from Cloud-based applications, VM servers, databases, and security services
Packaged and Custom Use Cases
Intelligent Event Search and Retrieval. Log requests will be completed on a best effort basis.
Forensic Analysis and Case Management tools
Expert Monitoring, Analysis, and Alerting
SIEM Architects and Advanced Content Authors
365x24x7 Analysis and Alerting
Alert notification via email, phone, or portal
Alert notification within 30 minutes of Very High Priority Event
Actionable Information with Low Noise
Access to SOC Security Analysts and Engineers
Watching Your Security Events are our Security Engineers, Information System Security Professionals, Firewall Analysts, Intrusion Analysts, Forensic Analysts, Incident Handlers, and Network/Web/Application Penetration Testers –
Reporting and Compliance
Standard security, SANS, network, server, configuration, operations and executive reports (as defined above)
Custom Reports, scheduled reports, and ad hoc reports (as defined in Section 2.6)
Reporting for Compliance requirements (if compliance package ordered)
Trend Analysis
Executive Summaries
ProSOC ProView Web Portal and SIEM Access
Role Based Access Control and Dashboards
Standard Operational and Custom Dashboards
Dashboards for Event Visibility

Powerful Log Search capability for investigations and ad hoc reporting
Powerful analysis and visualization tools
Case Management
Full case management system and portal
Event with Case Tracking
Auto-assignment of Alerts
Notifications and Escalations
On-Boarding and Operationalization
Rapid deployment and log collection
Complete asset, zone, user & correlation modeling
Collect configuration changes on all devices including firewalls, servers, databases, routers
Network Connectivity to SOC
Role Based Access Control for Customers
Security Log Normalization to Common Event Format
Custom Use Cases and Correlation Rules

c. Service Level Agreement

Proficio services include service level commitments that ensure the highest levels of service availability to our Customers. The Proficio Service Level Agreement for this SOW is:

Service Level Agreement	Description	Response Time
Security Alert Notification	24x7 Email Alert of a Very High Priority (Level 9-10) Risk Event	30 minutes
Priority Help Desk Response	Time for security professional to respond to a Customer request on a Very High Priority (Level 9-10) Risk Event	30 minutes
Non-priority Help Desk Response	Time for security professional to respond to a Customer request other than on a Very High Priority (Level 9-10) Risk Event	4 hours
Service Availability	Minimum percentage uptime of Security Operations Center (i.e. the availability of either the primary or secondary SIEM)	99.5%

d. Customer Responsibilities

Customer shall complete the Proficio 'Service On-boarding Package' documentation defining all current configurations, policies, rules, user's, network address, password controls, and other information required to provide services under this SOW. All information must be received at least 10 days prior to onboarding service delivery and Proficio must be notified of any changes at least 5 business days in advance.

Customer will notify Proficio immediately of any user account changes required due to termination of Customer's employee or contractor.

Customer shall provide Linux or Windows Server resources for installation of Proficio Virtual Machine Secure Data Collection Connector, if an appliance Data Connector has not been purchased for environment.

Customer shall provide a secure network connection from Customer network to Proficio SOC Data Centers using one of the Proficio supported deployment scenarios contained in the Proficio ProSOC Collector VM Introduction and Deployment Guide.

Customer is responsible for filtering all data provided to Proficio to obfuscate any Personally Identifiable Information (PII), Protected Health Information (PHI), or credit card information (Cardholder Data).

Customer is responsible for Customer's network and server resources that enable Proficio's ability to collect log data. Proficio is not responsible for the loss of logs or other service interruptions due to Customer changes. Should Proficio be required to reconfigure, or re-onboard services due to customer change of more than 5% of their devices annually, both parties will follow the change control process described below and Proficio will issue an invoice upon completion of the reconfiguration or re-onboarding. Proficio may waive reconfiguration or re-onboarding fees at its discretion; such waiver does not waive Proficio's rights for future changes.

Qty	Product/Service Description	Annual Cost (All Quantities)
2	24X7 Security Monitoring & Alerting - w/ SIEM SaaS - w/ 1 Yr Log Retention - Large NG FW/IDS - HA Pair - Annual Fee/5 Yr Term - T1 (1-2) Devices: PA 5220	$27,992.20
1	24X7 Security Monitoring & Alerting - w/ SIEM SaaS - w/ 1 Yr Log Retention - Medium NG FW/IDS - HA Pair - Annual Fee/5 Yr Term - T1 (1-2) Devices: PA 3260	$11,343.25
39	24X7 Security Monitoring & Alerting - w/ SIEM SaaS - w/ 1 Yr Log Retention - Small FW - Single - Annual Fee/5 Yr Term - T4 (26-50) Devices: ForcePoint N51 (4), ForcePoint 321 (34), ForcePoint 331 (1)	$63,813.50
39	24X7 Security Monitoring & Alerting - w/ SIEM SaaS - w/ 1 Yr Log Retention - SMB FW - Annual Fee/5 Yr Term - T4 (26-50) Devices: ForcePoint 110	$35,159.40
27	24X7 Security Monitoring & Alerting - w/ SIEM SaaS - w/ 1 Yr Log Retention - Network/Security Device/Server OS/Application/Database - Annual Fee/5 Yr Term - T2 (26-100)	$18,252.90
4000	24x7 Endpoint Security Monitoring and Alerting - w/ SIEM SaaS - w/ log collection from customer Endpoint Management Sever w/1 Year Log Retention - Per endpoint - Annual Fee/5 Yr Term - T3 (2,500 - 4,999) Devices: McAfee	$12,260.40
3100	24X7 Security Monitoring & Alerting - w/ SIEM SaaS - w/ 1 Yr Log Retention - For MS Office 365 - Annual Fee/5 Yr Term per user - T3 (2501-5,000) Devices: O365	$2,795.80
5	ProSOC/ProSIEM Web Portal Use - Per User - Annual Fee/5 Yr Term	$9,862.55
1	**One Time Setup Fee** - ProSOC Collector data collection software set-up on-site, SIEM use cases, report development, asset & priority development, and department dashboards. T2 (26-150 Total Devices plus A category Devices)	$9,650.00

END OF TERM:/RENEWAL : The Service Term shall automatically renew on a yearly basis with the then-current annual pricing, unless Customer provides written notice to ePlus of its intention not to renew at least one hundred twenty (120) days prior to the end of the Service Term or a new Order Form is executed.

FEES: Pursuant to the Agreement Customer hereby orders the Services and agrees to pay to ePlus the fees indicated below. ePlus shall invoice any applicable one-time fees upon execution of this Order Form. Recurring fees shall be invoiced annually, in advance, commencing upon the Start Date. Fees will be adjusted periodically based on net changes to the devices under contract as set forth in the Agreement.

	Annual Payment	One-Time Payment
Five Year Term		
Onboarding – One Time Setup Fee	*N/A*	**$9,650.00**
24x7 SECURITY MONTIORING & ALERTING WITH SIEM SAAS and 1 YEAR LOG RETENTION	**$181,480.00**	*N/A*

FIVE YEAR TERM DISCOUNT: Customer has chosen a 5 year term which includes a fifteen percent (15%) reduction in annual fees. Customer may terminate this Order Form without cause in month thirty-six (36) by providing sixty (60) days prior written notice. In the event of early termination under this Section, ePlus shall invoice and Customer agrees to pay a transition fee equaling: $96,078. This transition fee is equal to the total discount received during those thirty-six (36) months of service.

CUSTOMER BILLING AND CONTACT INFORMATION:

	Invoicing	Technical
Contact Name		
Title		
Street Address		
City, State, Zip		
Email		
Phone		

ePlus Technology, inc.

By: _____

Name: _____

Title: _____

Date: _____

Washoe County, Nevada

By: _____

Name: _____

Title: _____

Date: _____