

EXHIBIT A1

Managed Firewall Security Services (MFSS) SOW

1.0 SUPPORTED FIREWALL CONFIGURATIONS & MANAGED SERVICES CURRENT PLANS

Firewall Security Managed Security (24x7)

eSecurity Solutions provides a complete Managed Security Services for network firewalls which includes ongoing monitoring, maintenance, and support for firewalls with optional services for threat monitoring through our advanced SOC team and Threat Hunting analysts with Cloud SIEM.

Basic (Legacy)	Protect	Protect + Comply	Services Provided
♦	♦	♦	Complete 24x7 management and support by eSecurity Solutions SOC
♦	♦	♦	Backup and secure storage of Firewall configuration with revision ¹
♦	♦	♦	Updates to security software and firewall firmware ¹
♦	♦	♦	Traffic Policy / NAT / Route management – adds, changes, and deletes
♦	♦	♦	Branch Office VPN management
	♦	♦	Advanced VPN for site-to-site and mobile users
	♦	♦	Advanced Firewall and Network Configuration
	♦	♦	Industry best practices configuration and settings ¹
	♦	♦	Security profile (UTM) management ²
	♦	♦	HTTPS / SSL decryption and inspection for malware and threats ²
	♦	♦	Centralized management and change auditing ^{1 & 2}
	♦	♦	Availability and health monitoring
	♦	♦	Configure and verify remote logging and reports ^{1 & 2}
	♦	♦	Configuration, policy, and security profile (UTM) reviews ¹
		♦	SIEM Cloud Service with 24x7 SOC Monitoring ¹
		♦	Threat Monitoring - Log correlation, rule analysis, threat feeds, and ML
		♦	Threat Hunting performed by 24x7 threat analysts
		♦	Threat Incident Response
		♦	Compliance with security regulations (PCI, HIPAA, GBLA, etc.) ¹

¹ Compliance with security regulation

² Must meet hardware requirements, licenses may be required, and may impact firewall performance or throughput

2.0 DETAILED SCOPE OF SERVICES (All Plans)

2.1 Firewall Security Services

2.1.1 SETUP AND INSTALLATION

Tasks include:

- Customer survey regarding Customer's network, internet and user configuration requirements
- Pre-configuration of Customer firewall per Customer's network, internet and user requirements
- Remote installation assistance and final configuration of firewall.

Customer Responsibility

Customer should make sure that the following things are provided to make sure that this service is installed and delivered uninterrupted.

- Customer must complete the Customer survey providing accurate information related to the necessary environment and requirements so that firewall may be configured properly.
- Customer to provide a single point of contact for installation configuration requirements.
- Customer must assist in physical installation of firewall in the Customer environment with the remote guidance of Company response team.
- Firewall, internet and network equipment is in an isolated area safe from accidental disconnection. Equipment should be connected to a suitable UPS power device to prevent power interruption.
- Customer should inform Company about any changes to ISP services or network gateway equipment or any network configuration changes required.

Deliverable: Firewall installed per customer's requirements, according to Supported Firewall Configurations and Service Order.

2.1.2 FIREWALL MAINTENANCE

Tasks include:

- Updates to firewall firmware as deemed necessary by Company to keep firewall operating efficiently, securely and with latest usable features and management capabilities.
- Store recent backup of firewall configuration, scheduled backups monthly
- Ensure latest UTM subscriptions are downloaded and usable to maximize firewall security.
- Respond to Customer requests for setup changes that are within Maintenance Scope
- Respond to Customer requests that are not within Maintenance Scope as Custom Services Requests.

SCOPE / SLA:

- Maintain firewall firmware to a maintainable level or as appropriate upgrade to enhance performance, stability, and usable features
- Save a copy of the firewall to be used to re-setup firewall or revert configuration changes
 - Watchguard firewall configurations are saved upon changes made by eSecurity Solutions support team and stored in the eSecurity Solutions Data Center
 - Fortinet firewall configurations are saved upon major configuration changes, upon customer requests, and when available on a weekly scheduled basis (requires SSH connection to firewall) and stored in the eSecurity Solutions Data Center
 - Sophos firewall configurations are saved on a daily schedule automatically to the Sophos firewall internal storage and manually upon major configuration changes which will be stored in the eSecurity Solutions Data center
- Maintain UTM software and data to current levels to maintain high level of security.
- Respond to and take action on customer requests within the following Maintenance Scope:
 - Web management configuration changes
 - Email security settings including SPAM and AV (only certain firewalls support SPAM filtering – for advanced SPAM filtering, Company recommend a dedicated Email security solution)
- Network settings, static routes, and firewall policies changes excluding New VPNs and New Networks/Subnets

Deliverable: Maintenance on firewall and management infrastructure to ensure ongoing deliverable of secure firewall service within the current network architecture.

2.1.3 HOSTED CENTRAL MANAGEMENT PORTAL

Tasks include:

- Central management of firewalls for secure access and ease of use

SCOPE / SLA:

- Company response team uses central management server to securely maintain and administer firewalls
- Customers may request access to central management server to access their firewalls remotely
 - Company does not support changes to firewall made by customer
- For any incidents that require on-site presence or actions, Customer will be contacted for resolution
- Central Management subscription, server software, or appliance is required (varies by firewall vendor)

Deliverable: Managed securely from eSecurity Solutions public IPs

2.1.5 INFORMATION & EVENT LOGGING & REPORTING

Tasks include:

- Logging and Reporting
 - Firewall system (software and hardware) errors
 - Security events (Web Filter, IPS, App Control, Antivirus, and Email)
- Requires subscription and support by vendor/model
 - User Policy Violation
- Online on-demand standard reports
- Online custom reports generated by Customers

SCOPE / SLA:

- Logging is 24 x 7 and reports are generated on-demand and/or scheduled (scheduled sent by email)
- Reports first analyzed (weekly) by the Company response team and actionable items will be converted to tickets and responded to within the contracted response agreement timeframe
- Actionable alerts are responded to within four (4) hours during Business Hours (see definition) or if Premium Support, then 24 x 7 x 365 per plan definition
- For any incidents that require on-site presence or actions, Customer will be contacted for resolution
- Logging and Reporting subscription, server software, or appliance is require (varies by firewall vendor)

Deliverable: Monthly reports automatically sent via email

2.1.6 HEALTH MONITORING & AUTOMATED ALERTS

Tasks include:

- Firewall Availability (Uptime)
- External Internet Connection
- Firewall Performance (CPU, Memory, Sessions/Connections)

SCOPE / SLA:

- Monitoring is 24 x 7 and responded to automatically based upon the incident priority
- Issues will create alerts to Company escalation contacts based on the priority of the incidents
- Alerts will be first analyzed by the Company response team and actionable alerts will be converted to tickets and responded to within the contracted response agreement timeframe
- Actionable alerts are responded to within four (4) hours during Business Hours (see definition) or if Premium Support, then 24 x 7 x 365 per plan definition
- Alert historical information is available online and reports are generated on-demand
- For any incidents that require on-site presence or actions, Customer will be contacted for resolution
- Monitoring requires SNMP access enabled on firewall and may require an onsite agent installed on a server

Deliverable: Actionable alerts will be prioritized and worked to resolution.

2.1.7 SOC RESPONSE

Tasks include:

- Firewall security and health incident response
- Firewall policy and setting changes
- Firmware updates and patches

SCOPE / SLA:

- Review and respond to firewall security and health incidents
 - Service tickets are created for firewall security and health incidents
 - Company response team reviews ticket within 4 hours of recorded tickets during Business Hours (or 24 x 7 x 365 if Premium Support contract)
- Review and respond to firewall policy and setting changes required by Customer
 - Service tickets are created for firewall policy and setting changes
 - Company response team reviews ticket within 4 hours of recorded tickets during Business Hours (after hours support is available by phone at an additional charge of \$225/hour and must be scheduled)
- Schedule firmware and patch updates within customers maintenance window
 - Service tickets are created for firmware and patch updates
 - Company response team schedules firmware and patch updates with Customer
- For any incidents that require on-site presence or actions, Customer will be contacted for resolution

Deliverable: Actionable alerts will be prioritized and worked to resolution.

2.1.8 CONFIGURATION REVIEW AND RECOMMENDATIONS

Tasks include:

- Firewall security review, analysis, and recommendation

SCOPE / SLA:

- Review of firewall policies and UTM settings for best security practices
 - Review firewall policies, NAT settings, and VPN settings for potential security risks
 - Review UTM settings (Web Filtering, Application Monitoring, IPS, Gateway AV, and Email Filtering) and make recommendations to decrease security risks
 - Create a report with recommendations

Deliverable: Configuration review and recommendations report and follow-up discussion between Company response team and Customer

2.1.9 HA (HIGH AVAILABILITY)

Tasks include:

- HA and Redundancy for WAN/Internet
- HA and Redundancy for Firewall appliances

SCOPE / SLA:

- Configure firewall for WAN/Internet HA and Redundancy
 - HA - Internet failover to Secondary (or Tertiary) if Primary WAN fails
 - Redundancy – Balance traffic over Primary and Secondary (and Tertiary) WAN using round robin, spillover, or closest route methods
 - Redundancy – Policy based routing of traffic over Primary and Secondary (and Tertiary) WAN
 - HA and Redundancy is only available on certain models of firewalls and may require a license
- Configure two or more firewalls for HA and Redundancy
 - HA - Firewall failover to Secondary (or cluster) if Primary firewall fails
 - Redundancy – Cluster 2 or more (3 or more is recommended) firewalls to share load
 - HA and Redundancy is only available on certain models of firewalls and may require a license
- For any incidents that require on-site presence or actions, Customer will be contacted for resolution

Deliverable: Firewalls configured with redundant Internet connections and/or multiple firewalls configured for failover

3.0 SUPPORT (all plans)

Customer support related to the contracted services will be provided during for following times and availability. Support is provided either by email, online ticketing system or by phone.

Below are the terminologies used for support services.

Definition	Days	Service Timings	Availability
Business Hours (Covered under your chosen support Plan)	Monday through Friday	8:00 am PST to 6:00 pm PST	Yes, email and phone
Business Hours (Not Covered under your chosen support Plan)	Monday through Friday	8:00 am PST to 6:00 pm PST	\$175 per hour (Discounted Rate)
Off Business Hours	Monday through Friday	6:00 pm PST to 8:00 am PST	Emergency Service available at \$250 per hour
Weekend Hours	Saturday and Sunday	6:00 pm PST Friday to 8:00 am PST Monday	Emergency Service available at \$250 per hour
24x7 Premium SOC Response	Monday through Sunday	24 x 7	Optional: Add-on for 24x7 Active Monitoring and Emergency Afterhours Support

Note: All hours mentioned are Pacific time-zone (U.S.) hours.

Customer Responsibility

Customer to provide and identify a single point of contact for support purposes.

4.0 CUSTOM SERVICE REQUESTS (all plans)

Custom Services Requests will be billed at \$275 per hour or quoted on a project basis upon request.

EXHIBIT A2

Managed Endpoint Security Services (MESS) SOW

1.0 MANAGED ENDPOINT PLANS

MESS plans are listed below. These plans may be amended at any time to add, change or remove services and provide updated plans. Core service functionality for plan components is described herein. Please refer to www.eSecuritySolutions.com for the latest plan services components.

Managed Endpoint Security Services Comparison

Protect	Protect + Comply	Managed Service	
•	•	Complete antivirus and antimalware protection for endpoints ¹	ENDPOINT SECURITY
•	•	Manage endpoint security centrally with change auditing ¹	
•	•	Review and recommend Industry best practices configuration and settings ¹	
•	•	Manage endpoints policies in groups based on OS, function, and department	
•	•	Endpoint security policy management – adds, changes, and deletes	
•	•	Review of Endpoint agent issues - disconnected, uninstalled, or errors ¹	
•	•	Review of Endpoint agent software and signature updates and deploy ¹	
•	•	Endpoint Detection and Response (EDR) policy management	EDR MANAGEMENT
•	•	Machine Learning and automated incident detection policy management	
•	•	Policy based response to incidents with remediation actions	
•	•	Automated host containment (isolation) to prevent spread of malware	
•	•	Application / process classification and control via policy management ²	
•	•	Exploit and ZERO-day protection policy management	
•	•	Content / web filtering control and monitoring policy management ^{1 & 2}	
•	•	Review content / web filtering reports and make recommendations ^{1 & 2}	
	•	Windows Firewall and Host IPS policy management ¹	ADVANCED SECURITY
	•	Windows device and peripheral control policy management ^{1 & 2}	
	•	Patch Management - update applications and operating systems ^{1 & 2}	
	•	Host vulnerability assessment scans of applications and operating system ^{1 & 2}	
	•	Host asset inventory reports of hardware and software / applications ^{1 & 2}	

Note: EPP and EDR help organizations comply with security regulations. Organizations must meet hardware / software requirements and licenses / subscriptions requirements.

1 Aides with compliance with security regulations

2 Must meet hardware / software requirements and licenses / subscriptions may be required

2.0 DETAILED SCOPE OF SERVICES (All Plans)

- 2.1 **Licenses** of Cloud Hosted (Vendor Hosted) products are issued usually within one to four hours after a validated order is received by customer. All other licenses are issued usually with one to two days after a validated order is received by customer.
- 2.2 **License Management:** The following is managed related to customer licenses.
 - 2.2.1 New licenses
 - 2.2.2 Additional and removal of licenses
 - 2.2.3 Current number of license
 - 2.2.4 Licenses start dates
 - 2.2.5 License end dates
- 2.3 **Flex Billing:** Flex Billing allows customers to pay monthly, quarterly or annually to match their cash and expense requirements. Payment, plan terms and adjustments are described in the Base Services agreement.
- 2.4 **Technical Support:** Tier 1 Support provided by Company trained staff. Company staff is backed up by priority vendor technical support staffs.

2.4.1 Tasks include

2.4.1.1 Responding to customer:

- 2.4.1.1.1 Installation questions
- 2.4.1.1.2 Operational questions
- 2.4.1.1.3 Threat or infection questions
- 2.4.1.1.4 Installation change questions
- 2.4.1.1.5 Product questions

2.4.2 Scope / SLA:

- Issues will create alerts to Company escalation contacts based on the priority of the incidents.
- Alerts will be first analyzed by the Company response team and actionable alerts will be converted to tickets and responded to within the contracted response agreement timeframe.
- Actionable alerts are responded to within four (4) hours during Business Hours (see definition).
- Online reports will reflect system status and any system recorded alerts (See Reporting)
- For any incidents that require on-site presence or actions, Customer will be contacted for resolution.
- Customer support related to the contracted services will be provided during for following times and availability. Support is provided either by email, online ticketing system or by phone.
- **Custom Services Requests** will be billed at \$250 per hour or quoted on a project basis upon request.

Below are the terminologies used for support services.

Definition	Days	Service Timings	Availability
Business Hours	Monday through Friday	8:00 am PST to 6:00 pm PST	Yes, email and phone
Off Business Hours	Monday through Friday	6:00 pm PST to 8:00 am PST	Emergency Service available at Custom Services Hourly Rate
Weekend Hours	Saturday and Sunday	6:00 pm PST Friday to 8:00 am PST Monday	\$250 per hour

Note: All hours mentioned are client local U.S. hours.

- 2.5 Security Notifications:** Informative communications with customers notifying them of potential security risks, threats or issues they should be aware of that will help mitigate future or current risks. These notifications will come in the form of emails to the authorized contact for the customer.

2.6 Installation, Deployment, Setup, Configuration, Maintain and Adjust

2.6.1 Tasks include

- 2.6.1.1 Customer survey re: information related to IT infrastructure for install
- 2.6.1.2 Coordination with customer personnel (IT professional) re: any issues that facilitate installation
- 2.6.1.3 Installation and setup of AV management server and console
- 2.6.1.4 Guidance deploying licenses/contracted AV product(s) into customer environment per sales order
- 2.6.1.5 Setup and configuration of server and clients settings per best security practices
- 2.6.1.6 Adjustments to security policy per security threats, customer requests or circumstances.

2.6.2 Scope / SLA:

- Issues will create alerts to Company and Customer with escalation and management per Support SLA.

2.6.3 Customer Responsibility

Customer should make sure that the following things are provided to make sure that this service is installed and delivered uninterrupted

- Customer must complete the Customer survey providing accurate information related to the necessary environment and requirements so that service may be configured properly.
- Customer to provide a single point of contact for installation configuration requirements.
- Customer must provide a server computer suitable for installation of the management server (if required) in the Customer environment with the remote guidance of Company' managed services staff. Not required for hosted management solutions.
- Customer is responsible for deploying the endpoint security agent on all systems (servers, workstations, laptops, mobile devices, etc...) with the remote guidance of Company' managed services staff.
- Customer is responsible for damage cleanup and virus removal on systems. Company' managed service staff does not provide these services.
- Customer is responsible for the overall health of systems. Company does not guarantee endpoint security agents compatibility with systems and software. Compatibility issues with systems and software and endpoint security agents must be handled with the vendors directly. Company provides optional NOC and Helpdesk support using 3rd party security vendors.

2.7 Monitor and Alert

The goal of managed services is to provide security services without the need for customer involvement on a daily basis. However, alerts to Customers is provided whenever it is necessary or deemed important as described below.

2.7.1 Tasks include monitoring customer installation to ensure:

- Installed clients are online
- Installed clients are at current software levels
- Installed clients have current detection pattern updates installed
- Client licenses are current and functioning
- Security events are managed and remediation has occurred (log report inspection)
- Security Threats are mitigated
- User Policy Violations are managed and alerted if necessary

2.7.2 Event Log Monitoring Scope / SLA:

- Monitoring is 10 x 5 and responded to automatically based upon the incident priority.
- Optional Monitoring Available - 24 x 7 and responded to automatically based upon the incident priority.
- Issues will create alerts to Company with escalation and management per Support SLA.

2.7.3 Deliverable

- Actionable alerts will be prioritized and worked to resolution. Alerts will be delivered as soon as is practicable to Customers to notify customer of potential issues and action responses required when required.

2.8 Reporting and Reporting Assistance

AV Reporting is primarily done via an online report portal accessible to customers and reflects historic threats, mitigation and system status. Since the AV service will manage these issues, customers will not normally need to view this information on a regular basis. For Compliance purposes, this information is available as required.

2.8.1 Tasks include:

- Online access to current Antimalware and Endpoint system reports
- Assistance with custom report generation (see Services Plan)
- Report log access as required. Customers with specific requirements should notify Company in advance of the need.

2.8.2 Event Log Monitoring Scope / SLA:

- Online reports are available 24 x 7
- Support is provided per the Support SLA.

2.8.3 Deliverable

- Online reports. Reporting and log support as defined in this section and per the support SLA.

EXHIBIT A3

Managed Data/System BDR Services (MBDR) SOW

1.0 MANAGED SYSTEM / DATA BACKUP PLAN

MDBAK plan is listed below. The plan may be amended at any time to add, change or remove services and provide updated plan. Core service functionality for plan components is described herein. Please refer to www.eSecuritySolutions.com for the latest plan services components.

SERVICES PROVIDED

Rapid Account Provisioning	✓
Policy Definition	✓
Remote Installation & Configuration	✓
- Remote Deployment - Setup/Configuration per Policies	
Create Backups as required by Policy	✓
Verify Validity of Backups	✓
Test Restore function	✓
License Management (& Adjustments)	✓
Support	Tier 1 Company
Maintain/Adjust Configuration as necessary	✓
Data Restore / Disaster Recovery When Required	✓
Monitor & Alert	✓
Provide Standard Reports, Assist with Compliance or other Reporting	✓

2.0 DETAILED SCOPE OF SERVICES (All Plans)

2.9 Rapid Account Provisioning: The following is managed related to customer licenses.

- 2.9.1 New data backup accounts
- 2.9.2 Additional and removal of storage
- 2.9.3 Licenses start dates
- 2.9.4 License end dates
- 2.9.5 Additional features to be licensed

2.10 Flex Billing: Flex Billing allows customers to pay monthly, quarterly or annually to match their cash and expense requirements. Payment, plan terms and adjustments are described in the Base Services agreement.

2.11 Support: Tier 1 Support provided by Company trained staff.

2.11.1 Tasks include

2.11.1.1 Responding to customer:

- 2.11.1.1.1 Installation questions
- 2.11.1.1.2 Operational questions
- 2.11.1.1.3 Installation change questions
- 2.11.1.1.4 Product questions

2.11.2 Scope / SLA:

- Issues will create alerts to Company escalation contacts based on the priority of the incidents.
- Alerts will be first analyzed by the Company response team and actionable alerts will be converted to tickets and responded to within the contracted response agreement timeframe.
- Actionable alerts are responded to within four (4) hours during Business Hours (see definition).
- Online reports will reflect system status and any system recorded alerts (See Reporting)
- For any incidents that require on-site presence or actions, Customer will be contacted for resolution.
- Customer support related to the contracted services will be provided during for following times and availability. Support is provided either by email, online ticketing system or by phone.
- **Custom Services Requests** will be billed at \$250 per hour or quoted on a project basis upon request.

Below are the terminologies used for support services.

Definition	Days	Service Timings	Availability
Business Hours	Monday through Friday	8:00 am PST to 6:00 pm PST	Yes, email and phone
Off Business Hours	Monday through Friday	6:00 pm PST to 8:00 am PST	Emergency Service available at Custom Services Hourly Rate
Weekend Hours	Saturday and Sunday	6:00 pm PST Friday to 8:00 am PST Monday	\$250 per hour

Note: All hours mentioned are client local U.S. hours.

2.12 Installation, Deployment, Setup, Configuration, Maintain and Adjust

2.12.1 Tasks include

- 2.12.1.1 Customer survey re: necessary data to backup.
- 2.12.1.2 Installation and setup of backup software, management and agents
- 2.12.1.3 Back job creation & Scheduling
- 2.12.1.4 Coordination with customer personnel re: any issues that facilitate installation
- 2.12.1.5 Remote deployment of software agents per backup strategy
- 2.12.1.6 Setup and configuration of management, alerts and client agents per best security practices
- 2.12.1.7 Adjustments to security policy per customer driven requests or circumstance changes.
- 2.12.1.8 Install software agent updates as required to provide appropriate functionality

2.12.2 Scope / SLA:

- Issues will create alerts to Company with escalation and management per Support SLA.

2.12.3 Customer Responsibility

Customer should make sure that the following things are provided to make sure that this service is installed and delivered uninterrupted

- Customer must complete the Customer survey providing accurate information related to the necessary environment and requirements so that service may be configured properly.
- Customer to provide a single point of contact for installation configuration requirements.
- Customer must provide a server computer suitable for installation of the management server (if required) in the Customer environment with the remote guidance of Company' managed services staff. Not required for hosted management solutions.

2.13 Data Restore / Disaster Recovery

2.13.1 Tasks Include

- Assist customer in defining necessary data to restore
- Restore customer data from previously backed up data

2.1 Monitor and Alert

The goal of managed services is to provide security services without the need for customer involvement on a daily basis. However, alerts to Customers is provided whenever it is necessary or deemed important as described below.

2.13.2 Tasks include monitoring customer installation to ensure:

- Installed clients are online
- Installed clients are at current software levels
- Installed clients have current detection pattern updates installed
- Client licenses are current and functioning
- Security events are managed and remediation has occurred (log report inspection)
- Security Threats are mitigated
- User Policy Violations are managed and alerted if necessary

2.13.3 Event Log Monitoring Scope / SLA:

- Monitoring is 24 x 7 and responded to automatically based upon the incident priority.
- Issues will create alerts to Company with escalation and management per Support SLA.

2.13.4 Deliverable

Actionable alerts will be prioritized and worked to resolution. Alerts will be delivered as soon as is practicable to Customers to notify customer of potential issues and action responses required when required.

2.14 Reporting and Reporting Assistance

Reporting is done via online report portal & local management software accessible to customers and reflects backup jobs, available storage and backup status. Since the AV service will manage these issues, customers will not normally need to view this information on a regular basis. For Compliance purposes, this information is available as required.

2.14.1 Tasks include:

- Online access to current AV system reports
- Assistance with custom report generation (see Services Plan)
- Report log access as required. Customers with specific requirements should notify Company in advance of the need.

2.14.2 Event Log Monitoring Scope / SLA:

- Online reports are available 24 x 7
- Support is provided per the Support SLA.

2.14.3 Deliverable

Online reports. Reporting and log support as defined in this section and per the support SLA.

STATEMENT OF WORK - EXHIBIT A4

Article 1 - General

- 1) Alert Logic Managed Compliance Services provide any or all of the following compliance aiding services as provided by Alert Logic as contracted by Customer in the Services Order.
- a) Alert Logic Threat manager – Intrusion detection and vulnerability assessment
 - b) Alert Logic Active Watch – 24 x 7 monitoring and expert guidance services
 - c) Alert Logic Log Manager – Collect, search, analyze and report on consolidated log data
 - d) Log Review – PCI DSS compliant log analysis, alerting, audit trail and reporting
 - e) Other Alert Logic Managed Services

Additional details about Alert Logic managed services are provided in the Alert Logic Detailed Services Descriptions document available from Alert Logic. Services terms and conditions for these services are defined in this Exhibit and the MSA.

Article 2 – Service Level Agreement

Service Warranties.

(a) Service Level Warranty. Subject to the exceptions set forth herein, Alert Logic warrants that it will provide each Service at or above the service levels defined below (the “Service Level Warranty”):

(i) Alert Logic will provide 99.9% reliability for its hosted services. The 99.9% reliability is calculated by determining the total time in minutes for a month, subtracting all planned maintenance time, and then dividing all unplanned downtime of the hosted services by the remaining time. Alert Logic’s obligations under this MSA are in effect during all hours of operation, except during planned maintenance windows and any approved additional maintenance windows scheduled by Alert Logic.

(ii) Alert Logic will notify Customer at least 3 days in advance of any additional planned maintenance occurring outside of the standard maintenance window and make efforts to accommodate Customer’s needs regarding the additional maintenance requirement. Alert Logic will provide Customer as much notice as possible when unplanned (“Emergency”) maintenance occurs.

(iii) For Customers purchasing ActiveWatch, for all environments for which ActiveWatch services are deployed and properly configured (“Protected Environments”), Alert Logic will escalate detected security incidents for Protected Environments within 15 minutes of their occurrence. Alert Logic 15 minute incident SLA is measured from when Alert Logic identifies an incident to the time of initial escalation to the primary customer contact via automated system log, email, or phone call.

(iv) For Customers purchasing review services (e.g., LogReview), Alert Logic will (a) Review data for the prior day within 24 hours, (b) escalate potential security incidents to Customer upon detection and (c) maintain an audit trail of review activity on a daily basis that is accessible online.

(v) Alert Logic will respond to properly submitted service requests within 2 hours of receipt and either resolve or escalate properly submitted service requests within 24 hours of receipt. Service requests must be submitted via web portal, e-mail or telephone.

(vi) Initial response time for support requests related to Inline Devices will be within 15 minutes. The Inline Devices must be online and accessible to Alert Logic for support to be provided. For support requests related to potential block events, Customer must provide Alert Logic with the Incident ID found on the blocking page of the Web Security Manager product.

(vii) Customer must provide up-to-date SSL certificates and keys in order for Alert Logic to tune or configure the Web Security Manager and Threat Manager products for monitoring and protection of HTTPS traffic.

(viii) For Web Security Manager, Log Manager or Threat Manager instances deployed on Customer hardware, Alert Logic will not be responsible for any hardware-related issues and if not deployed on minimum recommended hardware specifications, Alert Logic will not be responsible for supporting degradation of performance.

If Alert Logic Cloud Defender is fully provisioned to utilize Threat Manager, Log Manager and out-of-band Web Security Manager, Alert Logic warrants that it will provide Service at or above the service levels (i), (ii), (iii), (v), (vii) and (viii), defined above.

Reliability for Hosted Services	
Monthly Uptime Percentage	Service Credit Percentage
<99.9%	10%
<95%	25%

ActiveWatch 15-Minute Escalation Commitment	
Monthly Failures	Service Credit Percentage
< 5	10%
5 or more	25%

Review Services 24-Hour Reporting Commitment	
Monthly Failures	Service Credit Percentage
< 5	10%
5 or more	25%

Submitted Service Requests 2-Hour Response Commitment	
Monthly Failures	Service Credit Percentage
< 5	1%
5 or more	2%

Inline Device Service 15-Minute Commitment	
Monthly Failures	Service Credit Percentage
< 5 occurrences	10%
5 or more occurrences	25%

(b) Remedies. In the event that Alert Logic fails to provide a Service at the level required by the Service Level Warranty, Customer's only remedies are those set forth in this service Level agreement (the "Remedies"). For Services purchased as part of a suite, the Service Credit will be based on the pro-rata portion of the cost of the Service, as determined by Alert Logic in its reasonable discretion.

(c) Customer Must Request Remedies. In order to receive any of the Remedies, Customer must notify Alert Logic via email to AR@AlertLogic.com within seven (7) days from the time Customer becomes eligible to receive such Remedies. Failure to comply with this requirement will forfeit Customer's right to receive such Remedies.

(d) Remedies Shall Not Be Cumulative; Maximum Remedy; No Remedies if Delinquent. The Remedies set forth herein are not cumulative. The aggregate maximum Remedy for any and all failures to provide Services at the level required that occur in a single calendar month shall not exceed one calendar month of service credit. If Customer is late in making any payments owing pursuant to this MSA at the time of the occurrence which would otherwise entitle Customer to Remedies, none of such Remedies shall be available to Customer.

(e) Termination Option for Problems. Customer may terminate this MSA if the Customer experiences Chronic Problems. Chronic Problems shall mean two (2) or more service level warranty deficiencies that are properly reported and credited within a three (3) month calendar period, as specified within this Service Level Agreement. The Submitted Service Requests 2-Hour Response Commitment is specifically excluded from qualifying as Chronic Problems. Customer must provide Alert Logic written notice of termination for Chronic Problems in writing within seven (7) days from the time Customer becomes eligible to terminate for Chronic Problems.

(f) The Service Level Warranty set forth in this Service Level Agreement does not apply to (i) any Custom Services; or (ii) any Services that expressly exclude this Service Level Warranty (as stated in the Order Form or Statement of Work for such Services).

EXHIBIT A5

Managed Security Services for Data Centers

1.0 MANAGED SECURITY SERVICES FOR DATA CENTERS PLANS

MSSDC plans are listed below. These plans may be amended at any time to add, change or remove services and provide updated plans. Core service functionality for plan components is described herein. Please refer to www.eSecuritySolutions.com for the latest plan services components.

1.1 APPROACH

eSecurity Solutions provides Managed Security Services and ongoing maintenance and support for servers and network devices in Data Center environments. As part of security, the availability of services and data is critical to most organizations. eSecurity Solutions goal is to provide best practices security and high availability for your organization Data Center infrastructure.

eSecurity Solutions provides 3 Levels of managed services for Data Center environments:

- **Bronze** – Automated monitoring and alerting of critical issues that affect the health of your servers and network devices. Windows servers also included Microsoft updates (with automatic reboots) and routine maintenance either scheduled weekly or monthly based on your maintenance windows. All additional services are billed hourly.
- **Silver** - Automated monitoring and alerting of critical issues that affect the health of your servers and network devices. Windows servers also included scheduled Microsoft updates (with automatic reboots) either weekly or monthly based on your maintenance windows. NOC services (during normal business hours – 8 x 5) are included with operating systems monitoring, maintenance and tuning, Active Directory maintenance, data/system backup monitoring and maintenance, and monitoring and maintenance of antivirus/antimalware endpoint protection. All additional services are billed hourly.
- **Gold** - Automated monitoring and alerting of critical issues that affect the health of your servers and network devices. Windows servers also included scheduled Microsoft updates (with automatic reboots) either weekly or monthly based on your maintenance windows. NOC services (24 x 7 x 365) are included with operating systems monitoring, maintenance and tuning, Active Directory maintenance, data/system backup monitoring and maintenance, and monitoring and maintenance of antivirus/antimalware endpoint protection. All additional services will be hourly.

1.2 BRONZE MSSDC

Bronze level MSSDC (Managed Security Services for Data Centers) are designed to assist your IT administrators by automating routine tasks performed in your Data Center. Bronze level MSSDC utilizes our automated monitoring and maintenance tools to provide basic health monitoring for Network Devices and Servers and Operating System maintenance and patching for Windows Servers. All alerts/notifications are sent to users in your organization that you have designated as well as the eSecurity Solutions team which will review any high or critical severity alerts during normal business hours and escalate to your organizations primary point of contact. Your organization may utilize eSecurity Solutions for performing maintenance and remediation under our Professional Services hourly rates.

1.2.1 SCOPE

Silver level MSSDC services are limited to:

- Automated monitoring and alerting of critical issues that affect the health of your Servers and Network Devices

- Windows Servers updates and patching (with automatic reboots) scheduled to run automatically either weekly or monthly based on your maintenance windows
- Automated tasks for Windows Servers to conduct routine maintenance to improve performance and reliability
- Review of critical and high severity System Health alerts (8 x 5) and escalation to your organizations point of contact

1.3 SILVER MSSDC

Silver level MSSDC (Managed Security Services for Data Centers) are designed to assist your IT administrators by automating routine tasks performed in your Data Center and provide 8 x 5 NOC (Network Operation Center) support for Windows Operating Systems, Active Directory, and supported Network Devices and Backup and Recovery solutions. Silver level MSSDC utilizes our automated monitoring and maintenance tools to provide basic health monitoring for Network Devices and Servers and Operating System maintenance and patching for Windows Servers. All alerts/notifications are sent to users in your organization that you have designated as well as the eSecurity Solutions team which will review any high or critical severity alerts during normal business hours and escalate to your organizations primary point of contact. Your organization may utilize eSecurity Solutions for performing maintenance and remediation under our Professional Services hourly rates.

1.3.1 SCOPE

Silver level MSSDC services are limited to:

- Automated monitoring and alerting of critical issues that affect the health of your Servers and Network Devices
- Windows Servers updates and patching (with automatic reboots) scheduled to run automatically either weekly or monthly based on your maintenance windows
- Automated tasks for Windows Servers to conduct routine maintenance to improve performance and reliability
- Review of critical and high severity System Health alerts (8 x 5) and escalation to your organizations point of contact
- Active Directory maintenance including adding/removing users and groups, changes to Group Policies and Objects, maintenance of the internal DNS server for Active Directory, and changing permissions on network shares
- Monitoring and maintenance of “supported” Network Devices
- Monitoring and maintenance of “supported” Backup and Recovery solutions
- Disaster recovery using “supported” Backup and Recovery solutions
- Monitoring and maintenance of “supported” Endpoint Protection

Note: See SLA for “supported” solutions

1.4 GOLD MSSDC

Gold level MSSDC (Managed Security Services) for Data Centers are designed to assist your IT administrators by automating routine tasks performed in your Data Center and provide 24 x 7 x 365 NOC (Network Operation Center) support for Windows Operating Systems, Active Directory, and supported Network Devices and Backup and Recovery solutions. Gold level MSSDC utilizes our automated monitoring and maintenance tools to provide basic health monitoring for Network Devices and Servers and Operating System maintenance and patching for Windows Servers. All alerts/notifications are sent to users in your organization that you have designated as well as the eSecurity Solutions team which will review any high or critical severity alerts during normal business hours and escalate to your organizations primary point of contact. Your organization may utilize eSecurity Solutions for performing maintenance and remediation under our Professional Services hourly rates.

1.4.1 SCOPE

Gold level MSSDC services are limited to:

- Automated monitoring and alerting of critical issues that affect the health of your Servers and Network Devices
- Windows Servers updates and patching (with automatic reboots) scheduled to run automatically either weekly or monthly based on your maintenance windows
- Automated tasks for Windows Servers to conduct routine maintenance to improve performance and reliability
- Review of critical and high severity System Health alerts (24 x 7 x 365) and escalation to your organizations point of contact
- Active Directory maintenance including adding/removing users and groups, changes to Group Policies and Objects, maintenance of the internal DNS server for Active Directory, and changing permissions on network shares
- Monitoring and maintenance of “supported” Network Devices
- Monitoring and maintenance of “supported” Backup and Recovery solutions
- Disaster recovery using “supported” Backup and Recovery solutions
- Monitoring and maintenance of “supported” Endpoint Protection

Note: See SLA for “supported” solutions

2.0 Requirements for MSSDC

2.1 RMM (Remote Monitoring and Management) Requirements

RMM tools allow for secure remote management and monitoring of network devices and Windows Servers. eSecurity Solutions utilizes a tool called Managed Workplace for RMM (we reserve the right to change RMM tools). The MWOM (Managed Workplace Onsite Manager) must be install on a Windows Server in your organizations Data Center.

2.1.1 Managed Workplace Onsite Manger Requirements

MWOM must be install on a Windows Server. The server can be multipurpose as long as resources are available for MWOM. Do not install Onsite Manager on a MS Exchange, MS SQL, or MS HyperV Host server.

The minimum hardware requirements (physical or virtual) and software requirements include:

- Minimum 8 GB of RAM free for MWOM
- 50 GB of Free Space for MWOM
- Windows Server 2008 R2 or above
- Windows Install 4.5
- MBSA 2.3 (Microsoft Base Line Analyzer)
- Microsoft SQL Server 2014 Express (included with the Onsite Manager installation)
- Microsoft .NET Framework 4.6 or above

2.1.1.1 Network Requirements

Outbound (Internet) Access for MWOM:

- HTTP (TCP 80) and HTTPS (TCP 443) to
 - us01.ccrmm.avg.com
 - www.whatismyip.com

Internal Network Communications from MWOM to network devices and servers:

- DNS (UDP 53)
- WMI (TCP 135 & TCP 445)

- SNMP (TCP 161 and UDP 162)
- SNMP Traps (UDP 162)
- Syslog (UDP 514)
- RDP (TCP 3389)

2.2 Windows Servers Requirements

Windows Servers must be running on Microsoft Windows 2008 R2 and above. Windows Servers are monitored using WMI and managed with RDP; appropriate permissions and host firewall setting must be in place to allow management of the Windows Servers.

2.3 Other Servers Requirements

Linux Servers must be running a currently supported version (able to receive new updates and patches from the vendor). Linux Servers are monitored using SNMP and managed with SSH; appropriate permission and host firewall settings must be in place to allow management of the Linux Servers.

2.4 Network Devices Requirements

Network Devices including Firewalls, Routers, Switches, and NAS must be running a currently supported version (able to receive new updates and patches from the vendor). Network Devices are monitored using SNMP and managed via SSH and HTTPS (in some cases only Telnet and HTTP is supported); appropriate permission and host firewall settings must be in place to allow management of the Network Devices.

eSecurity Solutions provides support for modify settings and policies on the following Network Devices:

- Firewalls – Watchguard, Fortinet, and Sophos
- Switches – Netgear, D-Link, Brocade, and HP
- NAS – Netgear and Synology

2.5 Backup and Recovery Requirements

Backup and Recovery solutions must be running a currently supported version (able to receive new updates and patches from the vendor). Support Backup and Recovery supported solutions include Infrastack Disaster Recovery, Unitrends Recovery, DATTO Siris, and AVG Cloud Backup (see SLA for full details). Backup and Recovery solutions are monitored using SNMP and managed via SSH and HTTPS; appropriate permission and host firewall settings must be in place to allow management of the Backup and Recovery solutions.

2.6 Endpoint Security Requirements

Endpoint Security is required for most Windows Servers (exceptions are made for system where Antivirus/Antimalware significantly impacts the operation of applications such as HyperV Hosts and SQL Servers). AVG and Kaspersky Endpoint Protection (Business Editions) are supported.

3.0 SLA

Note: Certain items within SLA do not pertain to Bronze level MSSDC.

3.1 SYSTEM HEALTH

- Monitor, review, and respond to critical and high severity health issues for systems including CPU, RAM, network connection, disk space, and server services
 - Notification emails are sent to Customer via email (24 x 7 x 365) if requested
 - Services tickets are created for all actionable items related to health issues

- eSecurity Solutions response team reviews tickets within 4 hours of creation during normal Business Hours (or 24 x 7 x 365 for Gold level MSSDC)

WINDOWS SERVERS

- Operating System updates, patching, and routine maintenance is set to automatically run on a set schedule; monitor, review, and respond to critical and high severity health issues that arise
 - Notification emails are sent to Customer via email (24 x 7 x 365) if requested
 - Services tickets are created for all actionable items
 - eSecurity Solutions response team reviews tickets within 4 hours of creation during normal Business Hours (or 24 x 7 x 365 for Gold level MSSDC)
- Review and respond to customer change requests for Windows Server related to Operating Systems settings, Active Directory changes, and Group & Local Policy changes
 - Services tickets are created for all actionable items related to health issues
 - eSecurity Solutions response team reviews tickets within 4 hours of creation during normal Business Hours (or 24 x 7 x 365 for Gold level MSSDC for AVG only)
- Monitor, review, and respond to critical and high severity issues related to supported Endpoint Security solutions
 - Notification emails are sent to Customer via email (24 x 7 x 365) if requested
 - Services tickets are created for all actionable items related to health issues
 - eSecurity Solutions response team reviews tickets within 4 hours of creation during normal Business Hours

NETWORK DEVICES

- Firmware updates and patching is scheduled at an agreeable time between Customer and eSecurity Solutions; monitor, review, and respond to critical and high severity health issues that arise
 - Notification emails are sent to Customer via email (24 x 7 x 365) if requested
 - Services tickets are created for all actionable items
 - eSecurity Solutions response team reviews tickets within 4 hours of creation during normal Business Hours (or 24 x 7 x 365 for Gold level MSSDC)
- Review and respond to customer change requests for supported Network Devices settings and policy changes
 - Services tickets are created for all actionable items related to health issues
 - eSecurity Solutions response team reviews tickets within 4 hours of creation during normal Business Hours

BACKUP AND RECOVERY

- Configure backup for Customer specified files/folder to run automatically on a set schedule with a set retention policy
 - eSecurity Solutions support Infrascala Disaster Recovery, Unitrends Recovery, DATTO Siris, and AVG Cloud Backup
- Configure backup for Customer specified Server systems (Windows Servers or supported Virtual Machines) on a set schedule with a set retention policy
 - eSecurity Solutions support Infrascala Disaster Recovery, Unitrends Recovery, DATTO Siris, and AVG Cloud Backup
- Configure backup for Customers specified MS Exchange Servers on a set schedule with a set retention policy
 - eSecurity Solutions support Infrascala Disaster Recovery and DATTO Siris
 - Customer must purchase the required licenses for MS Exchange backup support
- Configure backup for Customers specified MS SQL Servers on a set schedule with a set retention policy

- eSecurity Solutions support Infrascala Disaster Recovery and DATTO Siris
 - Customer must purchase the required licenses for MS SQL Server backup support
- Monitor, review, and respond to critical and high severity issues related to backup
 - Notification emails are sent to Customer via email (24 x 7 x 365) if requested
 - Services tickets are created for all actionable items
 - eSecurity Solutions response team reviews tickets within 4 hours of creation during normal Business Hours (or 24 x 7 x 365 for Gold level MSSDC for DATTO Siris)
- Recovery during an outage or disaster
 - Restore file/folders due to server disaster, data corruption, or loss of entire segment of data
 - Restore Server system due to server disaster or outage
 - Restore MS Exchange database due to disaster
 - Restore MS SQL Server database(s) due to disaster

3.2 Customer Responsibilities

Customer is responsible for any items are not covered in the Scope MSSDC for the level of service they subscribe (Bronze, Silver, or Gold). Customer must have an IT administrator for a point of contact and resources available for “hands-on” access at your Data Center. eSecurity Solutions offers Professional Service to perform these projects or to assist in most situations. Consult with eSecurity Solutions for more information.

- Application installation, maintenance, monitoring, and support
- Hardware installation, maintenance, support, and upgrades
- Designing, planning, and architecting of networks and servers
- Acquisition and implementation of new Servers and Network Devices
- Active Directory installation, migration, and upgrades
- MS Exchange Server installation, maintenance, support, migrations, and upgrades
- MS SQL Server installation, maintenance, support, migrations, and upgrades
- IIS and other Web server installation, maintenance, support, and upgrades
- Recovery of data in none outage or disaster situations
 - Users delete or overwrite files or folder
 - Users need access to email that has been deleted or lost
 - Users want to recover database for testing, trouble shooting, or other none disaster related needs

4.0 Support

Customer support related to the contracted services will be provided during for following times and availability. Support is provided either by email, online ticketing system or by phone.

Below are the terminologies used for support services.

Definition	Days	Service Timings	Availability
Business Hours (Covered under your chosen support Plan)	Monday through Friday	8:00 am PST to 6:00 pm PST	Yes, email and phone
Business Hours (Not Covered under your chosen support Plan)	Monday through Friday	8:00 am PST to 6:00 pm PST	\$175 per hour (Discounted Rate)
Off Business Hours	Monday through Friday	6:00 pm PST to 8:00 am PST	Emergency Service available at \$250 per hour
Weekend Hours	Saturday and Sunday	6:00 pm PST Friday to 8:00 am PST Monday	Emergency Service available at \$250 per hour
24x7 Premium SOC Response	Monday through Sunday	24 x 7	Included with Gold level MSSDC only

EXHIBIT A6

Other Security Managed Services

1.0 MANAGED SERVICES OF OTHER SECURITY PRODUCTS

Managed services of products not specified by other Exhibits will conform the following. These plans may be amended at any time to add, change or remove services and provide updated plans. Core service functionality for plan components is described herein. Please refer to www.eSecuritySolutions.com for the latest services. Unless otherwise specified in the provided Sales Order, services provided will generally comply with the following.

2.0 DETAILED SCOPE OF SERVICES (All Plans)

2.15 Account Provisioning: The following is managed related to customer licenses.

2.15.1 Policy definition and creation based upon customer input

2.15.2 License management

2.16 Flex Billing: Flex Billing allows customers to pay monthly, quarterly or annually to match their cash and expense requirements. Payment, plan terms and adjustments are described in the Base Services agreement.

2.17 Support: Tier 1 Support provided by Company trained staff.

2.17.1 **Tasks include**

2.17.1.1 Responding to customer:

2.17.1.1.1 Installation questions

2.17.1.1.2 Operational questions

2.17.1.1.3 Installation change questions

2.17.1.1.4 Product questions

2.17.2 **Scope / SLA:**

- Issues will create alerts to Company escalation contacts based on the priority of the incidents.
- Alerts will be first analyzed by the Company response team and actionable alerts will be converted to tickets and responded to within the contracted response agreement timeframe.
- Actionable alerts are responded to within four (4) hours during Business Hours (see definition).
- Online reports will reflect system status and any system recorded alerts (See Reporting)
- For any incidents that require on-site presence or actions, Customer will be contacted for resolution.
- Customer support related to the contracted services will be provided during for following times and availability. Support is provided either by email, online ticketing system or by phone.
- **Custom Services Requests** will be billed at \$250 per hour or quoted on a project basis upon request.

Below are the terminologies used for support services.

Definition	Days	Service Timings	Availability
Business Hours	Monday through Friday	8:00 am PST to 6:00 pm PST	Yes, email and phone
Off Business Hours	Monday through Friday	6:00 pm PST to 8:00 am PST	Emergency Service available at Custom Services Hourly Rate
Weekend Hours	Saturday and Sunday	6:00 pm PST Friday to 8:00 am PST Monday	\$250 per hour

Note: All hours mentioned are client local U.S. hours.

2.18 Installation, Deployment, Setup, Configuration, Maintain and Adjust

2.18.1 Tasks include

- 2.18.1.1 Customer survey or interviews re: setup and policy requirements
- 2.18.1.2 Installation and setup of software, hardware, management and agents
- 2.18.1.3 Coordination with customer personnel re: any issues that facilitate installation
- 2.18.1.4 Setup and configuration of management, alerts and client agents per best security practices
- 2.18.1.5 Adjustments to security policy per customer driven requests or circumstance changes.
- 2.18.1.6 Install software agent updates as required to provide appropriate functionality
- 2.18.1.7 Testing and monitoring post install

2.18.2 Scope / SLA:

- Issues will create alerts to Company with escalation and management per Support SLA.

2.18.3 Customer Responsibility

Customer should make sure that the following things are provided to make sure that this service is installed and delivered uninterrupted

- Customer must complete the Customer survey providing accurate information related to the necessary environment and requirements so that service may be configured properly.
- Customer to provide a single point of contact for installation configuration requirements.
- Customer must provide a server computer suitable for installation of the management server (if required) in the Customer environment with the remote guidance of Company' managed services staff. Not required for hosted management solutions.

2.19 Security Functionality

2.19.1 Tasks Include

- Setup security solution to provide Sales Order defined security functionality

2.1 Monitor and Alert

The goal of managed services is to provide security services without the need for customer involvement on a daily basis. However, alerts to Customers is provided whenever it is necessary or deemed important as described below.

2.19.2 Tasks include monitoring customer installation to ensure:

- Installed clients are online
- Installed clients are at current software levels
- Installed clients have current detection pattern updates installed
- Client licenses are current and functioning
- Security events are managed and remediation has occurred (log report inspection)
- Security Threats are mitigated
- User Policy Violations are managed and alerted if necessary

2.19.3 Event Log Monitoring Scope / SLA:

- Monitoring is 24 x 7 and responded to automatically based upon the incident priority.
- Issues will create alerts to Company with escalation and management per Support SLA.

2.19.4 Deliverable

Actionable alerts will be prioritized and worked to resolution. Alerts will be delivered as soon as is practicable to Customers to notify customer of potential issues and action responses required when required.

2.20 Reporting and Reporting Assistance

The type of reporting depends on the security solution installed. This might be delivered via online report portal, local management software accessible to customers or via reports sent to customers by Company. Certain information is on demand and available as requested by customers normally available once per month within 24 hours of requests.

EXHIBIT B
COMPANY, LLC ACCEPTABLE USE POLICY

Company, Inc. (“**Company**”) has formulated this Acceptable Use Policy (the “**Policy**”) in order to encourage the responsible use of the services (the “**Company Service**”) provided by Company to our users (“**Users**”), and to enable us to provide Users with secure, reliable and productive service.

General Conduct

The Company Service must be used in a manner that is consistent with the intended purpose of the Company Service and may only be used for lawful purposes. Users shall not use the Company Service in order to transmit, distribute or store material: (1) in violation of any applicable law or regulation, including export or encryption laws or regulations; or (2) that may expose Company to criminal or civil liability. Users are further prohibited from assisting any other person in violating any part of this Policy.

Usage Restrictions

Usage of the Services and underlying licensed software and products shall be limited to the licensed quantity which shall not exceed that amount for the number of seats, users, sites or other licensing criteria defined in the Sales Order. Use of the Services and licensed software shall be limited to the Customer’s employees, agents and locations as defined in the Sales Order.

Responsibility for Content

Company takes no responsibility for any material created or accessible on or through the Company Service. Company is not obliged to monitor or exercise control over such material, but reserves the right to do so. In the event that Company becomes aware that any such material may violate this Policy and/or expose Company to civil or criminal liability, Company reserves the right to block access to such material and suspend or terminate service with respect any User creating, storing or disseminating such material. Company further reserves the right to cooperate with legal authorities and third parties in the investigation of alleged wrongdoing, including disclosing the identity of the User that Company deems responsible for the wrongdoing.

Inappropriate Content

Users shall not use the Company Service to transmit, distribute or store material that is inappropriate, as reasonably determined by Company, or material that is indecent, obscene, pornographic (including child pornography), defamatory, libelous, threatening, abusive, hateful or excessively violent.

Intellectual Property

Material accessible through the Company Service may be subject to protection under privacy, publicity or other personal rights and Intellectual Property rights including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Company Service in any manner that would infringe, violate, dilute or misappropriate any such rights. If you use a domain name in connection with the Company Service you must not use that domain name in violation of the trademarks, service marks, or similar rights of any Third Party.

Harmful Content

Users shall not use the Company Service to transmit, distribute or store material that contains a virus, worm, Trojan horse or other component harmful to the Company Service or any other Users.

Fraudulent/Misleading Content

Users shall not use the Company Service to transmit or distribute material containing fraudulent offers for goods or services, or any advertising or promotional materials that contain false, deceptive, or misleading statements, claims, or representations. Users are prohibited from submitting any false or inaccurate data on any order form or online application, including the fraudulent use of credit cards.

Unsolicited Messages

Sending unsolicited mail messages, including, without limitation, commercial advertising and informational announcements, is explicitly prohibited. A User shall not use another site’s mail server to relay mail without the express permission of the site.