

## EMBARQ® MANAGED SECURITY SERVICES ANNEX

The following terms and conditions, together with the applicable Embarq cover agreement, end-user license agreement, and the Embarq Standard Terms and Conditions for Communication Services (collectively, the “Agreement”) govern Embarq’s provisioning and Customer’s use of the managed virtual private network, monitoring, and firewall services (“Services”) specified in the Agreement.

1. **SERVICE DESCRIPTION.** Services include monitoring and managing Customer’s physical equipment described in the Agreement (“Devices”) and perform Device-specific trouble resolutions. Services are provided by United Teleservices, Inc.
2. **ORDER TERM.** The order term for the Services will be stated on the Order and will begin on the first day of the billing month following the date Services are installed and available to Customer (“Order Term”). At the end of the initial Order Term, the Order Term will automatically renew for successive one-year periods, for the same Services, at the then-current monthly recurring charges for a one-year service period, unless either party terminates the Services by providing the other party 30 days’ written notice of termination before the end of the initial Order Term or during any renewal Order Term. Upon termination or expiration of the Order Term, Customer agrees to return to Embarq any hardware and software (other than if Customer has purchased such hardware and software from Embarq) which Embarq has provided to Customer in connection with the Services.
3. **EARLY TERMINATION FEE.** Embarq will charge Customer an early termination fee of 50% of the remaining amounts owed to Embarq under the Agreement if Customer terminates the Services before the end of the initial Order Term or any successive Order Term.
4. **SERVICE FEATURES.**
  - 4.1. **Options.** Services are provided under either of the following feature options.
    - A. **Monitoring and Notification Feature.** This option provides Customer with the monitoring of the up/down status of Devices by remote polling via ICMP PING. Monitoring is provided and performed over the Internet to static IPs that are publicly addressed and reachable from Embarq or its designated agents’ monitoring operations center. This option also includes the receipt of alarms based upon thresholds established for simple network management protocol (“SNMP”) data and includes other SNMP-generated events, such as traps. In addition, to up/down status, this Service feature includes managed device asset tracking, trouble ticket access, and performance reporting with near-real time access to this information via an Embarq-branded secured web portal provided for Customer to access Service-related information (“Branded Web Portal”). All notifications are automated email and/or pager, and sent to Customer’s designated personnel.
    - B. **Comprehensive Managed Security Service Feature.** This option includes all of the components of the Monitoring and Notification Feature described above, and the ability to receive live notifications via telephone on a 7x24x365 basis. Embarq performs trouble isolation of incidents and escalates issues to Customer on a per Device basis. If required, Customer will provide Embarq and its agents a letter of agency (“LOA”) to provide Service on Customer’s behalf. Embarq tracks all incidents to resolution and posts the status in a trouble ticket that Customer can access via the Branded Web Portal. Customer may also add information to trouble tickets. For issues that may not have been automatically generated, such as maintenance related events, Customer can create and submit trouble tickets. In addition, Customer may also submit change requests to modify or enhance their network or services via the Branded Web Portal. Telephone access to Embarq is included as a part of this package via an Embarq call center. This option includes Fault Management, Configuration Management, Change Management, and the Life Cycle Management for Devices under management

by Embarq. Customer permits Embarq to take read and write control of Devices and manages their configurations. Embarq tracks the progress of problems to resolution, and manages the break/fix agencies actions on Customer's behalf in support of equipment sold to Customer by Embarq. Customer will provide Embarq with the appropriate access, authority and necessary contact and account information to the maintenance, replacement and support accounts for each Device under the Services.

- C. In order to purchase the Services, Customer must purchase equipment maintenance support either from Embarq or another, recognized equipment maintenance provider. If Customer purchases Embarq Centurion maintenance service, Embarq will provide break, fix and repair coordination and support on the Device in accordance with Customer's maintenance agreement with Embarq.

**4.2. Individual Function Descriptions.** Customer may select the scope and depth of network monitoring and management support required based on the specific Device. These managed security levels provide functions that deliver support for the End Users' network management needs. Service includes set-up, security monitoring, security event notification and security reporting, IPS configuration, IPS Signature set-up, IPS Signature Update, and IPS management and reporting. Certain Services are configured in conjunction with Customer. Customer will be responsible for providing specific guidance to Embarq on any changes to any supporting equipment. The following information describes certain functions available under either of the Service options described in Section 4.1 above.

- A. **Product Upgrades.** Many Devices may be upgraded by adding remote VPN clients, depending on the model. To do so, Customer must Embarq to upgrade the firewall license and add remote VPN clients in five-unit bundles.
- B. **Configuration Management.** For purposes of this Annex, Configuration Management is the management of security features though control of changes made to the Device throughout the Order Term. Embarq will support the following functions as part of maintaining End User information:
  - (1) Create and maintain a database of Device configurations.
  - (2) Store current Device configurations and implement configuration reloads for re-initialization of Devices.
  - (3) Capture and maintain an inventory of assets per Customer location for Devices contracted for Services by Customer, maintain Customer site contact information, and track changes per location via Branded Web Portal.
  - (4) Perform tracking and logging for change requests.
- C. **Security Monitoring Services.** Embarq will provide event monitoring, which includes the following or similar services for Devices.
  - (1) Device availability to include up/down status monitoring, connection up/down status monitoring, location unreachable and location reachable. Embarq will set the monitoring levels at default unless otherwise specified by Customer. The value for an event threshold can be set at the Device level.
  - (2) Each Device is polled on a regular basis to determine if it is accessible by Embarq via the Internet. A Device will be classified as "going down" once it has missed a minimal number of cycles (three one minute polls). If the Device does not respond to six (6) consecutive polls (under 20 minutes), Embarq deems the service "down". Embarq will alert Customer once a Device has been classified to be in a "down" status via an email notification and/or phone call (i.e., ticket alert) within (10) minutes of the "down" status determination. Embarq will send an email to Customer via a Customer-designated email address to ascertain if the Device has been unplugged or if Customer has power

to the Device. Embarq will escalate service down condition after completion of the above steps. For managed Devices, Embarq will initially troubleshoot the Device to determine if the Device is operational by trying to connect with the Device. Tickets updates will be provided when new information is available on the ticket alert.

- (3) Device SNMP Threshold Events to include the following:
  - (a) Device Level - operational status, availability, CPU utilization, memory utilization, and environmental (Cisco Only).
  - (b) Port Level - operational status, packet loss levels, error levels, and load levels.
  - (c) Logical Connection (PVC, etc.) – operational status and load levels.
- (4) Security Events (SNMP and Syslog). The SNMP (via SNMP Gets and Traps) and Syslog Events will be for the Cisco Firewall and Cisco IOS Firewall (IOS) alarms are summarized into several types as follows: firewall system events, firewall interface events, failover events (PIX only), security events, intrusion detection system (IDS) events, IOS FW events, IPS events, and IOS IPS events.

**D. Site-to-Site VPN Management Support.** The following VPN events and conditions are monitored under this function.

- (1) VPN Router Up/Down Status Monitoring. The up and down status is determined by polling the router on a 3-minute interval using a single IP address. If a VPN router misses two IP polls, then Embarq generates a ticket. Embarq may update the polling intervals with notice to Customer.
- (2) VPN Connection Up/Down Status Monitoring –The Up and Down status is monitored through ICMP Polling and SNMP events and traps.
- (3) Serial Port Interface – Each serial port interfaces is monitored for an up/down state change and/or a link up/down state change. A ticket will be generated for a failure of a serial interface on a router or the loss of the physical connection to the network.
- (4) Ethernet Interface – An alarm will be generated with the failure of an Ethernet interface on the router. Embarq will generate ticket events for Cisco Environmental conditions including Device Voltage Status, Device Temperature Threshold Exceeded, Device Fan Failure, Redundant Power Supply Failure, and Flash Device inserted or removed. Embarq will also generate a ticket for HSRP and BGP state changes including HSRP Status Change and BGP Status Change. In order to generate these alarms the device must be active and present in the End User’s network in order to generate events. Embarq will also generate tickets for Module Status, Device Reset, Power Status and Module Insert/Removal.

**E. Remote VPN Management Support.** Embarq will provide remote IPSEC and SSL VPN monitoring and management as specified below. Any web interface configuration and implementation for the SSL VPN configuration required by Customer will be provided on a Time and Material basis at an Embarq-specified, per hour rate.

- (1) Configuration Management. This function provides the following capabilities: add/modify routes and interfaces, manage users and groups, backup and restoration of configurations, user profile management for remote users, provide

configuration validation and testing, security policy enforcement, configuration of VPN tunnels, configure high availability, configure authentication method, configure IP address management, IOS upgrades, and provide backups of configuration files.

- (2) Performance Management and Reporting. This function also provides the following management and reporting capabilities on VPN activity: user activity, CPU utilization, memory utilization, and anomaly detection

**F. Firewall Management.** Embarq provides monitoring and management services for deployed firewalls. Not all features and functions are available on all firewall vendors or models. Embarq only supports the features available on the deployed Device. A summary of the areas that may be configured and supported under this agreement are provided below.

- (1) Address Translation Functions - Network Address Translation (NAT), Port Address Translation (PAT), Static Translation, and Dynamic Port Mapping
- (2) Access Control (AAA Integration) Functions - access Control Lists (ACL), Terminal Access Controller Access Control System Plus (TACACS+), and Remote Authentication Dial-In User Service (RADIUS) servers.
- (3) Attack Protection Features - Reverse Route Look-up, Mail Guard, DoS Detection and Prevention or Flood Guard, FragGuard and Virtual Reassembly, DNS Control, ActiveX Blocking, Java Filtering, and Configurable Proxy Pinging.
- (4) Specific Protocols and Applications Support - Advanced Application Inspection and Control (ability to define and enforce security policies for port 80, control misuse of port 80 by rogue applications that tunnel traffic inside HTTP and use port 80 to avoid scrutiny, perform protocol anomaly detection services, HTTP Inspection Engine, and email inspection engine - SMTP/ESMTP/POP3/IMAP), Firewall Voice Traversal, Multimedia Applications, LDAP Version 2 and ILS, NetBIOS over IP, and Forwarding Multicast Transmissions.
- (5) Other Firewall Features Supported - Audit Trail, Real-Time Alerts, Event Logging, Secure Shell Version 2, Simple Network Management Protocol Version 3 (SNMPv3), and 802.1x.

**G. Cisco IOS Firewall Support.** Embarq supports the following features for the Cisco IOS (available for Cisco ISR routers).

- (1) Cisco IOS Firewall Engine (inspection of router local traffic and ICMP inspection)
- (2) Advanced Application Inspection and Control (HTTP Inspection engine and email inspection engine - SMTP/ESMTP/POP3/IMAP), Advanced Application Inspection and Control, Firewall Voice Traversal, DoS Detection and Prevention, Dynamic Port Mapping, Basic and Advanced Traffic Filtering, Network Address Translation (NAT), Real-Time Alerts, Event Logging, and Simple Network Management Protocol Version 3 (SNMPv3).

**H. Intrusion Prevention Service (“IPS”) Support.** Embarq provides management, administration, and security monitoring of deployed IPS solutions. The management and administration functions include remote administration, configuration, signature

management, and IPS software maintenance (patches, upgrades). Support includes IPS configuration, IPS Signature set-up, IPS Signature Update (monthly), IPS management and reporting.

- (1) Signature File Update Support. Embarq will initiate the update of the IPS Signature files within one (1) Business Day after notification that a new signature file is available and Embarq has reviewed and evaluated the IPS update, and provide notice to Customer of the update. Customer may reject that Embarq suspended the new update via a change request submitted to Embarq. This update support includes the IPS signature files that are provided by the Device vendor. This support option is available for multi-purpose Device in conjunction with firewall functionality.
- (2) Managed Host-Based IDS Support. Embarq provides management, administration, and security monitoring of deployed host-based intrusion detection systems (“HIDS”). The management and administration functions include remote configuration, attack signature management and HIDS software maintenance (patches, upgrades) for HIDS managers and the HIDS agents. Embarq or its agents will be the sole administrator of the HIDS Manager device. For systems that HIDS agents reside on, Embarq requires remote access to the Device with a level of system access that will allow for full application administration of the HIDS agent application. Embarq does not desire full system administrative access to systems with HIDS agents, and does not assume liability or responsibility for the core operating system components or other applications beyond the HIDS agent application that reside on a managed HIDS device. Embarq does not provide Customer with administrative access to the server supporting the HIDS Manager, but does have exclusive administrative access to any application servers monitored by a HIDS agent.
- (3) Feature Support. Embarq will support currently-supported Cisco IPS Software that is actively supported at Cisco. Feature availability for other releases will vary. Embarq will support the most current version of IPS deployed by Cisco.
- (4) IOS IPS Feature Support. Embarq will support the IOS IPS feature as deployed.

#### **4.3. Platform Updates.**

- A. Embarq or its agents will provide platform-specific software updates to correct material problems as and when updates are available from the software manufacturer or another applicable vendor. In case of emergency updates or updates highly recommended by the software manufacturer as critical Embarq or its agents will attempt to notify Customer at least 24 hours prior to the update via email to both their normal and emergency email address and provide prior notification. Embarq will provide regular or routine updates on a quarterly basis. Regular/routine updates will be performed on the first Friday of every quarter at 9PM Eastern Standard/Daylight Time (EST/EDT) or at a mutually agreeable time and date between Embarq (or its agents) and Customer.
- B. Embarq or its agents will access the managed Devices remotely to review hardware status and logical configuration condition. Embarq will engage vendor support as needed to resolve logical network configuration issues.

#### **4.4. End User Change Requests.**

- A. Embarq will allow End Users to submit 4 Customer-requested Change Requests per Device, per month to Embarq via the Branded Web Portal. Allocated Change Requests

are not carried over if unused to the next month or months. For purposes of this Annex, a Change Request is a configuration change to the setting of the Device and may include multiple types of actions (i.e., add user to the access list, delete a user and change user passwords on the firewall). Additional Customer-requested Change Requests will be fulfilled on a Time and Material basis at an Embarq-specified, per hour rate, subject to the Time and Materials Project Annex, as posted to [www.embarq.com/ratesandconditions](http://www.embarq.com/ratesandconditions). This includes site add, move and deletion as well as feature changes, policy changes or address changes as well as logical configuration changes (e.g., ACL changes and change priority queuing parameters). Because of the variety of change requests Customer may make, Customer is responsible for ensuring the Change Request is appropriate for its environment. In addition, Change Requests implemented to support the integration of the managed systems with non-managed systems require Customer to determine and provide any configuration specifics necessary.

- B.** Embarq will provide a qualified engineer to perform requested changes, but it is assumed that the work involved will not require more than 1 hour per single Change Request. If a single Change Request has such a volume of work surrounding it, that it exceeds this time allotment, then the action will be counted as multiple change requests with regards to change request limits per month and costs. Embarq will identify any excessive change request situation upon submittal of the Change Order. Embarq, where possible, will notify Customer of this situation and any potential cost implications of the submitted request prior to implementing the request.
- C.** Change Requests can include multiple types of actions. Examples of configuration Change Requests are password resets or changes (for the security appliance), password resets or changes (for Branded Web Portal access), user modifications (add a user to the access list; delete a user; change a user's access), request rule change to access lists of the security appliance, adding a new user with VPN client to the security appliance, and adding a new VPN tunnel. Change Requests do not include moves, additions and changes ("MAC") of Customer hardware and software that are managed by the Service.
- D.** Embarq may implement Change Requests during non-maintenance windows as appropriate and as other, prioritized Change Requests permit. If Embarq implements a change that impacts Customer during a non-maintenance window, Embarq will provide Customer with advance notice, where possible, if the change is not based on Customer's request.
- E.** All Change Requests will be coordinated with Customer. As part of the change control process, Embarq will review configuration Change Requests for validity, load the Change Requests into Devices, develop back-out procedures to previous configuration, update the appropriate systems upon change implementation; billing, inventory configuration and management, and support Device access and change management
- F.** Customer may submit a Service Order Change Request via the Branded Web Portal. Embarq, in its sole discretion, may approve the change. For purposes of this Annex, a Service Order Change Request is a Customer-requested change that requires a configuration change of the Device or service that requires a contractual change to modify the Services and prices for the Services.

## **5. SERVICE PROVISIONING AND SUPPORT**

- 5.1.** Embarq will establish a standard configuration on each Device. This configuration will be loaded on each Device, unless this configuration is modified by Customer as part of the ordering process,

in which case the modified configuration will be loaded on the appropriate Device(s). Embarq's standard procedure is to allow all traffic out and deny all traffic into the firewall.

- 5.2. If Customer contacts Embarq to report a problem with a Device, Embarq will acknowledge the problem and provide a trouble ticket number to Customer via email. Embarq will perform remote diagnosis and will provide Customer with an estimated time to repair within two hours for urgent issues of the initial contact from Customer. Responses will be in email form and all updates will be visible via the Branded Web Portal.
- 5.3. Embarq will resolve platform-specific trouble cases on the following priority basis. But if a problem is turned over to the Customer or any Customer-designated third party or resolution during any phase of the response time, the resolution time period described below will cease. For purposes of this section, business day means Monday through Friday, excluding recognized federal holidays and days the office is closed for emergency reasons (i.e., force majeure events).
  - A. Critical Event. This event includes mission critical system, sensors, and security Devices, defined in writing between Customer and Embarq. Embarq's time frame to initially respond to Customer is within 120 minutes of the event.
  - B. Urgent Event. These are critical events that Customer and Embarq have mutually decided in writing do not require 24x7x365 notification. Embarq's time frame to initially respond to Customer is within the next business day following the event.
  - C. Routine Event. These are events that Customer and Embarq have mutually decided in writing may occur within typical Customer systems. Embarq's time frame to initially respond to Customer is within 3 business days following the event.
  - D. Management Events. These are Customer or Embarq-requested changes to Customer sensors. Embarq's time frame to initially respond to Customer is within 3 business days following the event.
  - E. Sensor Statistics. These are either attempted and rejected connections by protocol and IP or a summary of alerts by sensor and category. Embarq will provide this information to Customer via weekly reports posted to the Branded Web Portal.
  - F. SNMP Alerts. Embarq agrees that a limited set of SNMP alerts will be acknowledged and ticketed. Embarq will resolve and close these events on a best available efforts method and without any timelines for resolution. Embarq will acknowledge the alerts within 10 minutes following the event. Critical level events will be ticketed and acted upon within 30 minutes of Embarq's acknowledgement. All other events will be ticketed and acted upon within 45 minutes of Embarq's acknowledgement.

## 6. REPORTING.

- 6.1. **Embarq Reporting.** Embarq will provide Customer with monthly reports via the Branded Web Portal no later than the 15th calendar day following the close of each month. These reports will provide information on usage statistics and security events for the managed Devices. These reports will be available via the secure Branded Web Portal for twelve (12) months. Embarq has the right to add new report features or content to the report at any time, or remove existing report features or content, at its sole discretion.
- 6.2. **Customer Reporting Requirements.**
  - A. For Embarq to provide effective and accurate Services, Customer will be responsible for reporting the following critical events to Embarq: minimum of 24 hour notice of

scheduled network outages, minimum 24 hour notice of changes in the network architecture, and immediate reporting of suspected network attacks

- B.** Embarq will charge Customer a fee for each Customer failure to meet the notification requirements, and reserves the right to terminate Services and cause Customer to forfeit monitoring service fees paid up to the point of termination should there be multiple failures to meet the notification requirements listed above.

## **7. ADDITIONAL TERMS**

- 7.1.** Activities to complete the tasks described in this Annex are based on accurate and validated information provided by Customer. Should any of this information prove to be inaccurate, Embarq will evaluate the impact of the misinformation and may, if required, initiate a change in the Services. Changes may include changes in scope, schedule, and price. Embarq is not liable or responsible for any inaccuracies, errors or misstatements resulting from incorrect information provided by or through Customer or Customer's network devices, that later affect the End User's environment.
- 7.2.** Embarq and Customer understand and agree that the performance of Services may improve Customer's security posture. But Services can neither identify nor eliminate all risks by unauthorized or authorized parties to affect Customer's environment. Services are limited to the description in this Annex, and Embarq is not liable or responsible for modifications made to Customer's network implemented after completion of Services, whether or not the modifications result from the Services.