AT&T General Policies

For

AT&T Services Software & Professional Services Master Agreement

These AT&T General Policies are a binding part of the AT&T Software & Professional Services Agreement between Supplier and AT&T Services, Inc. (the "Agreement").

These General Policies:

1. Set forth specific obligations and prohibitions that govern certain aspects of the relationship between Supplier and AT&T;
2. Supplement and have the same force and effect as the terms and conditions of Supplier's Agreement;
3. Are not intended to be, and cannot be construed as a waiver of any obligations in Supplier's Agreement.

New or revised General Policies issued by AT&T in the future supersede the previous version of the applicable General Policies.

1. Access –

a. When appropriate, Supplier shall have reasonable access to AT&T's or AT&T's Customer's premises and computer systems during normal business hours, and at such other times as may be agreed upon by the Parties to enable Supplier to perform its obligations under this Agreement. Supplier shall coordinate such access with AT&T's designated representative prior to visiting such premises. Supplier will ensure that only persons employed by Supplier or subcontracted by Supplier will be allowed to enter AT&T's or AT&T's Customer's premises. If AT&T requests Supplier or its subcontractor to discontinue furnishing any person provided by Supplier or its subcontractor from performing Work on AT&T's or AT&T's Customer's premises, Supplier shall immediately comply with such request. Such person shall leave AT&T's or AT&T's Customer's premises immediately and Supplier shall not furnish such person again to perform Work on AT&T's or AT&T's Customer's premises without AT&T's written consent. The Parties agree that, where required by governmental regulations, Supplier will submit satisfactory clearance from the U.S. Department of Defense and/or other federal, state or local authorities.

b. AT&T may require Supplier or its representatives, including employees and subcontractors, to exhibit identification credentials, which AT&T may issue to gain access to AT&T's or AT&T's Customer's premises for the performance of Services. If, for any reason, any Supplier representative is no longer performing such Services, Supplier shall immediately inform AT&T. Notification shall be followed by the prompt delivery to AT&T of the identification credentials, if issued by AT&T. Supplier agrees to comply with AT&T's corporate policy requiring Supplier or its representatives, including employees and subcontractors, to exhibit their company photo identification in addition to the AT&T issued photo identification when on AT&T's or AT&T's Customer's premises.

c. Supplier shall ensure that its representatives, including employees and subcontractors, while on or off AT&T's or AT&T's Customer's premises, will (i) perform Work which conforms to the Specifications, (ii) protect AT&T's or AT&T's Customer's material, buildings and structures, (iii) perform Work which does not interfere with AT&T's business operations, and (iv) perform such Work with care and due regard for the safety, convenience and protection of AT&T and AT&T's Customers, their employees, and property.

d. Supplier shall ensure that all persons furnished by Supplier work harmoniously with all others when on AT&T's or AT&T's Customer's premises.

e. When Supplier obtains access to AT&T's computer systems, whether directly or remotely by means of data/telecommunications, Supplier will access them only by way of a AT&T authorized remote access network gateway, and AT&T UID/strong password combination in compliance with AT&T's Supplier Information Security Requirements, attached hereto as Appendix O.

f. Supplier will ensure that its employees and agents will, while on the premises of AT&T or at any other location while performing subcontracted Services under this agreement for AT&T, perform such Services in conformance with all AT&T rules and policies (including its "Code of Business Conduct", a copy of which is available upon request and the rules and policies of the customer with whom AT&T is the prime contractor. AT&T will have the right to have the Supplier personnel removed and replace Supplier Personnel who in AT&T's opinion are not conforming to AT&T's or its customer's rules or policies. In addition, Supplier agrees that, where required by government regulations, it will submit satisfactory clearance from the U. S. Department of Defense and/or other federal or state authorities concerned.

2. AT&T Supplier Information Security Requirements (SISR) – v5.1, September, 2012

The following AT&T Supplier Information Security Requirements ("Security Requirements") apply to Supplier, its affiliates, its subcontractors, and each of their employees and/or temporary workers, contractors, vendors and/or agents who perform any Services for, on behalf of, and/or through AT&T and/or other obligations (for the purpose of this Appendix, each or all "Supplier") **that include <u>any</u> of the following:**

1. The collection, storage, handling, or disposal of AT&T's Information;
2. Providing or supporting AT&T branded services using non-AT&T Information Resources (as defined below);
3. Connectivity to AT&T's Nonpublic Information Resources (as defined below);
4. Incidental and/or AT&T-paid-for development of any software to the extent produced or developed by or on behalf of Supplier, or forming part of any software, pursuant to the Agreement to which these Security Requirements are attached (including under any statement of work, exhibit, order or other document under, subordinate to, or referencing this Agreement) for the development of which AT&T has been charged monies; or
5. Website hosting and development for AT&T and/or AT&T's customers.

Supplier represents and warrants that during the term of the Agreement and thereafter (as applicable with respect to Supplier's obligations under the Survival of Obligations clause) Supplier is, and shall continue to be, in compliance with its obligations as set forth herein. In addition to all other remedies specified in the Agreement, Supplier agrees that AT&T shall be entitled to seek an injunction, specific performance or other equitable relief and be reimbursed the costs (including reasonable attorney's fees) by Supplier to enforce the obligations in these Security Requirements, including those that survive termination or expiration of the Agreement. The provisions of this Appendix shall not be deemed to, and shall not, limit any more stringent security

or other obligations of the Agreement. For the avoidance of doubt, these requirements apply to Supplier's performance of Services from all locations, including primary, non-primary, remote, virtual, and/or telecommuting or telework locations, if any, used in connection with the Agreement. Section and paragraph headings contained in parentheses that follow the requirements below are for reference purposes only and are not to affect the meaning or interpretation of these Security Requirements.

AT&T reserves the right to update or modify its Security Requirements from time to time. Upon notification by AT&T of its need to modify the Security Requirements, Supplier agrees to promptly negotiate in good faith and expedite execution of an amendment to the Agreement to incorporate any such modification. Supplier acknowledges that AT&T may require modifications to Security Requirements:

1. Upon extension or renewal of the Agreement;
2. Upon any change in work scope or other substantive modification of the Agreement; or
3. At such time that AT&T deems necessary.

Definitions:

Unless otherwise set forth or expanded herein, defined terms shall have the same meaning as set forth in the main body of the Agreement.

"Customer Facing System(s)" means an Information Resource(s) accessible from public networks, intended for use by AT&T and/or its customers, which resides in a Demilitarized Zone (DMZ), as defined below, and where that DMZ:

a. Is protected by firewalls located between the Internet and the DMZ, between that DMZ and all other DMZs, and between the DMZ and the AT&T intranet,
b. Prohibits incoming TELNET connections from public networks, and
c. Prohibits incoming File Transfer Protocol (FTP) connections from public networks except to specific systems known as "FTP drop boxes".

Note: A Customer Facing System which also is used by AT&T employees, contractors, vendors or suppliers to perform work on behalf of AT&T is not considered a Customer Facing System when performing such work.

"Demilitarized Zone" or "DMZ" is a network or sub-network that sits between a trusted internal network, such as a corporate private Local Area Network (LAN), and an untrusted external network, such as the public Internet. A DMZ helps prevent outside users from gaining direct access to internal Information Resources. Inbound packets from the untrusted external network must terminate within the DMZ and must not be allowed to flow directly through to the trusted internal network. All inbound packets which flow to the trusted internal network must only originate within the DMZ.

The DMZ must be separated from the untrusted external network by use of a Security Gateway and must be separated from the trusted internal network by use of either:

a. another Security Gateway, or
b. the same Security Gateway used to separate the DMZ from the untrusted external network, in which case the Security Gateway must ensure that packets received from the untrusted external network are either immediately deleted or if not deleted are routed only to the DMZ with no other processing of such inbound packets performed other than possibly writing the packets to a log.

The following must only be located within the trusted internal network:

a. Any of AT&T's Sensitive Personal Information (SPI) stored without the use of Strong Encryption,
b. The official record copy of information to be accessed from requests originating from the untrusted external network,
c. The official record copy of information to be modified as the result of requests originating from the untrusted external network,
d. Database servers,
e. All exported logs, and
f. Development environments and source code.

The following must not be located within the DMZ:

a. Authentication credentials not protected by the use of Strong Encryption.

"Incident Management Process" is a Supplier-developed documented procedure to be followed in the event of an actual or suspected attack upon, intrusion upon, unauthorized access to, loss of, or other breach involving AT&T's Information Resources.

"Information Resource(s)" means systems, applications, networks, network elements, and other computing and information storage devices, including smart phones, tablets, and USB memory sticks, and AT&T's Information stored, transmitted, or processed with these resources in conjunction with supporting AT&T and/or used by Supplier in fulfillment of its obligations under the Agreement.

"Mobile and Portable Devices" means mobile and/or portable computers, devices, media and systems capable of being easily carried, moved, transported or conveyed that are used in connection with the Agreement. Examples of such devices include laptop computers, tablets, USB hard drives, USB memory sticks, Personal Digital Assistants (PDAs), and wireless phones, such as smartphones.

"Nonpublic Information Resources" means those Information Resources used under the Agreement to which access is restricted and cannot be gained without proper authorization and identification.

"Sensitive Personal Information" or "SPI" means any information that: (a) requires a high degree of protection by law and where loss or unauthorized disclosure would require notification by AT&T to government agencies, individuals or law enforcement, and (b) any information that, if made public, could expose individuals to a risk of physical harm, fraud, or identity theft. Examples of SPI include, but are not limited to, social security numbers, national government issued identification numbers, such as passport and visa numbers, state- or province-issued identification numbers, drivers license numbers, dates of birth, bank account numbers, credit card numbers, customer authentication credentials, and Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA). Note: Authentication credentials, encryption keys, and encryption passwords used to protect Sensitive Personal Information are themselves classified as Sensitive Personal Information.

"Security Gateway" means a set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers. Examples of Security Gateways include firewalls, firewall management servers, hop boxes, session border controllers, proxy servers, and intrusion prevention devices.

"Strong Authentication" means the use of authentication mechanisms and authentication methodologies stronger than the passwords required by Security Requirement 34 herein. Examples of Strong Authentication mechanisms and methodologies include digital certificates, two-factor authentication, and one-time passwords.

"Strong Encryption" means the use of encryption technologies with minimum key lengths of 128-bits for symmetric encryption and 1024-bits for asymmetric encryption whose strength provides reasonable assurance that it will protect the encrypted information from unauthorized access and is adequate to protect the confidentiality and privacy of the encrypted information, and which incorporates a documented policy for the management of the encryption keys and associated processes adequate to protect the confidentiality and privacy of the keys and passwords used as inputs to the encryption algorithm.

In accordance with the foregoing, Supplier shall:

System Security

1. Actively monitor industry resources (e.g., www.cert.org and pertinent software vendor mailing lists and websites) for timely notification of all applicable security alerts pertaining to Supplier's Information Resources. (Security Alerts)
2. At least quarterly, and in addition immediately following all significant changes and upgrades, scan externally-facing Information Resources, including, but not limited to, networks, servers, and applications, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities. (Externally-facing System Scanning)
3. At least quarterly, and in addition immediately following all significant changes and upgrades, scan internal Information Resources, including, but not limited to, networks, servers, applications and databases, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities, ensure that such Information Resources are properly hardened as documented in Security Requirement 9 below, and identify any unauthorized wireless networks. (Internal System Scanning)
4. RESERVED
5. In environments where such technology is commercially available and to the extent practicable, deploy one or more Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), or Intrusion Detection and Prevention Systems (IDP) in an active mode of operation that monitors all traffic entering and leaving Information Resources in conjunction with the Agreement. (Intrusion Detection/Prevention Systems)
6. Have and use a documented process to remediate security vulnerabilities in the Information Resources, including, but not limited to, those discovered through industry publications, vulnerability scanning, virus scanning, and the review of security logs, and apply appropriate security patches promptly with respect to the probability that such vulnerability can be or is in the process of being exploited. (Remediating/Patching Service Vulnerabilities)
7. Assign security administration responsibilities for configuring host operating systems to specific individuals. (Security Administration Responsibilities)
8. Ensure that its information security staff has reasonable and necessary experience in information and network security. (Necessary Staff Experience)
9. Ensure that all of Supplier's Information Resources are and remain 'hardened' including, but not limited to, removing or disabling unused network and other services (e.g., finger, rlogin, ftp, and simple Transmission Control Protocol/Internet Protocol (TCP/IP) services) and installing a system firewall, Transmission Control Protocol (TCP) wrappers or similar technology. (Hardened Systems)
10. Change all default account names and/or default passwords. (Changing Default Account Names and Passwords)
11. Limit system administrator (also known as root, privileged, or super user) access to operating systems intended for use by multiple users only to individuals requiring such high-level access in the performance of their jobs. (Limit Super User Privileges)
12. Require application, database, network and system administrators to restrict access by users to only the commands, data and Information Resources necessary for them to perform authorized functions. (Administrators to Restrict User Access)

Physical Security

13. Ensure that all of Supplier's Information Resources intended for use by multiple users are located in secure physical facilities with access limited and restricted to authorized individuals only. (Information Resources in Secure Facilities)
14. Monitor and record, for audit purposes, access to the physical facilities containing Information Resources intended for use by multiple users used in connection with Supplier's performance of its obligations under the Agreement. (Monitoring and Recording Access)

Network Security

15. When providing Internet-based services to AT&T, protect AT&T's Information by the implementation of a network DMZ. Web servers providing service to AT&T shall reside in the DMZ. Information Resources storing AT&T's Information (such as application and database servers) shall reside in a trusted internal network. (Internet Services Must Use DMZ)
16. Upon AT&T's request, provide to AT&T a logical network diagram documenting the Information Resources (including, but not limited to, Security Gateways, servers, etc.) that will support AT&T. (Provision of Logical Network Diagram)
17. Have a documented process and controls in place to detect and handle unauthorized attempts to access AT&T's Information. (Detection and Handling of Unauthorized Access)
18. a. Use Strong Encryption for the transfer of AT&T's Information outside of AT&T- or Supplier-controlled facilities or when transmitting AT&T's Information over any untrusted network.

    b. By no later than July 1, 2014, always use Strong Encryption to protect AT&T's customer proprietary network information ("CPNI"), as that term is defined in the Telecommunications Act of 1996, 47 U.S.C. §222 (h)(1), and AT&T's SPI when transmitted. Exception: Where elsewhere authorized in writing by AT&T, AT&T's CPNI transmitted for distribution to AT&T's customers may be exempted from this requirement.

    (Note: This also applies to AT&T's Information contained in email, or the attachments embedded within the email, as the case may be. For greater clarity, if, for example, the text in an email does not contain AT&T's Information, but the embedded attachments within that email do contain AT&T's Information, then the embedded attachments, but not the email, need to be encrypted.) (Encryption of Information in Transit)
19. Require Strong Authentication for any remote access use of Nonpublic Information Resources. (Remote Access Authentication)

Information Security

20. Isolate AT&T's applications and AT&T's Information from any other customer's or Supplier's own applications and information either by using physically separate servers or alternatively by using logical access controls where physical separation of servers is not implemented. (Separate AT&T's Information from non-AT&T information)
21. Have documented procedures for the secure backup and recovery of AT&T's Information which shall include, at a minimum, procedures for the transport, storage, and disposal of the backup copies of AT&T's Information and, upon AT&T's request, provide such documented procedures to AT&T. (Secure Backup, Transport, Storage and Disposal of AT&T's Information)
22. Maintain and, upon AT&T's request, furnish to AT&T a documented business continuity plan that ensures that Supplier can meet its contractual obligations under the Agreement, including the requirements of any applicable Statement of Work or Service Level Agreement. Such plan shall include the requirement that the included procedures be regularly tested at least annually. Supplier shall promptly review its business continuity plan to address additional threat scenarios. (Business Continuity Plan)
23. Use Strong Encryption to protect AT&T's CPNI and AT&T's SPI when stored. (Encryption at Rest/Storage)
24. Limit access to AT&T's Information, including, but not limited to, paper hard copies, only to authorized persons or systems. (Limit Access to AT&T's Information Regardless of Form)
25. Be compliant with any applicable government- and industry-mandated information security standards. (Examples of such standards include, but are not limited to, the Payment Card Industry-Data Security Standards (PCI-DSS), National Automated Clearing House Associates (NACHA) Rules, and Electronic Data Interchange (EDI) standards, and the information security requirements documented within laws, such as HIPAA.) (Compliance with Industry and Government Requirements)
26. At no additional charge to AT&T:
    a. Upon AT&T's request, provide copies of any of AT&T's Information to AT&T within fifteen (15) days of such request.
    b. Return, or, at AT&T's option, destroy all of AT&T's Information, including electronic and hard copies, within thirty (30) days after the sooner of:
        i. expiration or Termination of the Agreement;
        ii. AT&T's request for the return of AT&T's Information; or
        iii. the date when Supplier no longer needs AT&T's Information to perform Services under the Agreement.
    c. In the event that AT&T approves destruction as an alternative to returning AT&T's Information, then certify in writing the destruction (e.g., degaussing, overwriting, performing a secure erase, performing a chip erase, shredding, cutting, punching holes, breaking, etc.) as rendering AT&T's Information non-retrievable.
    d. In the event that Supplier needs to retain copies of AT&T's Information more than thirty (30) days past either the expiration or Termination of the Agreement, or AT&T's request for the return or destruction of AT&T's Information, Supplier shall be allowed to retain such copies when elsewhere agreed to in writing with AT&T. Exception: Copies of AT&T's Information retained as part of a backup-and-recovery, business continuity or disaster recovery process may be retained for more than thirty (30) days past the expiration or Termination of the Agreement without obtaining agreement in writing from AT&T allowing such retention provided that all such copies are destroyed within no more than three (3) years of the date of creation. (Return of AT&T's Information)
27. Unless otherwise instructed by AT&T in writing, when collecting, generating or creating Information for, through or on behalf of AT&T or under the AT&T brand, ensure that such Information shall be AT&T's Information and, whenever practicable, label such Information of AT&T as "AT&T Proprietary Information" or at a minimum, label AT&T's Information as "Confidential" or "Proprietary". Supplier acknowledges that AT&T's Information shall remain AT&T-owned Information irrespective of labeling or the absence thereof. (Confidential or Proprietary Markings)

Identification and Authentication

28. Assign unique UserIDs to individual users. (Unique UserIDs)
29. Have and use a documented UserID lifecycle management process including, but not limited to, procedures for approved account creation, timely account removal, and account modification (e.g., changes to privileges, span of access, functions/roles) for all Information Resources and across all environments (e.g., production, test, development, etc.). Such process shall include review of access privileges and account validity to be performed at least annually. (UserID Life Cycle Management)
30. Enforce the rule of least privilege (i.e., limiting access to only the commands and Information Resources necessary to perform authorized functions according to one's job function). (Rule of Least Privilege)
31. Limit failed login attempts to no more than six (6) successive attempts and lock the user account upon reaching that limit. Access to the user account can be reactivated subsequently through a manual process requiring verification of the user's identity or, where such capability exists, can be automatically reactivated after at least three (3) minutes from the last failed login attempt. Exception: Where elsewhere authorized in writing by AT&T, AT&T customer usage of Customer Facing Systems may be exempted from this requirement. (Limit Failed Logins)
32. Terminate interactive sessions, or activate a secure, locking screensaver requiring authentication, after a period of inactivity not to exceed fifteen (15) minutes. Exception: Where elsewhere authorized in writing by AT&T, AT&T customer usage of Customer Facing Systems may be exempted from this requirement. (Terminate Inactive Interactive Sessions)
33. Require password expiration at regular intervals not to exceed ninety (90) days. Exception: Where elsewhere authorized in writing by AT&T, AT&T customer usage of Customer Facing Systems may be exempted from this requirement. (Expire Passwords)
34. a. Use an authentication method based on the sensitivity of AT&T's Information. Whenever authentication credentials are stored, Supplier shall protect them using Strong Encryption.
    b. When passwords are used, they shall be complex and shall at least meet the following password construction requirements:
        - Be a minimum of six (6) characters in length.

- Contain characters from at least two (2) of these groupings: alphabetic, numeric, and special characters.
- Not be the same as the UserID with which they are associated.
- Not contain repeating or sequential characters or numbers.

Exception: Where elsewhere authorized in writing by AT&T, AT&T customer usage of Customer Facing Systems may be exempted from the password construction requirements.

c. Applications housing more sensitive copies of AT&T's Information, as identified in writing by AT&T, may require an authentication mechanism stronger than passwords. In such case the authentication mechanism shall be mutually agreed to in advance in writing. Examples of stronger authentication methods include Strong Authentication, passphrases, and biometrics. (Passwords and Construction Rules)

35. Use a secure method for the conveyance of authentication credentials (e.g., passwords) and authentication mechanisms (e.g., tokens or smart cards). (Use Secure Method to Convey UserIDs and Passwords)

Warning Banner

36. For AT&T branded products or services or for software developed for AT&T, display a warning banner on login screens or pages as specified in writing by AT&T. (Display Warning Banners)

Software and Data Integrity

37. In environments where antivirus software is commercially available and to the extent practicable, have current antivirus software installed and running to scan for and promptly remove or quarantine viruses and other malware. (Note: For the avoidance of doubt, this requirement also applies to Mobile and Portable Devices where antivirus software is commercially available.) (Scan and Remove Viruses)
38. Separate non-production Information Resources from production Information Resources. (Separate Production and Non-Production Information Resources)
39. Have a documented change control process including back-out procedures for all production environments. (Software Change Control Process)
40. For applications which utilize a database that allows modifications to AT&T's Information, have database transaction logging features enabled and retain database transaction logs for a minimum of six (6) months. (Utilize Database Transaction Logging)
41. a. For all software developed under the Agreement, review such software to find and remediate security vulnerabilities during initial implementation and upon any modifications and updates.

    b. Where technically feasible, for all software used, furnished and/or supported under the Agreement, review such software to find and remediate security vulnerabilities during initial implementation and upon any modifications and updates. (Review Code for Vulnerabilities)
42. Perform quality assurance testing for the security components (e.g., testing of identification, authentication and authorization functions), as well as any other activity designed to validate the security architecture, during initial implementation and upon any modifications and updates. (Quality Assurance Test Security Components)

Privacy Issues

43. Restrict access to any of AT&T's CPNI and AT&T's SPI to authorized individuals. (Restrict Access to AT&T CPNI and SPI)
44. Not store AT&T's CPNI and AT&T's SPI on removable media (e.g., USB flash drives, thumb drives, memory sticks, tapes, CDs, or external hard drives) except: (a) for backup, business continuity, disaster recovery, and data interchange purposes as allowed and required under contract, and (b) using Strong Encryption. Exception: Where elsewhere authorized in writing by AT&T, AT&T's CPNI stored for distribution to AT&T's customers may be exempted from this requirement. (Control AT&T CPNI and SPI on Removable Media)

Monitoring and Auditing Controls

45. Restrict access to security logs to authorized individuals, and protect security logs from unauthorized modification. (Restrict Access to Security Logs)
46. Review, on no less than a weekly basis, all security and security-related audit logs for anomalies and document and resolve all logged security problems in a timely manner. (Review Security Logs and Resolve Security Problems)
47. Retain complete and accurate records relating to its performance of its obligations arising out of these Security Requirements and Supplier's compliance herewith in a format that will permit assessment or audit for a period of no less than three (3) years, or longer as may be required pursuant to a court order or civil or regulatory proceeding. Notwithstanding the foregoing, Supplier shall only be required to maintain security logs for a minimum of six (6) months. (Retain Records)
48. Permit AT&T to conduct an assessment or audit to verify Supplier's compliance with its contractual obligations in connection with these AT&T Supplier Information Security Requirements. Upon AT&T's request for audit, Supplier shall schedule a security audit to commence within thirty (30) days from such request. In the event that AT&T, in its sole discretion, deems that a security breach has occurred, which has not been promptly reported to AT&T in compliance with the Supplier's Incident Management Process, Supplier shall schedule the audit to commence within one (1) day of AT&T's notice requiring an audit. This provision shall not be deemed to, and shall not, limit any more stringent audit obligations permitting the examination of Supplier's records contained in the Agreement. (Audit Rights)
49. Within thirty (30) days of receipt of the assessment or audit report, provide AT&T a written report outlining the corrective actions that Supplier has implemented or proposes to implement with the schedule and current status of each corrective action. Supplier shall update this report to AT&T every thirty (30) days reporting the status of all corrective actions through the date of implementation. Supplier shall implement all corrective actions within ninety (90) days of Supplier's receipt of the assessment or audit report. (Remediate Audit Findings)

Reporting Violations

50. Have and use an Incident Management Process and promptly notify AT&T whenever there is an attack upon, intrusion upon, unauthorized access to, loss of, or other breach of AT&T's Information Resources at:

    a. Asset Protection by telephone at 800-807-4205 from within the US and at 1-908-658-0380 from elsewhere, and

    b. Supplier's contact within AT&T for Service-related issues.

(Maintain and Use Incident Response Procedures)

51. After notifying AT&T whenever there is an attack upon, intrusion upon, unauthorized access to, loss of, or other breach of AT&T's Information Resources, provide AT&T with regular status updates, including, but not limited to, actions taken to resolve such incident, at mutually agreed intervals or times for the duration of the incident and, within five (5) days of the closure of the incident, provide AT&T with a written report describing the incident, actions taken by the Supplier during its response and Supplier's plans for future actions to prevent a similar incident from occurring. (Provide AT&T Incident Response Status and Final Resolution)

Software Development

52. RESERVED

Security Policies and Procedures

53. Ensure that all personnel, subcontractors or representatives performing work under this Agreement are in compliance with these Security Requirements. (All Work to Be In Compliance with SISR)

54. RESERVED

55. Return all AT&T-owned or -provided access devices (including, but not limited to, SecurID® tokens and/or software) as soon as practicable, but in no event more than fifteen (15) days after the sooner of: (a) expiration or Termination of the Agreement; (b) AT&T's request for the return of such property; or (c) the date when Supplier no longer needs such devices. (Return all AT&T Owned or Provided Access Devices)

Mobile and Portable Devices

56 Use Strong Encryption to protect all of AT&T's Information stored on Mobile and Portable Devices.

57 Use Strong Encryption to protect all of AT&T's Information transmitted using or remotely accessed by network-aware Mobile and Portable Devices.

58 a. When using network aware Mobile and Portable Devices that are not laptop computers to access and/or store AT&T's Information, such devices must be capable of deleting all stored copies of AT&T's Information upon receipt over the network of a properly authenticated command. (Note: Such capability is often referred to as a "remote wipe" capability.)

b. Have documented policies, procedures and standards in place to ensure that the authorized individual who should be in physical control of a network-aware Mobile and Portable Device that is not a laptop computer and that is storing AT&T's Information promptly initiates deletion of all AT&T's Information when the device becomes lost or stolen.

c. Have documented policies, procedures and standards in place to ensure that Mobile and Portable Devices that are not laptop computers and are not network aware, will automatically delete all stored copies of AT&T's Information after no more than three times the number of consecutive failed login attempts documented within Security Requirement 31.

59. Have documented policies, procedures and standards in place which ensure that any Mobile and Portable Devices used to access and/or store AT&T's Information:

a. Are in the physical possession of authorized individuals;

b. Are physically secured when not in the physical possession of authorized individuals; or

c. Have their data storage promptly and securely deleted when not in the physical possession of authorized individuals nor physically secured.

60. Prior to allowing access to AT&T's Information stored on or through the use of Mobile and Portable Devices, Supplier shall have and use a process to ensure that:

a. The user is authorized for such access; and

b. The identity of the user has been authenticated.

61. Implement a policy that prohibits the use of any Mobile and Portable Devices that are not administered and/or managed by Supplier or AT&T to access and/or store AT&T's Information.

62. Review, at least annually, the use of, and controls for, all Supplier-administered or -managed Mobile and Portable Devices to ensure that the Mobile and Portable Devices can meet the applicable Security Requirements.

Security Gateways

63. Require Strong Authentication for administrative and/or management access to Security Gateways, including, but not limited to, any access for the purpose of reviewing log files.

64. Have and use documented controls, policies, processes and procedures to ensure that unauthorized users do not have administrative and/or management access to Security Gateways, and that user authorization levels to administer and manage Security Gateways are appropriate.

65. At least once every six (6) months, ensure that Security Gateway configurations are hardened by selecting a sample of Security Gateways and verifying that each default rule set and set of configuration parameters ensures the following:

a. Internet Protocol (IP) source routing is disabled,

b. The loopback address is prohibited from entering the internal network,

c. Anti-spoofing filters are implemented,

d. Broadcast packets are disallowed from entering the network,

e. Internet Control Message Protocol (ICMP) redirects are disabled,

f. All rule sets end with a "DENY ALL" statement, and

g. Each rule is traceable to a specific business request.

66. Ensure that monitoring tools are used to validate that all aspects of Security Gateways (e.g., hardware, firmware, and software) are continuously operational.

67. Ensure that all Security Gateways are configured and implemented such that all non-operational Security Gateways shall deny all access.

Wireless Networking

68. When using radio frequency (RF) based wireless networking technologies to perform or support Services for AT&T, ensure that all of AT&T's Information transmitted is protected by the use of appropriate encryption technologies sufficient to protect the confidentiality of AT&T's Information; provided, however, that in any event such encryption shall use no less than key lengths of 256-bits for symmetric encryption and 256-bits for asymmetric encryption. Exception: The use of RF-based wireless headsets, keyboards, microphones, and pointing devices, such as mice, touch pads, and digital drawing tablets, is excluded from this requirement.

Connectivity Requirements

69. In the event that a data connection agreement, such as a "Master Data Connection Agreement," "Data Connection Agreement," and/or "Connection Supplement" ("DCA") exists between the Parties, and incorporates the Agreement by reference, or is otherwise integrated with, or used to govern the Parties' connectivity obligations under, this Agreement, agree that any information security requirements incorporated within such DCA are hereby superseded by the terms of these Security Requirements, effective as of the date these Security Requirements become effective under the Agreement, and the terms of such DCA are amended to require that the Security Requirements and not the information security requirements incorporated within the DCA are controlling in the Agreement (as well as any agreements subordinate to the Agreement). Notwithstanding the foregoing, the DCA remains in full force and effect for all other agreements between the Parties to which it applies.

70. In the event that Supplier has, or will be provided, connectivity to AT&T's or AT&T's customers' Nonpublic Information Resources in conjunction with this Agreement, then in addition to the foregoing:

    a. Use only the mutually agreed upon facilities and connection methodologies to interconnect AT&T's and AT&T's customers' Nonpublic Information Resources with Supplier's Information Resources.

    b. NOT establish interconnection to AT&T's and AT&T's customers' Nonpublic Information Resources without the prior consent of AT&T.

    c. Provide AT&T access to any applicable Supplier facilities during normal business hours for the maintenance and support of any equipment (e.g., router) provided by AT&T under the Agreement for connectivity to AT&T's and AT&T's customers' Nonpublic Information Resources.

    d. Use any equipment provided by AT&T under this Agreement for connectivity to AT&T's and AT&T's customers' Nonpublic Information Resources only for the furnishing of those Services or functions explicitly authorized in the Agreement.

    e. If the agreed upon connectivity methodology requires that Supplier implement a Security Gateway, maintain logs of all sessions using such Security Gateway. These session logs must include sufficiently detailed information to identify the end user or application, origination IP address, destination IP address, ports/service protocols used and duration of access. These session logs must be retained for a minimum of six (6) months.

71. In the event that Supplier has, or will be provided, connectivity to AT&T's or AT&T's customers' Nonpublic Information Resources in conjunction with this Agreement, in addition to other rights set forth herein, permit AT&T to:

    a. Gather information relating to access, including Supplier's access, to AT&T's and AT&T's customers' Nonpublic Information Resources. This information may be collected, retained and analyzed by AT&T to identify potential security risks without further notice. This information may include trace files, statistics, network addresses, and the actual data or screens accessed or transferred.

    b. Immediately suspend or terminate any interconnection to AT&T's and AT&T's customers' Nonpublic Information Resources if AT&T, in its sole discretion, believes there has been a breach of security or unauthorized access to or misuse of AT&T data facilities or AT&T Information Resources.

3. Background Checks –

a. Supplier, with respect to the following requirements in this Section (collectively, "Background Checks") and subject to any federal, state, or local laws, rules or regulations which may limit any Supplier action otherwise required by this section, shall:

    1. make all reasonable and legally permitted efforts, including checking the background, and verifying the personal information to determine all information necessary to verify whether any Supplier employee, contractor or subcontractor and any employee or agent of any Supplier contractor or subcontractor ("Supplier Person") whom Supplier proposes to have perform any Service that permits Physical Entry or virtual or other access to AT&T's or its customers' systems, networks, or Information ("Access") at any time during the term:

        i. has been convicted of any felony, or has been convicted of any misdemeanor involving violence, sexual misconduct, theft or computer crimes, fraud or financial crimes, drug distribution, or crimes involving unlawful possession or use of a dangerous weapon ("Conviction") or

        ii. is identified on any government registry as a sex offender ("Sex Offender Status"); and

    2. in addition to the requirements of 1., perform a Drug Screen on any Supplier Person whom Supplier proposes to have Physical Entry onto AT&T's or its customers' premises and not permit any such Supplier Person presenting a positive Drug Screen to have Physical Entry onto AT&T's or its customers' premises.

    Supplier shall comply with the obligations of Subsection a(i) above through the use of a third party service which shall perform a review of applicable records for those counties, states, and federal court districts in which a proposed Supplier Person has identified as having resided, worked, or attended school in the previous ten (10) years, unless a shorter period is required by any federal, state, or local law.

b. Supplier acknowledges and agrees that it is Supplier's sole and exclusive responsibility to determine whether a Supplier Person's Conviction or Sex Offender Status has a reasonable relationship to the individual's fitness or trustworthiness to perform the Service, subject to any federal, state, or local restrictions on the consideration of criminal convictions in making employment decisions and whether such Supplier Person should be permitted Access during the term under the terms of this Agreement and in compliance with all federal, state, and local laws, unless an exception is granted by AT&T under paragraph e. of this Section.

c. Supplier represents and warrants to AT&T that, to the best of its knowledge, no Supplier Person has (i) falsified any of his or her Identification Credentials, or (ii) failed to disclose any material information in the hiring process relevant to the performance of any Service. Supplier shall not permit any Supplier Person who has falsified such Identification Credentials or failed to disclose such information to perform any Service that permits Access.

d. The following definitions apply:

1. "Physical Entry" means that an individual (i) is permitted to bodily enter, on an unsupervised (or badged) basis, into secured areas not available to the general public, or (ii) is permitted on a regular basis to have supervised or escorted bodily access into secured areas not available to the general public for more than thirty (30) days in the aggregate annually.
2. "Identification Credentials" includes, with respect to each Supplier Person, his or her Social Security number, driver's license, educational credentials, employment history, home address, and citizenship indicia.
3. "Drug Screen" means the testing of any individual for the use of illicit drugs (including opiates, cocaine, cannabinoids, amphetamines, and phencyclidine (PCP)).

e. The failure of Supplier to comply with the requirements of this Section shall be considered a material breach of this Agreement. Notwithstanding any of the foregoing, exceptions for individual Supplier Persons may be granted by AT&T on a case-by-case basis.

4. Entry on AT&T Property –

a. If the performance of the Services provided hereunder requires Supplier's entry upon property owned or controlled by AT&T, Supplier is hereby notified that AT&T presumes for safety planning purposes that all tile and sheet/rolled vinyl flooring contains asbestos unless verified otherwise through sampling of the material and that AT&T-owned buildings constructed prior to 1981 may contain other asbestos containing materials ("ACM") and/or presumed asbestos containing materials ("PACM"). All AT&T buildings, regardless of age, may also contain both natural and manmade conditions and/or activities involving risk of harm. AT&T has not inspected such property for the purposes of this Agreement and has not taken any efforts to discover or make safe dangerous conditions or activities for the purpose of Supplier's performance of Services.

b. If the performance of the Services provided hereunder requires disturbance of ACM/PACM other than flooring material (surfacing/fireproofing coatings, thermal system insulation (TSI) or other suspect materials), then Supplier must contact the project manager and request records to determine the presence, location and quantity of ACM/PACM in or adjacent to which Supplier's employees may reasonably be expected to work. At AT&T's discretion, the project manager may supply records that indicate which areas, if any, of the premises contain ACM. If AT&T does not provide records or does not know if the premises contain ACM, the material will be presumed to be asbestos containing until proven otherwise. If records regarding the presence, location, and quantity of ACM do not exist, the project manager may arrange for a survey of materials that may be disturbed to determine the presence, location, and quantity of asbestos. If AT&T is aware that ACM or PACM is indicated in materials that may be disturbed, AT&T will advise Supplier of the presence, location and quantity of all known ACM and/or PACM at the work site. Supplier will have no obligation to provide Services in areas of premises containing ACM and/or PACM if its work could potentially disturb the ACM/PACM, except work requiring the drilling or cutting/lifting of asbestos containing flooring in accordance with paragraph e below. Supplier will not be liable for any liquidated damages related to any delay associated with AT&T's failure or delay in providing Supplier with information related to the presence, location and quantity of ACM/PACM.

c. If ACM or PACM is indicated on AT&T's premises, it is AT&T's responsibility to assure that the ACM/PACM does not present a hazard while Supplier conducts work operations on the premises. If it is determined that Supplier's work, other than drilling or cutting/lifting of asbestos-containing flooring, will potentially disturb ACM/PACM, releasing asbestos fibers into the air, AT&T must have a contractor meeting the requirements of applicable laws remove the asbestos prior to Supplier's performing work in the area.

d. Upon entering AT&T's premises, Supplier shall be responsible for inspecting the Services site for visually obvious unsafe conditions and taking the necessary safety precautions for protection of Supplier, its employees, and its agents and ensuring a safe place for performance of the Services. As a material condition of this Agreement, Supplier, for itself and its employees and agents, assumes all risk of visually obvious dangers associated with the property, and responsibility for the following OSHA notice requirements:

1. informing its employees of the information provided by the AT&T Asbestos Records Contact regarding the presence, location and quantity of ACM/PACM present in the property in or adjacent to which Supplier's employees may reasonably be expected to work and the precautions to be taken to reasonably insure that airborne ACM/PACM is kept well below permissible exposure levels; and
2. informing the appropriate AT&T project manager and other employers of employees at the property of the presence, location and quantity of any newly discovered ACM/PACM identified by Supplier within twenty-four (24) hours of its discovery.

e. Should Services require the drilling or cutting/lifting of presumed asbestos containing/asbestos-containing flooring (e.g., floor tile or sheet rolled goods such as linoleum), Supplier agrees that its employees and subcontractors performing such drilling or cutting/lifting will use AT&T's Technical Practice 76300 (section G) Procedure for Drilling or Cutting/Lifting Asbestos-Containing/Presumed Asbestos Containing Flooring ("AT&T's Procedure") which has a Negative Exposure Assessment when drilling or cutting/lifting such flooring and that only employees and subcontractors who have received the annual training required to perform AT&T's Procedure will perform such drilling or cutting/lifting procedures.

1. In accordance with AT&T's Procedure, AT&T shall either supply Supplier written documentation verifying the absence of ACM in states where asbestos disturbance is not allowed and Supplier shall proceed with drilling or cutting/lifting when the cuts or drills will be in non-asbestos containing floors.
2. If no information regarding asbestos content of the flooring is available, in accordance with AT&T's Procedure, the AT&T project manager will arrange for either 1) a licensed asbestos building inspector to obtain a sample of the floor to determine asbestos content or lack thereof; or 2) a licensed asbestos abatement contractor to drill the holes or remove the asbestos-containing materials and properly dispose of the debris.
3. Supplier will not be liable for any liquidated damages related to any delay associated with AT&T's failure or delay in providing Supplier with the information, documentation or work by a licensed asbestos contractor pursuant to this sub-paragraph (e).

f. Supplier hereby releases AT&T from any and all claims or causes of action in connection with the responsibilities assumed by Supplier in Sections d (1), d (2) and (e) above, and agrees to indemnify, hold harmless and defend AT&T, its Affiliates and its and their employees, agents, officers, and directors against any Loss arising therefrom or in connection therewith, in accordance with the Section of this Agreement entitled "Indemnity."

g. If in Supplier's judgment, the Services, other than Services requiring the drilling or cutting/lifting of asbestos-containing flooring, should not proceed due to the presence of ACM/PACM and/or any other unsafe condition, the correction of which may require changes or alterations in AT&T's operations or property, Supplier shall notify the AT&T project manager immediately, and shall suspend the Services until Supplier and AT&T agree on the

corrections or alterations necessary for the safe performance of the Services. Supplier will not be liable for any liquidated damages related to any delay associated with such a suspension.

5. Insurance –

a. With respect to Supplier's performance under this Agreement, and in addition to Supplier's obligation to indemnify, Supplier shall at its sole cost and expense:

i. maintain the insurance coverages and limits required by this Section and any additional insurance and/or bonds required by law:

1. at all times during the term of this Agreement and until completion of all work associated with this Agreement, whichever is later; and
2. with respect to any coverage maintained in a "claims-made" policy, for two (2) years following the term of this Agreement or completion of all work associated with this Agreement, whichever is later. If a "claims-made" policy is maintained, the retroactive date must precede the commencement of work under this Agreement;

ii. require each subcontractor who may perform work under this Agreement or enter upon the work site to maintain coverages, requirements, and limits at least as broad as those listed in this Section from the time when the subcontractor begins work, throughout the term of the subcontractor's work and, with respect to any coverage maintained on a "claims-made" policy, for two (2) years thereafter;

iii. procure the required insurance from an insurance company eligible to do business in the state or states where work will be performed and having and maintaining a Financial Strength Rating of "A-" or better and a Financial Size Category of "VII" or better, as rated in the A.M. Best Key Rating Guide for Property and Casualty Insurance Companies, except that, in the case of **Workers' Compensation** insurance, Supplier may procure insurance from the state fund of the state where work is to be performed; and

iv. deliver to AT&T, certificates of insurance stating the types of insurance and policy limits. Supplier shall provide or will endeavor to have the issuing insurance company provide at least thirty (30) days advance written notice of termination, non-renewal, or reduction in coverage, terms, or limits to AT&T. Supplier shall deliver such certificates:

1. prior to execution of this Agreement and prior to commencement of any work;
2. prior to expiration of any insurance policy required in this Section; and
3. for any coverage maintained on a "claims-made" policy, for two (2) years following the term of this Agreement or completion of all work associated with this Agreement, whichever is later.

b. The parties agree that:

i. the failure of AT&T to demand such certificate of insurance or failure of AT&T to identify a deficiency will not be construed as a waiver of Supplier's obligation to maintain the insurance required under this Agreement;

ii. the insurance required under this Agreement does not represent that coverage and limits will necessarily be adequate to protect Supplier, nor shall it be deemed as a limitation on Supplier's liability to AT&T in this Agreement;

iii. Supplier may meet the required insurance coverages and limits with any combination of primary and Umbrella/Excess liability insurance; and

iv. Supplier is responsible for any deductible or self-insured retention.

c. The insurance coverage required by this Section includes:

i. **Workers' Compensation** insurance with benefits afforded under the laws of any state in which the work is to be performed and **Employers Liability** insurance with limits of at least:
$500,000 for Bodily Injury – each accident
$500,000 for Bodily Injury by disease – policy limits
$500,000 for Bodily Injury by disease – each employee

To the fullest extent allowable by Law, the policy must include a waiver of subrogation in favor of AT&T, its Affiliates, and their directors, officers and employees.

In states where **Workers' Compensation** insurance is a monopolistic state-run system, Supplier shall add **Stop Gap Employers Liability** with limits not less than $500,000 each accident or disease.

ii. **Commercial General Liability** insurance written on Insurance Services Office (ISO) Form CG 00 01 12 04 or a substitute form providing equivalent coverage, covering liability arising from premises, operations, personal injury, products/completed operations, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract) with limits of at least:
$2,000,000 General Aggregate limit
$1,000,000 each occurrence limit for all bodily injury or property damage incurred in any one (1) occurrence
$1,000,000 each occurrence limit for Personal Injury and Advertising Injury
$2,000,000 Products/Completed Operations Aggregate limit
$1,000,000 each occurrence limit for Products/Completed Operations
$1,000,000 Damage to Premises Rented to You (Fire Legal Liability)

The **Commercial General Liability** insurance policy must:

1. include AT&T, its Affiliates, and their directors, officers, and employees as Additional Insureds. Supplier shall provide a copy of the Additional Insured endorsement to AT&T. The Additional Insured endorsement may either be specific to AT&T or may be "blanket" or "automatic" addressing any person or entity as required by contract. A copy of the Additional Insured endorsement must be provided within sixty (60) days of execution of this Agreement and within sixty (60) days of each **Commercial General Liability** policy renewal;
2. include a waiver of subrogation in favor of AT&T, its Affiliates, and their directors, officers and employees; and
3. be primary and non-contributory with respect to any insurance or self-insurance that is maintained by AT&T.

iii. **Business Automobile Liability** insurance with limits of at least $1,000,000 each accident for bodily injury and property damage, extending to all owned, hired, and non-owned vehicles.

iv. **Umbrella/Excess Liability** insurance with limits of at least $1,000,000 each occurrence with terms and conditions at least as broad as the underlying Commercial General Liability, Business Auto Liability, and Employers Liability policies. **Umbrella/Excess Liability** limits will be primary and non-contributory with respect to any insurance or self-insurance that is maintained by AT&T.

6. Quality Assurance –

a. In addition to its obligations under the Section entitled "Warranty," Supplier represents and warrants that:

1. All processes utilized to produce Material and provide Services are controlled and adequate to Deliver consistent with Specifications and this Agreement;
2. Supplier has evaluated the process controls of its subcontractors and vendors and has determined that they are adequate to Deliver Materials and Services consistent with Specifications and this Agreement; and
3. All Material and Services are subjected to the above-mentioned process controls.

For information purposes only, excellent Quality Management System guidance can be found in TL 9000 and ISO 9001. Copies of ISO 9001 may be ordered through the American Society for Quality at 800.248.1946. Copies of TL 9000 Handbooks may be ordered through the QuEST Forum web site at www.tl9000.org. Select the Handbook' link from the TL 9000 home page, which will direct you to the TL 9000 Handbooks purchase page.

b. Throughout the term of this Agreement, Supplier shall periodically evaluate process controls to verify whether each is still adequate to Deliver Material and Services consistent with Specifications and this Agreement. AT&T reserves the right to request a review of such process controls throughout the term of this Agreement.

c. If Supplier or AT&T, at any time during the term of this Agreement, determines that the process controls are insufficient to meet the obligations herein, then at no additional charge to AT&T, Supplier shall provide to AT&T a quality plan to remedy such insufficient Quality Process. Such quality plan shall include the following information, in detail: (i) a schedule for achieving an adequate Quality Process; and (ii) the actions that will achieve and remedy such insufficiencies. Should remedy efforts described above fail to address insufficiencies within thirty (30) days or upon AT&T's notification to Supplier that remedy efforts are insufficient, whichever is earlier, or within a time period as mutually agreed, Supplier shall engage a third party consultant to perform quality control or quality assurance activities. Supplier shall provide AT&T or AT&T's agent with notice of such engagement, including the name of the third party consultant, and shall provide AT&T or AT&T's agent with cooperative assistance to such consultant.

d. If requested by AT&T, Supplier shall provide performance measurements periodically that demonstrate compliance with the Specifications and this Agreement. The Parties shall mutually agree upon appropriate performance measurements.

e. Nothing contained in this Clause, "Quality Assurance," will diminish Supplier's obligation to Deliver Material and perform Services in conformance to Supplier's obligations in this ***Agreement.***

7. Supplier Citizenship and Sustainability – Supplier shall conduct business with an abiding respect for corporate citizenship, sustainability, and human rights ("Citizenship and Sustainability"). As such, to the extent Supplier has an existing Citizenship and Sustainability program, such program shall be no less stringent than AT&T's Principles of Conduct for Suppliers available at: http://www.attsuppliers.com/misc/SupplierSustainabilityPrinciples.pdf and the AT&T Human Rights in Communication Policy available at: http://www.att.com/Common/about_us/downloads/Human_Rights_Communications_Policy.pdf (as amended from time-to-time) ("AT&T Citizenship and Sustainability Policies"). In the event that Supplier does not have a Citizenship and Sustainability program, or such program does not address all areas addressed in the AT&T Citizenship and Sustainability Policies, Supplier shall conduct its business operations in a manner consistent with the AT&T Citizenship and Sustainability Policies. Upon AT&T's request, Supplier shall provide to AT&T such information, reports, or survey responses as AT&T deems necessary to periodically monitor Supplier's business operations in the context of Citizenship and Sustainability. Supplier shall respond to such requests within timelines as set forth by AT&T.

8. Supplier's Audited Financial Statements – In the event that Supplier is not a publicly traded corporation, Supplier shall provide to AT&T (or its third party delegate), upon request and at no charge, its bona fide and unedited audited fiscal year financial statements and other financial documents as reasonably requested by AT&T to allow an assessment of Supplier's financial condition. If Supplier is a subsidiary of, is owned by, has a majority of its interest held by, or is controlled by an entity (e.g., a parent company) that is not a publicly traded corporation, then Supplier shall furnish such documents for both Supplier and its owning, controlling or parent company. If Supplier is a subsidiary of, is owned by, has a majority of its interest held by, or is controlled by an entity (e.g., a parent company) that is a publicly traded corporation, then Supplier shall furnish such documents for both Supplier and its owning, controlling or parent company to the extent that such documents are not publicly available.

9. Third Party Administrative Services – Supplier acknowledges that a third party administrator will perform certain administrative functions for AT&T in relation to this Agreement. Such administrative functions may include: (i) Collecting and verifying certificates of insurance; (ii) Providing financial analysis; and (iii) collecting and verifying Supplier profile information. Supplier shall cooperate with such third party administrator in its performance of such administrative functions and shall provide such data as from time to time the third party administrator may request. Further, notwithstanding any other provision of this Agreement, Supplier agrees that AT&T may provide any information regarding Supplier to such third party administrator. Supplier agrees to pay the third party administrator an annual fee for the performance of these administrative functions, which annual fee shall not exceed three hundred dollars ($300.00), and a one time set-up fee of thirty dollars ($30.00).