SENSITIVE INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS OF ATN INTERNATIONAL AND ATN INTERNATIONAL AFFILIATES

Suppliers providing services to and/or performing services for ATN International Services, LLC and/or its Affiliates (collectively "ATN") and have access to Sensitive Information as defined below shall comply with the information security requirements set forth in this document.

The security requirements herein shall supplement the security requirements agreed to in an Agreement between ATN and Supplier including Orders and Statements of Work thereunder (collectively or individually, the "Agreement(s)"). This document does not limit other rights of ATN or obligations of Supplier that otherwise exist under applicable laws or Agreement(s), including, but not limited to, additional security requirements that may be imposed to address protection of specific information, specific agreements, specific engagements, or changes in applicable law; and any security protection requirements in such laws and agreements that are more stringent than those set forth in this document shall replace and supersede the corresponding terms of this document .

Any exceptions to the following requirements must be approved in writing by ATN in advance of implementation. Unless expressly stated otherwise in the Agreement(s), the terms of this document shall take precedence and prevail over any conflicting or inconsistent provisions in the Agreement(s) only to the extent that they are more stringent than the conflicting or inconsistent provisions of the Agreement(s).

As used in this document , compliance is required with those requirements that are preceded by the words "shall" or "must." Those requirements that are preceded by the word "should" are important, however Supplier is free to adopt alternatives that result in information protection and security that is at least equivalent to conformance to those requirements.

1) **Definitions**:

a) Information Definitions

Confidential Information	Defined in the Agreement(s)
CPNI Privacy Information (CPNI-PI)	One or more of the following CPNI related personal information data elements that may be combined with a person's identifying information (name, telephone number, email address, driver's license number, internet address, etc.): (1) Call detail records (2) Credit information (3) Internet Usage Information (4) Video Viewership Information
Personally Identifiable Information (PII)	Information capable of being associated with a particular individual through one or more identifiers, including but not limited to: (1) Military ID number (2) Passport Number (if applicable) (3) Work Visa Number (if applicable) (4) Access Codes, Pin, Password, challenge responses for individual user access to information systems

(5) Mother's Maiden Name

(6) Federal Tax ID (Social Security Number) in many cases)

(7) Driver's license number

(8)) State identification card number

(9) An account number or credit or debit card number

(10) Alien registration number

(11) Health insurance identification number

"Personally Identifiable Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Sensitive Information	Any SPI, PII or CPNI-PI, collectively or individually.
Sensitive Personal Information (SPI)	One or more of the following personal data elements that may be combined with a person's identifying information (name, telephone number, email address, driver's license number, internet address, etc.): (1) Social Security number, (2) driver's license number or state-issued identification card number, (3) financial account number, or credit or debit card number, with our without any required security code, access code, personal identification number (PIN) or password that would permit access to that person's financial account, (4) medical information (including, but not limited to, any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional), (5) health insurance information (i.e., an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records). "Sensitive Personal Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

b) General Definitions

Industry Standard	"Industry Standard" means: (1) actually used or adopted by a substantial number of comparable companies working with comparable information of a comparable

nature; (2) prescribed for use by an a governing industry standards body or group; or (3) assessed by recognized experts in the field as acceptable and reasonable.

Media Destruction

A process that destroys media on which information is located and thereby makes recovery of such information impossible, and means "destroyed" as specified in Guidelines for Media Sanitization, National Institute of Standards and Technology, NIST Special Publication 800-88 (NIST 800-88). Incineration, shredding and pulverizing are all permissible physical destruction methods in accordance with minimum standards specified in NIST 800-88. Media that have been subject to such Destruction are "Destroyed" under these Information Security Requirements.

Storage Encryption

Data encryption using at least using a non-proprietary industry standard algorithm that has not been broken (AES and 3Des are acceptable encryption methods). To the extent that this is applicable to Supplier's information security systems, the ATN Sensitive Information stored by Supplier shall be protected using the following minimum encryption standards:

File/Data Type	Cipher	Encryption Algorithm	Strength
Flat (ASCII) files	Symmetric Block	Triple DES	168 bits
	Symmetric Block	AES	256 bits
Database Tables		Symmetric Block	Triple DES 168 bits
	Symmetric Block	AES	256 bits
Backup/Tape[1]	Symmetric Block	Triple DES	168 bits
	Symmetric Block	AES	256 bits
Other[2]	Symmetric Block	Triple DES	168 bits
	Symmetric Block	AES	256 bits

Sanitization

"Sanitized" or "sanitization" is a process that removes information from media or that renders such information irretrievable, such that data recovery is not possible, and means "sanitized" no less effectively than as specified in Guidelines for Media

[1] Full tape encryption not required if all Sensitive Data is already encrypted and if the process to move to backup preserves prior encryption

[2] Any other stored file/data type not specifically mentioned herein

	Sanitization, National Institute of Standards and Technology, NIST Special Publication 800-88 (NIST 800-88).
Secure Transportation	Transport utilizing a licensed, bonded, secure carrier that implements and adheres to a "chain of custody program", approved by ATN, for tracking the movement and disposition of storage media or other equipment from receipt to final disposition, including tracking the following specific items: (1) Ownership of the media (2) Serial number of the media (3) Verification at collection/pick-up location (owner/end user) (4) Driver name, date and time Stamp (5) Receipt at Supplier's location (date and time Stamp);
Security Breach	The unauthorized acquisition or unauthorized use of unencrypted data, or the unauthorized acquisition or unauthorized use of encrypted data along with the confidential process or key that is capable of compromising the security, confidentiality, or integrity of such encrypted data.
Strong Authentication	Authentication is a process for verifying an individual and/or the individual's electronic identity. An individual or the individual's electronic identity can be certified by positively identifying any one of the following: 1) Something they know (an authentication code), such as a password; 2) Something they have (an authentication device), such as a proximity door card or a SecurID card; or 3) Something they are (physical characteristics), such as facial features, retina pattern, or a fingerprint Strong Authentication occurs when a user is required to submit or use at least two of these identification indicators for verification.
Supplier Devices	Servers, computers, mobile devices (other than mobile workstations), and communications equipment provided by Supplier in connection with work under the Agreement.
Supplier Staff	Supplier staff includes employees, contract employees, temporary staff, authorized subcontractors, and employees, contract employees and temporary staff of the foregoing subcontractors.
Transport Encryption	Transport encryption shall be no less secure than encryption consisting of TLS 1.1 or better protected by a minimum of 128 bit encryption with a 1024 bit keys using ATN approved digital certificates. In the case Cardholder Data is present then TLS 1.2 is required minimum of 256 bit encryption is required. Public certificates must be used for all web-based servers. If other transport encryption methods are utilized, they must conform to these minimum standards.

2) Information Security Program Requirements:

Supplier is required to maintain an information security program that at minimum includes the following:

a) One or more designated qualified employees must be responsible to maintain the Supplier information security program.

b) Supplier must maintain written information security policies and standards that address all information security requirements contained in the Agreement(s); that are at minimum consistent in all material respects with the requirements of this document and with applicable Industry Standards; and that support the *confidentiality, integrity and availability* of Supplier systems, information and business operations and the confidentiality, integrity and availability of ATN Sensitive Information and Confidential Information. In addition, such policies and standards must conform to all applicable data protection laws and regulations.

c) Supplier executive management must endorse information security polices and standards;

d) Supplier Staff must receive periodic training (at least annually) to understand Supplier's security policies, and must acknowledge their adherence to Supplier's security policies. Written certification of the periodic training and of the acknowledgement of information security policies by Supplier employees and permitted contractors must be maintained by supplier for inspection by ATN upon reasonable request.

e) Non-compliance with Supplier's information security policies must result in meaningful discipline.

f) Supplier Information Security program must include periodic education and awareness messages to Supplier Staff that consist of relevant and timely information to sensitize such staff to the importance of security for Sensitive Information and Confidential Information, complying with applicable use requirements and limitations, the proper use of Supplier's security systems, and the requirements of Supplier's information security program.

g) Supplier must review its security measures on an ongoing basis, at least annually and whenever there is a material change in business practices that may implicate the security or integrity of records containing Sensitive Information. Such review will identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing Sensitive Information.

h) Supplier must regularly monitor its security measures to identify and assess reasonably foreseeable risks to the security, confidentiality and/or integrity of Sensitive Information and to ensure that its information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Sensitive Information, and to ensure that the security program continues to comply with applicable laws. Supplier will promptly notify ATN of any findings of deficiencies in its security program and of its plans mitigating such deficiencies, and Supplier will upgrade its information security safeguards as necessary to minimize the risks associated with those deficiencies.

i) Supplier must, no less often than annually, audit each computer (PC or workstation) that is connected to the ATN corporate network or to ATN servers to verify that each such computer has the antivirus and firewall capabilities and the periodic updates thereto required in this document . Supplier must immediately remedy any non-conforming computer before it is reconnected with the ATN corporate network or a ATN server. Supplier must maintain the results of such audits, including records of non-conformities found and their remediation, for no less than three years, and provide those results to ATN on request.

j) Supplier must flow down to all permitted subcontractors the obligation to comply with this document .

3) Physical Security Requirements (Suppliers conducting information processing of ATN Sensitive Information at Supplier Premises)

a) Personnel Security

i) To the extent Supplier Staff are provided access to ATN computers, systems, servers, systems and resources ("ATN Resources") in order to perform services for ATN, Supplier must ensure that such staff are notified that they are not entitled to privacy protection if they access such ATN Resources, and that access to and communications with ATN Resources may be monitored by ATN.

b) Facilities Access Control

i) Supplier must have controls in place to allow only authorized individuals into Supplier facilities where ATN Sensitive Information and/or Confidential Information is stored or is accessible.

ii) Facility access control systems must be secured from tampering, circumvention or destruction.

iii) Facility access control systems must be maintained at all times in functional order and must be updated or changed if they become compromised or ineffective (for example, if keys are stolen, the locks should be changed).

iv) Facility access controls must be Industry Standard, and should include some or all of the following elements:

(1) Issuance of employee or contractor identification badges;

(2) Use of smartcards or other electronic or physical identity verification systems (pin/key access locks, biometrics, etc.);

(3) Use of dedicated security personnel who control access to the Supplier's facilities;

(4) 24x7 main lobby security guard station;

(5) Locks on all ground floor windows;

(6) Alarmed locks on all external doors; and

(7) Use of CCTV on all entrances and entrances to data computing facilities, to include ninety (90) days of video storage.

v) Visitors accessing the facility must be managed in accordance with the following practices:

(1) Visitors to Supplier facilities must be registered in a visitor log. The log should document the visitor's name, the firm represented, and the employee authorizing physical access on the log. The log should be retained for inspection by ATN for a minimum of three months, unless otherwise restricted by law.

(2) Visitors should be issued temporary identification badges specific to the length of the expected visit in the facility. Visitor identification badges must be returned upon the visitor's departure.

(3) Temporary visitor identification should be noticeably different from Supplier's normal employee and contractor identification.

(4) Supplier must inform employees of the approved formal policies for granting access to visitors at Supplier facilities.

(5) Any visitor to a Supplier facility that accesses areas where ATN Sensitive Information and/or Confidential Information is stored, processed or transmitted must be accompanied and supervised at all times by a Supplier employee who is specifically authorized to access confidential ATN data.

(6) Prior to granting a visitor to a Supplier facility access to any computer, server or system containing ATN Sensitive Information and/or Confidential Information, access by each such visitor must be approved in writing by the designated ATN contact, and the visitor must be positively identified as the person for whom ATN has given such approval.

(7) Under no circumstances may visitors be left unattended in an area where they have physical access to equipment that handles ATN Sensitive Information and/or Confidential Information.

c) Facilities Access Monitoring:

i) The Supplier should utilize appropriate levels of monitoring equipment in public areas of their facilities to ensure the auditing of Supplier facility entry and exit activity can be performed.

ii) For all Supplier access control and monitoring installations, appropriate safeguards and retention of records should be implemented to ensure the integrity of the systems and the availability of the records if the need arises.

d) Separate Information Processing Environments

At a minimum, the following physical security and access controls must be implemented and maintained throughout the terms of the engagement:

i) ATN Sensitive Information and/or Confidential Information must not be processed on servers that are accessible in general business areas of Supplier's facility and must be isolated in dedicated information processing areas with independent physical, monitoring, environmental and health and human safety systems (referred to as a "Computer Room").

ii) Access to any information processing area where ATN Confidential and/or Sensitive information is processed must be restricted to authorized Supplier personnel only.

iii) Supplier must implement physical access policies and procedures to ensure that physical access is revoked when it is no longer needed or appropriate (for example, immediately removing access for separated employees or removing access for employees who are no longer authorized to access ATN Confidential and/or Sensitive Information). Removal of Physical Access should occur in a timely manner not to exceed 24 hours.

iv) Supplier must employ technical and organizational mechanisms to prevent unauthorized copying of Sensitive Information within Information Processing Environments. These mechanisms shall include disabling/restricting local ports so as to prevent downloading of data onto removable USB drives, MP3 players or similar devices, restrictions on uploading or file transfer from the facility to unauthorized recipients, and a prohibition on the use of cameras (excluding CCTV security unit) and other screen capture devices.

e) Computer Room Physical Security Requirements

Computer room facilities where ATN Sensitive Information and/or Confidential Information is stored, processed or transmitted must implement the following information security controls:

i) All computer room doors must be secured to prevent unauthorized access into the room.

ii) Each computer room door must have signs on both sides indicating it is to be closed and locked with a contact to notify if it is found unsecured.

iii) Supplier Staff must be instructed to immediately report unsecured doors.

iv) Supplier must implement a reliable process of designating staff access to Computer Rooms.

v) Supplier Staff should only be authorized to enter a Computer Room for a legitimate business need and a record of the individual's identity, justification and duration of access should be maintained.

vi) A separate electronic access control system utilizing strong authentication should be installed on Computer Room doors that will only allow authorized personnel access to the room, unless access to the room is controlled 24 hours a day, 7 days a week, by a guard.

(1) The access control system must be secured against tampering.

(2) The access control system must log the entry and exit of staff for each time the door is opened. Entry and exit logs should contain a reliable time stamp, room location and identification of the person who gained access or exited the room.

(3) The access control system should alert security staff in the event that a secured door has been open beyond a reasonable amount of time (for example, by being propped open and unattended).

vii) Supplier should periodically review access records to ensure that access controls are being enforced effectively. Any discrepancies or unauthorized access must be investigated immediately by Supplier information security personnel and reported to the ATN Sponsor.

viii) Supplier should periodically review CCTV video storage to ensure that access controls are being enforced effectively to prevent unauthorized entry. Any unauthorized access must be investigated immediately by Supplier information security personnel and Supplier must provide ATN notice of such breach of security in accordance with this document .

f) Asset Disposal and Reclamation

i) Upon conclusion or termination of Supplier's work for ATN, at ATN's option Supplier must either:

(1) Sanitize or Destroy all copies of all ATN information maintained under the Agreement or an applicable Order or Statement of Work (collectively, "work agreement"), including all backup and archival copies within Supplier's control, or

(2) return to ATN all copies of all ATN information maintained under work agreement, as well as all backup and archival copies.

ii) When no longer required for performance under the Agreement and prior to disposition, recycle, or resale, electronic and non-electronic (hardcopy) media containing ATN Sensitive Information and/or Confidential Information shall be rendered unreadable and unrecoverable by Sanitization or Destruction.

iii) All non-electronic media must be Destroyed utilizing a cross cut shredder.

iv) All electronic media containing ATN Sensitive Information and/or Confidential Information shall be destroyed or rendered unusable when such information is no longer required for performance under this agreement and prior to disposition, recycle or resale, using methods that prevent access to information stored in that type of media. At minimum, media containing ATN Sensitive Information and/or Confidential Information shall be "sanitized" in accordance with NIST Special Publication 800-88. Although ATN prefers that data be disposed of in a manner consistent with "Destruction", at a minimum, electronic media that at any point contains ATN Confidential and/or Sensitive Information must be disposed in a manner consistent with "Sanitization" requirements in the NIST standard. Additionally the following minimum standards must be met:

(1) All tape must be degaussed with a degausser that meets the performance standards provided by the US National Security Agency (NSA) which can be found at http://www.nsa.gov/ia/_files/Government/MDG/NSA_CSS-EPL-9-12.PDF.

(2) When Sanitizing magnetic or flash media, the preferred method of Sanitization is to perform a Secure Erase (to be used only for ATA Drives and SCSI drives, where technically feasible - available from the University of San Diego CMRR, at http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml). Alternatively, if Secure Erase is technically inappropriate or is not used, a minimum of a three pass block erasure shall be utilized that removes the data from magnetic disk media by sequentially overwriting all addressable locations in the following manner, and then verifying the same by a disk read: (i) overwriting with a random pattern; (ii) overwriting with binary zeros; and (iii) overwriting with binary ones. The National Institute of Standards and Technology and Federal Agencies Security Practices initiative (FASP) have specified the Active KillDisk software, http://www.killdisk.com/eraser.htm, as a compliant sanitization tool for IDE, SCSI and ATA drives.

(3) Optical Disk media must be destroyed.

(4) Removal of non-functional electronic storage media: Non-functional electronic storage media (e.g., a failed drive) may not be capable of Sanitization, and therefore must be either returned to ATN or Destroyed. When removing non-functional electronic storage media from a ATN or Supplier facility, Supplier may Destroy the media onsite prior to removal as specified herein. If the electronic storage media are not Sanitized or Destroyed, and must be removed from the ATN or Supplier premises without such sanitization or destruction, Supplier shall utilize Secure Transportation to a ATN or other disposal site. Supplier shall track disposition of the media (e.g., Destroyed by Supplier, Sanitized by Supplier, conveyed to a ATN-authorized third party for Destruction, etc.) and provide to ATN a Certificate of Sanitization (COS) and/or Certificate of Destruction (COD) upon completion of the Sanitization, or Destruction.

v) Required Records: Supplier shall maintain records at the serial number level for four years of all receipts and disposition which identify the media (or computing assets) being processed. All records pertaining to the disposition of each of the media or computing assets must be available for audit and verification by ATN during this four year period. The Supplier must provide reports monthly to ATN

g) **Shipment of Sensitive Information:**

i) Non-Electronic Sensitive Information: Whenever possible, Sensitive Information in non-electronic form should be converted to electronic form for secure transmission in accordance with this document , and all non-electronic hard copies Destroyed as specified in this document . If such conversion is impracticable, Sensitive Information in non-electronic hardcopy form must be shipped in the United States using U.S.

Postal Service Registered Mail with return receipt, or the substantial equivalent thereof by a licensed overnight courier or delivery service. Any shipment of Sensitive Information in non-electronic (hardcopy) form between a United States and foreign point must be specifically pre-approved by ATN in writing and must be shipped in accordance with such instructions as ATN provides in its approval.

ii) Electronic Media containing Sensitive Information: If electronic media containing Sensitive Information are shipped, the Sensitive Information must be encrypted using Storage Encryption unless shipped in accordance with the Secure Transportation requirements herein.

4) <u>Logical Security Requirements (Suppliers conducting information processing of ATN Information)</u>

a) Logical Access Control

Supplier must develop logical access controls for all computing systems handling ATN Confidential and/or Sensitive Information. Logical Access controls must include:

i) The assured enforcement of authentication controls to limit access to information systems to only those individuals who are currently active and who are authorized to access a given information system.

ii) A secure and reliable method of enforcing authorization controls which limit access to ATN Sensitive Information and ATN Confidential Information to only previously-authorized Supplier Staff.

iii) Use of the "principle of least privilege" model for access, enabling Supplier personnel to access only such information and resources as are necessary when they perform under the Agreement for the role assigned to the authorized user,

iv) A process of controlling User IDs and other identifiers to ensure they are unique among users and are not shared.

Note: Sensitive Personal Information must not be used as an authentication or an authorization mechanism to obtain a password, or for log in rights or for access to any application, system, website or database owned or operated by ATN or on ATN's behalf. The last four digits of a Social Security number, passwords, PINs, challenge responses and/or access codes are permitted to be used for such purposes in conjunction with other data.

v) A process which will immediately terminate access by an employee or contractor who no longer requires access to perform under the Agreement (e.g., a terminated or reassigned employee/contractor).

vi) Periodic review of access, authorization and other applicable monitoring logs on all systems to ensure the access control and authentication systems are performing as expected.

vii) Supplier shall use processes that utilize industry standard password selection and aging procedures to limit opportunities for compromise of password security. Such password procedures should include some but not be limited to the following:

(1) A process to ensure that no user or information system may utilize Supplier-supplied default account passwords.

(2) A secure method of assigning and selecting passwords or other unique identity validation values, such as biometric registration values or the issuance of one-time-password token devices.

(3) Limit repeated access attempts by locking out the user ID after not more than six (6) attempts with a thirty (30) minute minimum lockout duration

(4) Verification of user identity before password resets;

(5) All passwords must be have first-time passwords set to a unique value for each user and change immediately after the first use;

(6) Inactive accounts must be disabled after 90 days;

(7) Password must be changed at least every ninety (90) days;

(8) Passwords must be at least eight (8) characters and must include letters and numbers;

(9) Supplier must require users to submit passwords that are different than any of the last four (4) passwords the individual has used;

(10) If a session has been idle for more than fifteen (15) minutes, require the user to re-enter the password to reactivate the terminal.

(11) Control and encrypt with a 1-way hash, data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect.

b) Access Logging and Monitoring

i) Supplier must maintain electronic logs of persons accessing ATN Confidential and/or Sensitive Information depicting the details of the access and transactional changes made.

ii) Logs must be maintained for inspection by ATN for a minimum of ninety (90) days.

iii) Logs shall be stored centrally on Supplier owned or third party controlled systems that cannot be altered by users or privileged users.

iv) At a minimum logs shall capture the following information for all access to ATN Confidential and/or Sensitive Information:

(1) Unique user ID;

(2) Login/Logout time;

(3) System/data set accessed;

(4) Failed login attempts;

(5) Activity (for privileged users such as data base administers, system administrators, etc.) including changes to permissions, changes to data, etc.)

v) Access logs shall be reviewed by Supplier at least daily and provided to ATN for inspection upon reasonable request. Alternatively, log parsing tools which automatically generate alerts based on information security rules may be utilized provided that alerts are reviewed and appropriate action is taken, at least daily.

c) Network and Communications Security

The Supplier must develop and implement network and communications security policies, procedures and technology to control and detect potential network and communications information security system issues and failures.

At a minimum, Supplier must have:

i) Firewall controls at appropriate points in the Supplier network to control the ingress and egress of communications and data to environments containing ATN Sensitive Information and/or Confidential Information. At a minimum, Network Firewalls must protect all connections to open, public networks. System Security Patches and updates for Firewalls must be implemented in a timely manner not to exceed 30 days following release.

ii) Supplier must employ industry standard intrusion detection systems (IDS) for any environment into which Sensitive Information will be placed.

(1) Network IDS must be placed on network connection points between the Supplier environment containing the ATN Confidential and/or Sensitive Information and other network environments. Alternatively, Host- Based IDS may be placed on all computing assets storing, processing or transmitting ATN Confidential and/or Sensitive Information.

(2) IDS must be configured with business rules appropriate to the environment and must be configured to generate alerts immediately.

(3) Signatures and software for IDS must be kept current and up to date.

(4) IDS alerts must be reviewed at least daily by trained security personnel.

iii) System Segmentation

(1) Information systems storing, processing or transmitting Sensitive Information must be logically isolated from systems that handle other companies' information. For example, Supplier must use separate database server instances for the processing of ATN data or must use separate virtual

operating system images than those used or accessed by other companies who the Supplier may also service.

(2) At no time may ATN Sensitive Information and/or Confidential Information be housed on a server shared by companies other than the contracting Supplier. For example, a shared web server that is used by several companies and maintained by an Internet Service Provider must not be used to house ATN data. This requirement also applies to "cloud-based" services.

(3) Internet-facing web servers must be dedicated to this task, and must not host internal (intranet) applications for the Supplier.

iv) Transport Encryption for all electronic communications that contain Sensitive Personal Information, and Transport Encryption for ATN Confidential and/or Sensitive Information that traverses networks outside of the direct control of the Supplier or ATN (including, but not limited to, WI-FI, the Internet and cell phone networks).

v) Transport encryption of all data containing Sensitive Information to be transmitted wirelessly.

vi) Policies, procedures and appropriate technology solutions to ensure all systems receive and apply the most current security updates on a regular basis.

vii) No remote access to Sensitive Information, from home or other location that is not at the premises of the Supplier or ATN shall be permitted without the specific authorization of ATN, and such authorization will be conditioned on measures that maintain the security of such Sensitive Information and that prevent unauthorized access thereto, or unauthorized copying or retention thereof. All remote access to Sensitive Information must require Strong Authentication and Encrypted transmissions.

viii) Logical Security Requirements when connecting Supplier controlled devices to ATN Networks

(1) All Supplier Devices to be used to connect to the ATN Network must be either provided by ATN or alternative must be owned or leased by the Supplier (personally-owned equipment may not be used to perform work for ATN).

(2) Supplier personnel accessing ATN networks must not have any concurrent access to other non-ATN networks from their workstation(s) while connected to ATN's Network unless that access is through the ATN Network.

(3) All computing device remote access to the ATN Network must utilize approved ATN Virtual Private Networks including Client-based access, transport encryption and strong authentication.

(4) Supplier Devices must not traverse any unencrypted wireless networks while attaching to the ATN network. All wireless connections should utilize transport encryption utilizing WPA2 in enterprise or PSK mode at a minimum (WEP encryption is not permitted).

d) Information Systems and Device Management

i) General Requirements

(1) All Supplier Devices used to store, process or transmit ATN Confidential and/or Sensitive Information, and/or to provide information services to ATN in connection with work under the Agreement, must either be provided by ATN or alternatively, must be owned or leased by the Supplier (personally-owned equipment may not be used to perform work for ATN).

(2) All assets controlled by Supplier used to perform work for ATN must be tracked using an inventory management system including the following information.

a. Name, location, retention schedule, and ATN-assigned data classification level f the information asset such as a database or file system.

b. A knowledgeable individual owner of each information asset (the default owner of an information asset is its creator)

c. Computer systems (i.e. Servers – Host Name/IP Address) that house ATN data

d. Storage encryption status for any Sensitive Information (both at rest and on any back up media).

(3) All Supplier Devices used to perform work for ATN should be centrally managed by the Supplier.

(4) All Supplier Devices used to perform work for ATN must be managed for the application of operating system and applicable software patches. Critical operating system and software security patches must be installed in a timely manner not to exceed one (1) month following release for public availability.

(5) All Critical Security Patches for workstations shall be installed within 7 days of publication from the software or hardware Supplier.

(6) All Supplier Devices shall have current antivirus software installed (if technically feasible) and configured to check for updates on a daily basis at a minimum.

(7) All Supplier Devices that connect to the Internet shall have a personal firewall or its equivalent enabled and configured to only allow connections to authorized business applications. By default, the personal firewall must use a default deny rule that blocks inbound traffic that is not specifically allowed in the course of a specific communication

(8) All Supplier mobile computing devices (tablets, notebooks computers, PDAs, etc.) and portable storage devices (portable drives, flash drives, thumb drives, optical disc media, etc.) used to store or process ATN Sensitive Information and/or Confidential Information must have "whole disc" or other device Storage Encryption enabled for internal as well as peripheral and removable media. Encryption keys for mobile computing devices and portable storage devices must be kept in escrow and sufficiently protected by the Supplier to enable forensic recovery of data on any protected device. Whole disk Encryption should be implemented with a Pre-Boot authorization configuration.

(9) Supplier personnel must not communicate, store or process any ATN confidential data on any email, storage or processing repository that is outside of the direct ownership and control of Supplier. For example, the use of personal web email accounts, web-based backup services, Internet-based document editing or public cloud-based computing services are prohibited without express written permission from the ATN Sponsor.

(10) Sensitive Information data should not be stored or used in testing or other non-production environments. If this use is required, an authorized exception permitting such use must granted in writing by ATN, and such data must either be (a) masked so that it no longer meets the definition of Sensitive Information, or (b) protected using controls against unauthorized access, copying or viewing that are comparable to those required for the protection of Sensitive Information in production environments.

ii) Data Storage Requirements

(1) Data Obfuscation

a. All Sensitive Personal Information and Personally Identifiable Information at rest must be encrypted using Storage Encryption. CPNI-PI should be encrypted using Storage Encryption. Storage Encryption of the device on which such information is stored will satisfy these requirements.

b. Data Replacement or field level masking may be acceptable methods of obfuscation. Such methods must be approved in writing by ATN prior to implementation.

(2) Encryption Key Management

a. Supplier shall implement key and seed management procedures that enable ATN Confidential or Sensitive Information to be retrieved if the person who encrypted such data is unable or unwilling to decrypt the data.
b. Supplier shall maintain a written and tested process for key rotation on a periodic basis (at least annually) or in event of compromise (does not apply to keys for data stored in offsite backup).
c. Keys and seeds shall be properly protected, using either physical procedures including very limited access control, separation of duties and logging/monitoring key access or encryption no less robust than is required for Supplier's own most highly confidential or Sensitive Personal Information and not accessible by unauthorized personnel.
d. Additionally, Supplier shall require split keys for all key encryption such that one person does not have the full key for any data encrypted at rest. Generally, Encryption Keys should also be encrypted.

iii) Data Backup Requirements

(1) ATN Sensitive Information and/or Confidential Information must be backed up on separate tapes/drives than data belonging to or accessed by other companies.

(2) Backups must be encrypted with Storage Encryption that accommodates key escrow by supplier

(3) Backup media must be physically secured against theft or tampering and must implement physical controls that comply with all applicable state and federal requirements.

(4) Chain of custody records must be maintained for all backup media containing ATN Sensitive Information and/or Confidential Information moving to offsite storage of backups

(5) Supplier must ensure that all backup media is tracked and must ensure that contractual data destruction requirements can be met.

5) Use of Open Source Code, Peer Review and Code Review

a) Supplier must disclose to ATN all open source code utilized to develop custom code and provide ATN an opportunity to review all such open source code prior to its utilization within or with custom developed code.

b) Supplier shall implement peer review throughout the development process and make use of code review tools to ensure secure coding and to identify malicious code or code misconfigurations.

6) Requirement for Suppliers performing Information Processing at Supplier Locations to have Business Continuity Planning/Disaster Recovery (BCP/DR) Plan

a) Supplier must ensure preparation, maintenance, and regular test of a BCP/DR plan that ensures that all critical computer and communication systems will be available in the event of emergency or a disaster, and meet service level and recovery time and recovery point objectives.

b) BCP/DR plans must be tested at least annually, and all test results must be periodically reported to ATN.

c) So that the business processes may be quickly re-established following a disaster or outage, Supplier must maintain an updated inventory of all critical production systems and supporting hardware, applications and software, projects, data communications links, and critical staff at both primary and secondary sites.

d) Any emergency event-related disruption of business activities must be reported forthwith to a designated ATN contact.

7) Requirement for Notification of Breach of Security

a) Supplier must maintain an internal or third-party professional security service with the capability of investigating, responding to and mitigating any potential or actual security incidents within Supplier's area of operations that involves ATN Sensitive Information and/or Confidential Information throughout the period of time in which Supplier maintains such information in its systems or facilities (or those of permitted subcontractors).

b) Supplier must establish and maintain an easily understandable procedure for Supplier Staff to report security incidents to an appropriate Supplier security contact, and for such information to be reported to a designated ATN contact.

c) The supplier's incident response team must have documented formal procedures that comply with Industry Standards and applicable laws addressing investigation and response to information security incidents. The procedures must include documentation describing the steps taken to correct discovered breaches.

d) Supplier's information security policies and procedures must require the immediate reporting of suspected or actual violations of policy to an appropriate Supplier security contact.

e) Supplier must as soon as practicable, not to exceed four hours following discovery of an unauthorized disclosure or security breach, notify and update ATN via electronic mail to ITsupport@ATNI.com and by calling ATN's Helpdesk number (**404-554-8222)** of such disclosure or breach, with confirmation sent to the contract notice addressee set forth in the Agreement by the means set forth therein, of:

i) Any Security Breach or other actual or threatened unauthorized access or release of ATN Sensitive Information or Confidential Information or to the systems holding or providing access to such ATN information.

ii) Any occurrences of viruses and malicious code, not mitigated by deployed detection and protection measures, on any workstation or server used to provide services under the Agreement or applicable Statement of Work or Order thereunder.

f) Following notification to ATN in accordance with the previous subsection, or notification to Supplier by ATN of a security incident or breach that ATN reasonably believes was caused by Supplier, Supplier must: provide regular updates to ATN; investigate the incident or potential breach of security; report the results of such investigation to ATN; cooperate with ATN in any ATN investigation of the breach and the effects thereof; allow ATN to inspect Supplier computers that ATN reasonably believes caused or were involved in the breach; and implement corrective measures to prevent future breaches.

g) Notwithstanding its notification(s) to ATN, Supplier must comply with all applicable notification requirements imposed by law, including but not limited to notification requirements under federal, state and local laws protecting privacy.

8) <u>Audit Compliance and ATN's Right to Audit Supplier Operations</u>

a) Supplier must be prepared to provide necessary confirming documentation in support of ATN's external audits (such as Sarbanes-Oxley or PCI) upon ATN's request pursuant to the terms of the Agreement.

b) Supplier must permit ATN to audit its security controls periodically (no more than once per calendar year or other period specified in the Agreement), and cooperate with ATN in such audit.

c) Supplier shall provide ATN internal controls reporting ("Controls Reports") prepared under SSAE 18 (AT801) or ISAE 3402 attestation standards on an annual basis covering all systems and facilities used to provide the Services to ATN and/or any ATN affiliate. Such Controls Reports will be of the SOC1 Type 2 and SOC 2 Type 2 designations and will cover at least nine months of a respective twelve-month period. Subscriber shall issue bridge letters for those periods (not to exceed three (3) months) where coverage is not provided. The SOC2 Type 2 shall cover the following trust principles: security, confidentiality, availability, processing integrity, and privacy. Supplier shall provide a copy of the Controls Reports to ATN by December 31 of each year. If any Controls Report identifies any deficiency, Supplier shall promptly remediate such deficiency at its expense.

d) Supplier must provide copies of relevant security policy, process, and procedure documents to ATN for review and audit purposes upon request. ATN may review and recommend reasonable changes, and Supplier must amend the policies or respond with mitigating controls and responses within a reasonable time period.