AT&T Supplier Information Security Requirements (SISR) – v6.2, January 2017

The following AT&T Supplier Information Security Requirements ("Security Requirements") apply to Supplier (as previously defined) when performing any action, activity or work under the Agreement where any of the following occur (**hereinafter referred to as "In-Scope Work"**):

1. The collection, storage, handling, backup, disposal, and/or access to In-Scope Information (as defined below);
2. Providing or supporting AT&T branded applications and/or services using non-AT&T Information Resources (as defined below);
3. Connectivity to AT&T's Nonpublic Information Resources (as defined below);
4. The development or customization of any software for AT&T; or
5. Website hosting and development for AT&T and/or AT&T's customers.

The Security Requirements are not intended to apply to products or applications acquired from the Supplier by AT&T for use by AT&T.

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.

"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 Internet. A DMZ helps prevent outside users from gaining direct access to internal Information Resources. Inbound packets from the untrusted external network terminate within the DMZ and are not allowed to flow directly through to the trusted internal network. All inbound packets which flow to the trusted internal network originate within the DMZ.

"Information Resource(s)" means systems, applications, websites, networks, network elements, and other computing and information storage devices, along with the underlying technologies and delivery methods (e.g., social networks, mobile technologies, cloud services, call and voice recording, Application Program Interfaces (APIs)), used in conjunction with supporting AT&T and/or used by Supplier in fulfillment of its obligations under the Agreement.

"In-Scope Information" means confidential data, including, Sensitive Personal Information (SPI) (as defined below), proprietary data and/or trade secret data of AT&T, including data of others that AT&T is obligated to protect, if any. In addition to the SPI data elements listed in the Table of AT&T SPI Data Elements found at the end of this appendix, examples of In-Scope Information include general AT&T internal operational information, network architecture and/or engineering information, Customer Proprietary Network Information (CPNI), software source code for software developed or customized for AT&T, information security incident reports, nonpublic marketing and financial information, and AT&T end user customer contact lists.

"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.

"Multi-Factor Authentication" (also known as Two-Factor Authentication and Strong Authentication) means the use of at least two of the following three types of authentication factors:

- A physical or logical credential the user has, such as an electronically readable badge, a token card or a digital certificate;
- A knowledge-based credential, such as a password or PIN; and
- A biometric credential, such as a fingerprint or retina image.

"Nonpublic Information Resources" means those Information Resources used in connection with the Agreement to which access is restricted and requires proper authentication and authorization.

"Sensitive Personal Information" or "SPI" means the data elements listed in the "Table of AT&T SPI Data Elements" located at the end of this appendix. All SPI Data Elements are considered In-Scope 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 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.

"Supplier Entity" or "Supplier Entities" means Supplier, its affiliates and subcontractors.

In accordance with the foregoing, Supplier shall:

System Security

1. Actively monitor industry resources (e.g., www.cert.org, pertinent software vendor mailing lists and websites, and information from subscriptions to automated notifications) for timely notification of all applicable security alerts that pertain to Supplier's Information Resources.
2. At least quarterly scan Supplier's Information Resources with industry-standard security vulnerability scanning software to detect security vulnerabilities, and remediate all critical, high, and medium risk security vulnerabilities identified.
3. Deploy Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS), in an active mode of operation that monitors all traffic entering and leaving Information Resources in conjunction with the Agreement.
4. Maintain and adhere to a documented process to remediate security vulnerabilities that may impact Information Resources, including, those discovered through industry publications, vulnerability scanning, virus scanning, IDS/IPS alerts, and the review of security logs, and promptly apply appropriate security patches.
5. Assign security administration responsibilities for configuring the security parameters of host operating systems to authorized users only.

6. Harden Supplier's Information Resources by utilizing a minimum security baseline configuration based upon industry best practices to reduce available ways of attack. This typically includes changing default passwords, the removal of unnecessary software, unnecessary UserIDs, usernames or logins, and the disabling or removal of unnecessary services. This hardening of the system's security configurations, operating system software, firmware and applications are to prevent exploits that attack flaws in the underlying code.
7. RESERVED
8. Limit authorized system administrators (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. All usage of system administrator access must ensure that individual accountability is maintained. All privileged activities must be enforced with appropriate segregation of duties.
9. Enforce the rule of least privilege by requiring application, database, network and system administrators to restrict access by users to only the commands, In-Scope Information and Information Resources necessary for them to perform authorized functions. Supplier shall ensure that the use of AT&T's Information Resources by Supplier Entities shall only be for the performance of In-Scope Work or functions explicitly authorized in the Agreement.

Physical Security

10. Ensure all Supplier's Information Resources intended for use by multiple users must be located in secure physical facilities with access limited and restricted to authorized individuals only.
11. 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.

Network Security

12. When providing Internet accessible services to AT&T, have Denial of Service (DoS/DDoS) protections in place. In addition, protect In-Scope Information by the implementation of a network DMZ. Web servers providing service to AT&T shall reside in the DMZ. Information Resources storing In-Scope Information (such as application and database servers) shall reside in a trusted internal network.
13. For the purpose of demonstrating compliance with certain Security Requirements applicable to network architecture and network topology, if requested by AT&T, provide AT&T with a high-level copy of their logical network diagram. The network diagram needs to provide information regarding placement of information resources and security devices (such as Security Gateways, servers, DMZs, IDS/IPS, DoS/DDoS protections, database and applications servers, etc.) within the Supplier's network that are and/or will be used to support AT&T.
14. Use Strong Encryption for the transfer of In-Scope Information outside of AT&T-controlled or Supplier-controlled networks or when transmitting In-Scope Information over any untrusted network. This applies to all transmissions of In-Scope Information, including, In-Scope Information transmitted using IM, video, emails, and VoIP. This also applies to In-Scope Information contained in emails or attachments to emails.
15. Require Multi-Factor Authentication for any remote access use of Nonpublic Information Resources.

Information Security

16. Use logical access controls to protect In-Scope Information and applications from unauthorized access; and use physical access controls where adequate logical controls are not implemented to provide such protection.
17. Maintain procedures for the backup, recovery and eventual destruction of In-Scope Information. Such procedures shall be documented, secure, and available to AT&T upon request.
18. Limit access to In-Scope Information only to authorized users or systems on a need to know basis. Supplier shall ensure that the use of In-Scope Information by Supplier Entities shall only be for the performance of In-Scope Work.
19. Maintain documented processes and controls to detect and terminate unauthorized attempts to access, collect, modify, store, handle and/or dispose of In-Scope Information; and monitor, and remediate unauthorized access and/or changes to system and application configuration files.

Identification and Authentication

20. Assign unique UserIDs to authorized individual users, assign individual ownership to system service accounts, and ensure that system service accounts are not-shared by administrators.
21. Maintain a documented UserID lifecycle management process that includes manual and/or automated processes for approved account creation, account removal within one (1) business day, and account modification for all Information Resources and across all environments. Such process shall include review of access privileges and account validity to be performed at least each calendar year.
22. Limit failed login attempts by no more than six (6) consecutive failed login attempts by locking the user account. Access to the user account can be reactivated through the use of 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.
23. Terminate interactive sessions on a user's workstation, or activate a secure, locking screensaver requiring authentication, after a period of inactivity not to exceed fifteen (15) minutes. On all other Information Resources terminate inactive sessions not to exceed thirty (30) minutes.
24. a. Use an authentication method based on the sensitivity of In-Scope Information. Whenever authentication credentials are stored, Supplier shall use Strong Encryption and/or one-way hashing based upon strong cryptography.

    b. Passwords must be complex and meet the following password construction requirements:

    - Be a minimum of eight (8) characters in length.
    - Include characters from at least two (2) of these groupings: alpha, numeric, and special characters.
    - Not be the same as the UserID with which they are associated.
    - Not contain repeating or sequential characters or numbers.

    c. PINs must meet the following:

    - Be a minimum of four (4) numbers; and
    - Not contain repeating or sequential numbers.

    d. Require password and PIN expiration at regular intervals not to exceed ninety (90) calendar days.

25. When providing users with a new or reset password, or other authentication credentials, use a secure method to provide this information, and require reset at first login whenever a temporary credential is used.

Warning Notice

26. For Nonpublic Information Resource(s) that are AT&T-branded, display a warning notice, or alternatively provide a link to such warning notice, on login screens/pages that cover the following:

    a. Information Resources are restricted to authorized users. In jurisdictions where unauthorized access is a violation of the law, add the following statement to the warning notice:

       "Unauthorized access is a violation of law."

    b. Where the use of the Nonpublic Information Resources are monitored, add the following statements to the warning notice:

       "This Information Resource may be monitored for administrative and security reasons;" and

       "By proceeding the user consents to this monitoring."

    c. AT&T may specify in writing alternative warning notice content that Supplier shall use in place of the information listed above.

Software and Data Integrity

27. Have current antivirus software installed and running to scan for and promptly remove or quarantine viruses and other malware.

28. Separate non-production Information Resources and In-Scope Information from production Information Resources and In-Scope Information

29. Maintain a documented change control process including back-out procedures for all production environments.

30. For applications which utilize a database that allows modifications to In-Scope Information, logs for forensic analysis purposes shall be created, retained and available to AT&T for a minimum of six (6) months either on-line or on backup media as follows:

    a. where transaction logging is supported have database transaction logging features enabled; or

    b. where transaction logging is not supported have some other mechanism that logs all modifications to In-Scope Information stored within the database including timestamp, UserID and information modified.

31. a. For all software developed or customized for AT&T under the Agreement, review and scan such software to find and remediate security vulnerabilities prior to initial deployment and upon any modifications and updates, as follows:

        i. Source code vulnerability scanning must be performed where such tools are commercially available. Where such tools are not commercially available, automated and/or manual processes and procedures must be documented and used.

        ii. Scan results and remediation plans must be made available to AT&T upon request.

    b. Where technically feasible, for all software used, furnished and/or supported under the Agreement, review and scan such software to find and remediate security vulnerabilities prior to initial

deployment and upon any modifications and updates based on potential risk that a given vulnerability is or can be exploited.

32. 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.

Monitoring and Auditing Controls

33. Restrict access to security logs to authorized individuals, and protect security logs from unauthorized modification.

34. Review, on no less than a weekly basis, all anomalies from security and security-related audit logs and document and resolve logged security problems in a timely manner.

    a. Such reviews may initially be performed by automated processes that promptly issue alarms and/or alerts when such processes detect significant anomalies so that the issuance of such alarms and/or alerts causes prompt investigation and review by responsible individuals; and

    b. If automated processes successfully resolve a logged security problem, no further action by responsible individuals is required.

Reporting Violations

35. Maintain a documented procedure to be followed in the event of a suspected attack upon, intrusion upon, unauthorized access to, loss of, or other security breach involving In-Scope Information in which Supplier shall:

    a. Promptly investigate and make a determination if such an attack has occurred; and

    b. In the event that a successful attack has occurred involving In-Scope Information or it is impossible to determine whether the attack was successful then Supplier shall promptly notify AT&T by contacting:

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

        ii. Supplier's contact within AT&T for service-related issues.

36. After notifying AT&T whenever there is a successful attack upon, intrusion upon, unauthorized access to, loss of, or other breach of In-Scope Information, provide AT&T with regular status updates, including, actions taken to resolve such incident, at mutually agreed intervals or times for the duration of the incident and, within seven (7) calendar 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.

Mobile and Portable Devices

37. Use Strong Encryption to protect all In-Scope Information stored on Mobile and Portable Devices.

38. Use Strong Encryption to protect all In-Scope Information transmitted using or remotely accessed by network-aware Mobile and Portable Devices.

39. Maintain documented policies, standards and procedures for Mobile and Portable Devices used to access and/or store In-Scope Information that include the following requirements:

    a. All users must be authorized for such access and their identity authenticated;

b. Mobile and Portable devices must be physically secured and/or in the physical possession of authorized individuals;

c. Where technically feasible, use a remote wipe capability on such devices to promptly and securely delete In-Scope Information, when such devices are not in the physical possession of authorized individuals nor otherwise physically secured; and

d. Jailbroken or rooted smartphones cannot be used to perform In-Scope Work.

40. Implement and maintain a documented policy that prohibits the use of any:

a. Supplier-issued Mobile and Portable Devices to access and/or store In-Scope Information unless the device is administered and/or managed by Supplier; and

b. Non-Supplier issued Mobile and Portable Devices to access and/or store In-Scope Information, as in cases where Supplier has a "Bring Your Own Devices" (BYOD) program, unless adequately segregated and protected such as by a Supplier administered and/or managed secure container-based solution.

Security Gateways

41. Require Multi-Factor Authentication for administrative and/or management access to Security Gateways, including any access for the purpose of reviewing log files.

42. Maintain 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.

43. At least annually, ensure that each Security Gateway rule was properly authorized and is traceable to a specific business request, and that all rule sets either explicitly or implicitly end with a "DENY ALL" statement.

44. Use monitoring tools to ensure that all aspects of Security Gateways (e.g., hardware, firmware, and software) are operational at all times. Ensure that all non-operational Security Gateways are configured to deny all access.

Wireless Networking

45. When using radio frequency (RF) based wireless networking technologies (e.g., Bluetooth and Wi-Fi) to perform or support In-Scope Work for AT&T, ensure that all In-Scope Information transmitted must be protected by the use of appropriate encryption technologies sufficient to protect the confidentiality of In-Scope Information; provided, however, that in any event such encryption shall use no less than key lengths of 256-bits for symmetric encryption and 1024-bits for asymmetric encryption. 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.

46. RESERVED

Connectivity Requirements

47. 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 Supplier shall not establish additional interconnections to AT&T's and AT&T's customers' Nonpublic Information Resources without the prior consent of AT&T and shall:

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. If the agreed upon connectivity methodology requires that Supplier implement a Security Gateway, maintain logs of all sessions using such Security Gateway. Such session logs must include sufficiently detailed information to assist with a security incident or a forensic investigation (e.g., identification of the end user or application accessing AT&T). Such session logs must include origination IP address, destination IP address, ports/service protocols used and duration of access. Such session logs must be retained for a minimum of six (6) months.

c. When presented with evidence by AT&T of a threat to AT&T or AT&T's customers' Nonpublic Information Resources originating from the Supplier's network (e.g., worm, virus or other malware, bot infection, Advanced Persistent Threat [APT], DoS/DDoS attack, etc.), promptly cooperate with AT&T to isolate and terminate the threat. In addition, Supplier shall provide AT&T with a written plan to prevent any such future threats within seven (7) calendar days after mitigation of the threat. In the event Supplier fails to cooperate with AT&T in resolving the threat AT&T reserves the right to terminate the appropriate Order and/or Agreement.

Supplier Entity Compliance

48. Supplier shall:

Ensure all Supplier Entities performing In-Scope Work are aware of, and in compliance with, these Security Requirements. Supplier shall contractually obligate, or cause (as the case may be) its Subcontractors that perform any In-Scope work to comply with these Security Requirements, or in any event, requirements that are no less stringent. Upon AT&T's request, Supplier will provide documentation and/or evidence to substantiate such compliance to AT&T's satisfaction.

Protection of AT&T's SPI

49. Use Strong Encryption to protect AT&T's SPI when transmitted over any network.

50. Use Strong Encryption to protect AT&T's SPI when stored.

Business Continuity Plan

51. Supplier shall maintain and upon AT&T's request, promptly furnish to AT&T Supplier's Business Continuity Plan that complies with the requirements set forth in Business Continuity Plan Requirements (BCPR) available at http://www.attsuppliers.com/downloads/Business-Continuity-Plan-Requirements-BCPR-SISR.pdf and incorporated herein by reference, which may be changed from time-to-time by AT&T.

Table of AT&T SPI Data Elements

Data elements in the following tables are classified as *AT&T Proprietary (Sensitive Personal Information)* and **must** be treated as such when used in their entirety, unless:

a. Explicitly stated in the following tables.
— or —
b. It relates to an individual's own information kept for their own purposes (This type of personal data **should not** be stored on AT&T assets or premises).

The following are true for all data formats including scanned images, PDFs, JPGs.

The following "Privacy" data elements have been classified as AT&T Proprietary (Sensitive Personal Information) when they apply to an employee, contractor, customer or supplier, except where explicitly stated otherwise.

Individual Identification

Data Element	Description
Driver's License Number	
Taxpayer Identification Number	
U.S. Social Security Number (SSN)	
Nationally-Issued Identification Number	Includes visa and/or passport values. Excludes any such numbers that are issued on the understanding that they must be a matter of public record, e.g., U.S. FCC Radio License.
State or Province-Issued Identification Number	

Financial Data

Data Element	Description
Payment Card Number	Primary Account Number (PAN) for all types of payment card (corporate, personal, etc.)
Payment Card Security Data	The security data used in association with a payment card (corporate, personal, etc.) in order to confirm legitimate use. Includes for example Personal Identification Numbers (PINs) used with payment cards but excludes PINs used to authenticate access to AT&T systems.
Bank Account Number	Includes all types of bank accounts (savings, checking, etc.) both personal and business in an individual's name. Excludes bank routing number.

Computer Identification and Authentication

Data Element	Description
Customer Authentication Credentials Applies to Customers only	Values used by customers to authenticate and permit access to: • The customers' personal information, including CPNI and AT&T Proprietary (Sensitive

	Personal Information) — or — • An application enabling the customer to subscribe to, or unsubscribe from, AT&T services — or — • An AT&T service the customer is subscribed to Includes: Personal Identification Numbers (PINs), passwords or passcodes. Excludes Card Security Codes and PINs used in association with payment cards.
Customer Authentication Credential Hints Applies to Customers only	Answers to questions used to retrieve customer authentication credentials, for example mother's maiden name.
Location-Based Information (LBI)	Information that identifies the current or past location of a specific individuals' mobile device. This element contains two factors both of which must be present and able to be associated with each other: 1. A mobile device's location (e.g. a map address, or latitude and longitude together with altitude where known) derived from the mobile device through activities such as GPS or network connectivity rather than as a result of user action (e.g. revealing location in the content of an email, or SMS) -and - 2. An individual's identity derived from a unique identifier assigned to that mobile device such as customer name, MSISDN, IMSI, IMEI or ICCID.

Other Data

Data Element	Description
Date of Birth (DOB)	An individual's full and complete DOB, i.e. including Month, Day and Year. Excludes partial DOB where only Month and Day are used without Year. This element contains two factors both of

	which must be present and able to be associated with each other: 1. A full and complete DOB - and - 2. The individual's identity, either explicitly or via a unique identifier that can be linked to that individual.
Biometric Data	Measures of human physical and behavioral characteristics used for authentication purposes, for example fingerprint, voiceprint, retina or iris image. Excludes templates that contain discrete data points derived from biometric data that do not hold the complete biometric image, where the template cannot be reverse engineered back to the original biometric image.
Criminal History Subject to non-U.S. jurisdiction[1]	Information about an individual's criminal history, e.g. criminal check portion of a background check.
Racial or Ethnic Origin Subject to non-U.S. jurisdiction[1]	Data specifying and/or confirming an individual's racial or ethnic origin.
Trade Union Membership Subject to non-U.S. jurisdiction[1]	Data specifying and/or confirming an individual is a member of a trade union outside of the U.S.
Information Related to an Individual's Political Affiliation, Religious Belief, or Sexual Orientation Subject to non-U.S. jurisdiction[1]	Data specifying and/or confirming an individual's political affiliation, religious or similar beliefs, or sexual life or orientation.

The following "Human Resources" data elements have been classified as AT&T Proprietary (Sensitive Personal Information) when they apply to an employee, contractor, customer or supplier:

Health Data

Data Element	Description
U.S. Protected Health Information (PHI)	Includes any U.S. health information used in AT&T's Group Health Care plans or belonging to

	AT&T's customers that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individuals that include information about: • The individual's past, present or future physical or mental health or condition, • The provision of health care to the individual — or — • The past, present, or future payment for the provision of health care to the individual. Health information of retirees, employees, or employee beneficiaries used by AT&T for purposes other than a group health plan is not PHI.
Medical and Health Information Subject to non-U.S. jurisdiction[1]	Any information concerning physical or mental health or condition. Includes disability information.

Footnotes:

Where data elements have the term "Subject to non-U.S. jurisdiction" associated with them, that data element is to be classified as AT&T Proprietary (Sensitive Personal Information) when applied to data elements subject to non-U.S. jurisdiction, irrespective of whether the data is created, handled, processed, destroyed or sanitized inside or outside the U.S.

Data Management - Sensitive Customer Data (SCD)

Data Element	Description
Customer Set Top Box Viewing History	Information about programs watched or recorded, games and applications used, etc. by AT&T customers.
Customer Web Browsing History	Information about what websites the AT&T customers visit and applications they use on any network (wireline and wireless including Wi-Fi); this does not include browsing and activities associated with the AT&T customers' use of official AT&T corporate websites.
Digital Life Data	Includes video files, sensor data and other data that is generated by our customers' use of the Digital Life service.