



NOTE: This addendum is not a pre-approved template or “envelope”. It was developed by CSO and GES Sales Legal for the SCG and PCG channels, and reviewed by Product Legal. It is intended for use when enterprise customers seek to have AT&T add the customer's data security terms to a master agreement. Use of this addendum requires review and analysis by a sales attorney, particularly when other clauses in a master agreement are non-standard (e.g., confidentiality, privacy laws, limitations of liability, disclaimer of damages).

**MASTER AGREEMENT
DATA SECURITY ADDENDUM**

Customer	AT&T
Customer Legal Name Street Address: City: State/Province: Zip Code: Country:	AT&T Corp. or enter the International Affiliate Name
Customer Contact (for notices)	AT&T Contact (for notices)
Name: Title: Street Address: City: State/Province: Zip Code: Country: Telephone: Fax: Email:	Street Address: City: State/Province: Zip Code: Country: With a copy to: AT&T Corp. One AT&T Way Bedminster, NJ 07921-0752 ATTN: Master Agreement Support Team Email: mast@att.com

This Master Agreement Data Security Addendum (“Addendum”) is an addendum to the Master Agreement referenced above. This Addendum is effective when signed by both Customer and AT&T (“Effective Date”), and continues in effect as long as Services are provided under the Master Agreement.

Customer (by its authorized representative)	AT&T (by its authorized representative)
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

Data Security - General

1.1. Neither AT&T nor Customer represents or guarantees that security procedures will prevent the loss of, alteration of, or improper access to data in its possession or under its management, but each party will comply with this Addendum concerning measures taken : (i) by Customer to encrypt data prior to transmission or storage via the Services; and (ii) by AT&T to safeguard data in transit on an AT&T network or stored by Customer on AT&T servers.

1.2. AT&T will maintain programs and processes under which employees, contractors, and subcontractors are screened, trained on security policies and made aware of their responsibilities with regard to AT&T and Customer's data. AT&T will also maintain a comprehensive security program with the objective of broadly incorporating security measures into all AT&T's computing and networking environments ("AT&T Security Program").

1.3. AT&T will maintain a set of security standards drawing upon leading industry standards (e.g., ISO/IEC 27001:2005, etc.). In providing Services under the Agreement, AT&T will observe AT&T security standards.

1.4. AT&T will regularly re-evaluate and modify its security standards at its discretion as generally accepted industry standards evolve, as new technologies emerge or as new threats are identified. AT&T's security standards are themselves sensitive information and as part of the AT&T Security Program the standards are kept confidential and generally not disclosed to third parties.

1.5. The parties acknowledge that Services offered by AT&T have varying levels of inherent security risk. In addition, some Services may involve the transmission or storage of voice and data traffic from, to, on or over third-party networks or facilities which may not have the same protections against unauthorized access that AT&T employs.

2. AT&T Information and Network Security Customer Reference Guide/AT&T Security Program

2.1. AT&T has provided Customer with a copy of the *AT&T Information & Network Security Customer Reference Guide January 2016 v5.3* which provides an overview of the AT&T Security Program as of the publication date. AT&T anticipates that the AT&T Security Program will continuously evolve, and AT&T therefore has advised Customer that the policies and procedures described in the *AT&T Information & Network Security Customer Reference Guide* may be changed by AT&T without notice to or consultation with Customer. Upon request AT&T will provide a then-current copy of the *AT&T Information & Network Security Customer Reference Guide* to Customer.

2.2. AT&T employs a broad spectrum of security tools and methods in the AT&T Security Program. Following are some of the tools and methods used by AT&T in one or more aspects of the program as of the Effective Date of this Addendum. Although the tools and methods will evolve over time, the current description provides a general indication of the depth and scope of the AT&T Security Program.

- (a) **Security Policy** – AT&T security standards are formally reviewed, approved, published, and communicated to employees and relevant parties responsible for supporting AT&T's business operations and services. AT&T has established security standards that, in combination with other processes, procedures, and responsibilities within AT&T, are consistent with the controls documented within the generally accepted international security management standard ISO/IEC 27001:2013.
- (b) **Classification of Information** – AT&T uses a multi-tiered information classification framework for categorizing and labeling information based on sensitivity of the content and specific legal requirements.
- (c) **Information and Media Handling** – AT&T security standards specify the means and levels of protection for information in transit or in storage with regard to the type of environment and media and within each information classification. The standards also specify the requirements for information destruction and media sanitization.
- (d) **Physical Access Controls** – AT&T maintains appropriate physical security practices that include the use of physical monitoring and intrusion detection systems, implementation of locks and access barriers, and screening access to facilities and equipment.
- (e) **Logical Access Controls** – AT&T maintains appropriate logical access controls that include authentication of claimed identity (using means such as passwords, PINS or tokens), periodic review of user IDs and accounts to verify continued business need, and management of user privileges in accordance with job function and business need. Password rules follow strict requirements, including a minimum number and type of characters and uniqueness from previous user passwords, user name or dictionary words.

- (f) **Network Perimeter Protection** – AT&T employs firewalls that screen incoming and outgoing traffic, and intrusion detection tools that detect unauthorized attempts to penetrate AT&T's global network. AT&T does not monitor individual customer connections for intrusions except when part of a managed security service provided for an additional fee.
- (g) **Workstation Security Management** – AT&T uses a variety of processes and technologies that include anti-malware protection and updates, personal firewall, operating system hardening and updates, power-on passwords, password-protected keyboard or screen locks that automatically trigger through inactivity, and full disk encryption where permitted by law to protect sensitive information on portable assets.
- (h) **Security Incident Management** – AT&T uses a disciplined global process for the identification of security incidents and threats in a timely manner to minimize the loss or compromise of information belonging to both AT&T and its customers and to facilitate incident resolution. AT&T 24 x 7 global network monitoring and the AT&T threat management platform and program provide real-time situational awareness and data correlation that support active incident investigation and security event case management.
- (i) **Monitoring** – AT&T maintains security audit logs that record access attempts and other security events. AT&T security administration limits user control over system security functions to protect against tampering and unauthorized access.
- (j) **Security Advisories** – AT&T internally distributes security advisories that originate from industry security organizations and equipment, software and systems suppliers. Each security advisory is categorized, assigned a severity rating, and published by the AT&T global security organization along with the timeframe within which AT&T will endeavor to resolve the vulnerability in accordance with AT&T security standards.
- (k) **Compliance** – AT&T conducts regular tests to determine if security controls are maintained and are functioning in accordance with policy. These initiatives include security status checking and vulnerability testing and management.

3. Internal and External Reviews and Audits

3.1. For certain Services, AT&T retains external auditors for periodic reviews of AT&T's security practices against various standards, such as SSAE16/ISAE3402, SysTrust, and Payment Card Industry (PCI) Data Security Standard (DSS). Additional information about external audits and certifications relevant to the Services is available from Customer's AT&T account team upon request. AT&T will provide Service Organization Control (SOC) audit reports to Customer for any audits of the Services against the SSAE16/ISAE3402 standards that AT&T undertakes as part of its general business operations. AT&T shall provide these reports to Customer upon request. Such reports are AT&T's Confidential Information and will be subject to restrictions on use and disclosure.

4. Customer Inquiries and Audits

4.1. Upon request AT&T will enter into discussions in an effort to address Customer's questions concerning the AT&T Security Program. In addition, once during a rolling 12 month period AT&T will also respond to a reasonable number of formal written questions (e.g., a questionnaire) concerning the AT&T Security Program. If AT&T's involvement in responding to such questions and concerns is more than periodic and limited in nature, Customer and AT&T will agree upon the fees to be paid by Customer to AT&T to cover costs that are not reflected in rates and charges for Services.

4.2. If the discussions and responses, along with available reports of independent auditors, do not satisfy Customer's needs, Customer may request to conduct its own security audit of certain AT&T facilities or services. No audit will be conducted until the parties have mutually agreed on the scope, time frame, and location of the audit. If Customer intends to use a third party to conduct an audit or tests, the third party will be required to enter into an appropriate non-disclosure agreement with AT&T prior to commencing the audit or testing. Audits and tests may not be conducted by third parties who are direct competitors of AT&T without AT&T's written consent or by third parties who have previously misused or misappropriated AT&T's confidential information. For some services, AT&T may require a separate written agreement setting forth specific terms and conditions for audits or tests. The following terms and conditions will generally apply to all audits, and there may be other terms or restrictions as well:

- (a) AT&T reserves the right to charge Customer reasonable fees that are proportional to AT&T's anticipated costs for providing access to facilities, information and personnel in the course of facilitating the audit.
- (b) Audits will be performed according to AT&T Security requirements and will be limited to once per rolling twelve (12) month period during normal AT&T business hours for the identified location.
- (c) AT&T will require adequate protection for AT&T's Confidential Information. AT&T will not make any disclosure which would result in the disclosure of information about other AT&T customers or services.

- (d) There may be a limit on the number of onsite auditors.
- (e) No copies may be taken of any documents (whether electronic or in hard copy) provided during the course of the audit and no document may be removed from the area where documents are available for inspection.
- (f) Physical security audits and on-site reviews of AT&T operational facilities and locations will be subject to policies maintained by AT&T Asset Protection and AT&T Corporate Real Estate or their successor organizations.

4.3. If Customer is subject to regulation and audit by governmental or other regulatory authorities having authority to examine Customer's records, AT&T will provide reasonable assistance as requested by Customer to facilitate such examinations, subject to Customer's agreement to pay reasonable fees that are proportional to AT&T's anticipated costs in facilitating the examination, and subject to the restrictions and conditions similar to those described above.

4.4. If Customer identifies a security issue during a discussion, response, audit or test, which Customer reasonably identifies as causing an unacceptable level of threat to Customer, then AT&T will work cooperatively with Customer to determine if another service with a different type or level of security might be more suitable for Customer, or if there are commercially reasonable changes that AT&T might make without altering the cost, functionality or general characteristics of the Service in question.

4.5. AT&T will review Customer's request to perform vulnerability or other testing activities on a service-by-service basis. Such activities will be subject to additional terms and conditions in order to protect AT&T infrastructure and the services and data of other AT&T customers. No tests may be conducted until the parties have entered into a separate written agreement setting forth the scope of the testing and associated terms and conditions.

5. Security Incidents

5.1. If AT&T discovers that a third party has obtained unauthorized access to Customer's data during a security breach of AT&T's network and/or data storage facilities, AT&T will promptly conduct an investigation to determine when, and if possible, how the breach occurred, and will notify the Customer of such breach. AT&T will reasonably assist Customer in investigating and assessing the extent and nature of the breach and will reasonably inform Customer of the progress of AT&T's investigation and its remediation and prevention efforts. Similarly, if Customer becomes aware of any security breach that affects the Services, Customer will promptly notify AT&T of such breach and will reasonably inform AT&T of the progress of and resolution of Customer's investigation. Customer and AT&T will each provide to the other contact information for such notifications and reporting.

6. Customer's General Security Responsibilities

6.1. Customer is responsible for establishing and implementing policies and procedures to safeguard its data and sensitive information against unauthorized access or use. Customer may have additional security responsibilities, depending on the nature of the AT&T Services used by Customer. With respect to use of AT&T Services, these responsibilities include the following, without limitation:

- (a) Selecting and implementing appropriate security measures (which may include encryption) based on the nature of the Services Customer uses and the type of information Customer transmits or stores via the Services.
- (b) Selecting and using appropriate AT&T Services, security features and options, based on Customer's specific business practices, security requirements and the type of information Customer transmits or stores via the Services.
- (c) Developing and maintaining appropriate management and security procedures, such as physical and logical access controls and processes (e.g., application logon security, including unique user identifications and passwords/pins/tokens complying with prudent security policies) on any Customer-provisioned or managed networked devices and systems.
- (d) Protecting and providing physical security of devices and systems on Customer's premises, including preventing unauthorized sensors, sniffers and eavesdropping devices from being installed on devices and systems located on Customer's premises.
- (e) Ensuring no security testing or scanning is initiated by Customer or its employees, agents or contractors on: (i) AT&T's network; or (ii) application components outside the responsibility and ownership of Customer, except pursuant to the terms of a separate written agreement with AT&T.
- (f) Promptly notifying AT&T of any actual or suspected security incidents or vulnerabilities Customer discovers relating to the Services.

7. AT&T Security Products and Services

7.1. AT&T offers managed security products and services designed to assess and protect network infrastructure. Information about managed security products and services is available from Customer's account team. From time to time AT&T may offer

some customized services. Execution of this Addendum by AT&T is not intended to imply, and will not be interpreted as implying, that any managed security service products or services, or any security-related service options offered by AT&T for a fee, will be provided to Customer free of charge.