AT&T Information & Network Security Customer Reference Guide

February, 2013

Version 5.1

Table of Contents

1 To the Reader

This document is designed for the use of AT&T current and potential business customers. The document provides:

- An introduction to AT&T and its global security organization,
- A review of AT&T security roles and responsibilities,
- A summary of customers' security responsibilities,
- An overview of AT&T's security policy and comprehensive programs that strive to ensure security is incorporated into every facet of AT&T's computing and networking environments. This overview focuses on the key elements and initiatives to safeguard AT&T's customers and their data while managed by AT&T or in transit on an AT&T network.

In general, the use of 'security' throughout this document refers to 'information and network security'.

For further information regarding AT&T, visit our website at http://www.att.com or contact your local AT&T account team.

2 Disclaimer

This document provides a summary overview of the AT&T security policy and program. In order to maximize security, AT&T does not divulge details regarding the tools and processes utilized to manage security. AT&T operates a common infrastructure shared by its customers. Consequently, AT&T must safeguard all customers on the shared network platforms, including those with uniquely hosted environments and custom safeguards.

This document is provided as summary information only. It is not a contract, and no statement, representation, or characterization within this document shall be construed as an implied or express commitment, obligation or warranty on the part of AT&T Inc. or any of its affiliates, or any other person. Accordingly, this document is not intended and shall not be construed as a contract exhibit or supplement.

All contractual obligations between AT&T and its customer are set out exclusively in a written agreement with the customer, and nothing in this document shall amend, modify, supplement or otherwise change the provisions or terms of that agreement.

AT&T may, at its sole discretion, alter the policies and procedures described in this document without notice to or consultation with any customer or other person. AT&T customers are responsible for maintaining security policies and programs appropriate to their enterprises.

3 About AT&T

AT&T Inc. is a premier communications holding company. Operating globally under the AT&T brand, AT&T is recognized as the leading worldwide provider of Internet Protocol (IP)-based communications services to businesses and a leading U.S. provider of wireless, high speed broadband Internet access, local and long distance voice. AT&T operates one of the world's most advanced and powerful global backbone networks, carrying more than 43.4 petabytes of data traffic on an average business day to nearly every continent and country, with up to 99.999 percent reliability.

4 The AT&T Global Network

AT&T provides worldwide, world-class network services to businesses in 64 countries through the AT&T Global Network. Many AT&T customers are multinational corporations with locations in multiple global regions. AT&T is responsible for managing this worldwide data network with presence on six (6) continents. This document relates to security as it is applied to the AT&T global network which consists of multiple components converging into a common Multi-Protocol Label Switching (MPLS) network:

- A global Internet Protocol/MPLS backbone network
- A circuit switched network
- Frame Relay and ATM private networks
- Internal business and management networks
- Intelligent optical network.

5 The AT&T Laboratories

AT&T Laboratories (http://labs.att.com) is the driving force behind groundbreaking communications innovations that transform the way people work, live and play. With a rich heritage of innovation, our teams of researchers and engineers continue to invent technologies that enable AT&T to bring a new generation of universal network, communications, and entertainment services to the market. AT&T Labs, Inc. is made up of approximately 1,300 of the world's best scientists and engineers, including experts in mobility and wireless data networks, IP network management, optical networking technology, high-speed / broadband Internet transport and delivery systems, information mining and data management, and next-generation speech technology. Innovations include new technologies, applications and services that support our security portfolio which enhance and safeguard the customer experience.

6 AT&T Chief Security Office - A Worldwide AT&T Security Organization

AT&T maintains a comprehensive global security organization comprised of over 1000 security professionals. This organization, the AT&T Chief Security Office (CSO), is dedicated to the protection of the AT&T global network and its service offerings. It supports a broad range of functions, from security policy management to customer-facing security solutions. The AT&T global security organization reviews and assesses the Corporation's security control posture to keep pace with industry security developments and to satisfy regulatory and business requirements. Recommendations are made to the Corporation on the technology solutions and critical skills that are to be developed or acquired in order to maintain the required security posture.

The AT&T Chief Security Office establishes policy and requirements, as well as comprehensive programs, to ensure security is incorporated into every facet of AT&T's computing and networking environments. At the executive level, the Chief Security Officer chairs the AT&T Security Advisory Council, a program where key business and functional leaders meet on a regular basis to discuss corporate security strategy, vision, and concerns. This global AT&T security organization's technical personnel work in partnership with other AT&T business units to evaluate threats, determine protective measures, create response capabilities, and ensure compliance with best security practices.

AT&T and its employees interact with and participate in several US and international security organizations.

These organizations include

- Computer Emergency Response Team/Coordination Center (CERT/CC)
- Forum of International Response and Security Teams (FIRST) Team
- U.S. Department of Homeland Security's National Security Telecommunications Advisory Committee (NSTAC) and its National Coordinating Center (NCC) for Telecommunications
- U.K. Centre for the Protection of National Infrastructure (CPNI) National Security Information Exchange (NSIE)
- Various Information Sharing and Analysis Centers (ISACs), including Information Technology-ISAC and Communications-ISAC
- US InfraGard
- Security activities within the Internet Engineering Task Force (IETF)

AT&T also participates in

- National Infrastructure Protection Center (NIPC)
- National Telecommunications and Information Administration (NTIA)
- Communication Security, Reliability, and Interoperability Council (CSRIC)
- Network Reliability Steering Committee (NRSC)

AT&T is proud to be a leader and a participant in these and other organizations both to set standards and to keep pace with industry developments.

7 Security Organization Mandate

AT&T considers network and information security to be a cornerstone of the services that it delivers worldwide. By the security policy mandate of AT&T's Chief Security Office, AT&T is committed to protecting its customers and its own information and resources from unauthorized access, disclosure, corruption or disruption of service. This security policy is designed to protect AT&T and AT&T-managed assets, and is applicable to network elements, systems, applications, data and computing devices owned or managed by AT&T.

Execution of the policy is led by the AT&T Chief Security Office organization whose role is to:

- Protect AT&T owned and managed assets and resources from security breaches by monitoring potential security threats, correlating network events, executing corrective actions, and enabling compliance with legal, regulatory, and contractual security requirements.
- Own and manage the AT&T security policies and standards for the entire AT&T Corporation and maintain ultimate responsibility for all aspects of network and information security within the corporation.
- Ensure compliance to AT&T's security policies and network and information security program in a globally consistent manner on all networks, systems, and applications, and ensure senior executives are accountable for security compliance in their business unit or region.
- Provide a competitive advantage to AT&T and offer best-in-class security for our customers.

8 AT&T Security Standards and ISO 27001 Certification

AT&T has developed and maintains AT&T Security Policy and Requirements (ASPR) a comprehensive set of security control standards based in part on leading industry standards such as ISO/IEC 27001:2005. Given the dynamic environment that AT&T supports, ASPR content is continually re-evaluated and modified as industry standards evolve and as circumstances require. In addition, operating procedures, tools and other protective measures are regularly reviewed to ensure the highest standards of security are observed throughout the corporation.

AT&T's security policies and control standards are proprietary to AT&T and are not generally disclosed to any organization or entity external to the AT&T corporate family. Maintaining the confidentiality of this information is, in itself, a facet of our security program that protects AT&T customers.

The Enterprise Mobility Security Standard (EMSS) provides guidance for organizations to follow as they are mobilizing their operations. EMSS helps organizations develop mobile security controls to strengthen data and information protection and to ensure that the many applicable regulatory or compliance concerns are sufficiently addressed on smartphones and associated ecosystems. This document is available by request from your account team.

AT&T maintains global ISO 27001 certification. This certification includes all enterprise sites and functions performed globally including all AT&T IDCs and AT&T's Hosting & Cloud Services. AT&T Executive Management has produced and implemented an approved Information Security Management System (ISMS) which complies with the requirements of ISO 27001. To maintain the certification, AT&T must undergo annual recertification assessments, which it is committed to completing and achieving ongoing certification. In compliance with the ISO 27001:2005 standard for information security, AT&T has prepared a Statement of Applicability. Additional information about AT&T's ISO 27001 certification**,** Information Security Management System (ISMS), and AT&T's Statement of Applicability is available upon request from the Customer's AT&T account team

9 AT&T Security Program

9.1 Privacy

To ensure confidentiality and appropriate protection information is accessible only to those authorized to access and view it. AT&T has implemented a four-tiered Information Classification framework for categorizing information based on sensitivity of the content and specific legal requirements. Document markings are specified for each data classification in order to identify the means and levels of protection required to safeguard information in each classification.

Sensitive personal information (SPI), such as Social Security numbers, credit card numbers, etc., related to the provision and administration of AT&T services is accorded significant protections, including encryption (where permitted by law) when stored or transmitted on untrusted networks. Customer information managed by AT&T is further protected by a standard privacy policy applicable to all employees and contractors, and a Code of Business Conduct that assigns severe penalties for violation of the duty to protect the confidentiality of SPI and other data. AT&T personnel receive periodic awareness and compliance training to reinforce the company's privacy standards.

AT&T employs information and data destruction and sanitization procedures to ensure that electronic and physical media used to store proprietary data and information are physically destroyed, shredded, erased or wiped according to commercially accepted practices when the media is no longer required for business purposes or hard copy leaves the control of the company. Equipment containing storage media are checked to ensure that any proprietary data and licensed software has been removed or securely overwritten prior to disposal.

The AT&T Chief Privacy Office maintains AT&T's corporate privacy policy. Compliance with legal and regulatory privacy requirements is addressed in section 9.11 "Internal and External Reviews and Audits."

9.2 Access Controls

9.2.1 Physical Access Control

AT&T operates in secured environments where physical access to staff office space, switching centers, global network and service management centers and other network facilities are controlled through an Enterprise-wide Physical Security standard that applies to AT&T companies and its Affiliates. Physical access to AT&T facilities is controlled with the use of an AT&T issued ID Card and one or more devices including Access Card, code and/or Company-issued key. All access devices are approved and validated by an authorizing manager.

Critical Facilities are controlled through alarming and monitoring based on physical security standard criteria and periodic audits are performed to ensure adherence to the requirements of this standard.

9.2.2 Logical Access Control Measures

Logical access controls are based on the principle of "Least Privilege" that strives to ensure that all access to computer resources is restricted or limited to only the commands, data and systems necessary to perform authorized functions. A user who needs access to AT&T's and customers' systems must have a current business requirement, must be allocated a unique identifier (a User ID), and must verify that they are who they claim to be. This access is controlled by:

- Authenticating a claimed identity to the satisfaction of an access permission-granting authority. This authentication entails all individual users being positively and uniquely identified prior to being granted access using authentication mechanisms such as: passwords, personal identification numbers (PIN) and tokens.
- Having systems and network administrators or access providers review and verify with the user's supervisory manager that the user's UserIDs, accounts, and associated command and data access permissions are appropriate for the person's respective job responsibilities. Where a valid business requirement does not exist for the continuance of such privileges, the access is revoked.
- Controlling privileged access to systems and network elements through established security administration controls that restrict access to sensitive information, and network processors, as well as limiting the ability to set, modify or disable system security functions to authorized staff.
- Identifying and recording through audit logging each successful and unsuccessful access attempt, and blocking access when access attempts exceed threshold settings.
- Requiring that all passwords, passphrases, and two factors for user authentication (employee, contractor, business partner, etc.) conform to established rules. The rules for passwords specify: the minimum number and types of characters, uniqueness both from previous user passwords, as well as from user name or dictionary words, avoidance of repeating characters, limitations on password sharing or group use, and requiring passwords to be changed at regular intervals.

9.2.3 Network Element Access Controls

Current industry and AT&T developed tools are utilized for managing the authentication and approval of support personnel to access the large population of AT&T network elements including routers, switches, and wireless access points in the worldwide network. Access is provided to AT&T technical support personnel only on an as-needed basis for individuals with responsibility for network element maintenance and support.

Access to network elements supporting customer services is controlled by:

- Using authenticating servers that validate and verify user access, ensuring that only personnel currently responsible for managing these networks have access.

- Logging all access to the authenticating servers and subsequent devices.
- Flagging repeated failed login attempts and blocking offending accounts.
- Changing passwords or passphrases for routers at regular intervals and complying with AT&T internal requirements for both.
- Reviewing passwords or passphrases on routers, or their management applications, whenever an employee possessing such a password or passphrase terminates employment with AT&T or is re-assigned.
- Using strong authentication when required, specifically two-factor token-based authentication for access to managed network elements.

9.2.4 Access Authorization Control

Only those AT&T personnel with a current business need are authorized with physical and logical access to facilities and systems. All access (physical and logical accesses) is removed upon staff re-assignment or termination of employment. As a control measure, physical and logical accesses are revalidated regularly at defined time intervals to ensure that the staff continues to have a legitimate business requirement for the access.

9.3 Network Perimeter Protection

AT&T external network connections are protected by firewalls that screen incoming and outgoing traffic based on source and destination address, protocol and port, in accordance with AT&T security policy. In particular, Internet connections and Extranets are protected by firewalls and demilitarized zones (DMZs) that block any direct network routing between the Internet and internal AT&T networks.

External customer and partner connections to AT&T networks are protected by access controls (such as access control lists or network based firewalls) that screen incoming and outgoing packets to ensure only authorized traffic is allowed.

9.4 Public-facing Website Protection

Public-facing website platform requires protection at each of the layers: network, operating system, application, and database).

Protection for the Network and Operating system layers includes:

- User management systems maintaining user account access and type of access.
- Monitoring systems and user activities, through event logging along with automated log analysis.
- Web host scanning tools to assess vulnerabilities and configuration issues along with searching for Malware.

- Network scanning to look at each device on the network from the outside-in to determine additional potential vulnerabilities.

Protection for the Application layer including database entails fulfilling the AT&T Security Policy and Requirements for Application Development and Sustainment including Mobile Applications. For example strong authentication and change of passwords regularly are required on our public facing websites where authentication is used. New threats and vulnerabilities are addressed on an ongoing basis to ensure that the public-facing website platform applications are protected against known attacks.

9.5 Intrusion Detection

AT&T employs a combination of internally developed and commercial tools to detect attempts by unauthorized persons to penetrate the AT&T Global Network. AT&T does not monitor individual customer connections for intrusions, except when part of a managed security service. For customers who have subscribed to this component of managed security service, AT&T will promptly notify the customer if it believes that a detected intrusion attempt may impact the customer's service.

9.6 Workstation Security Management

The workstation security policies protect AT&T and customer assets through a series of processes and technologies including verification of personnel workstation accesses, PC anti-virus and anti-spyware protection, Operating System hardening and updates, full disk encryption where permitted by law to protect sensitive information on portable assets, along with a personal firewall intrinsic to remote access software implemented on workstations or portable PCs that remotely connect to the AT&T network.

Securing of the personal computer while in use is further managed by the requirements for power-on passwords, hard drive passwords where possible, and password-protected keyboard or screen-locks that are automatically triggered through inactivity. Management at AT&T is responsible for ensuring compliance with these policies.

AT&T workstations are required to have active, up-to-date "anti-virus" software. AT&T's anti-virus software vendor regularly provides virus signature updates, which are propagated automatically to workstations across the Corporation. Furthermore, security advisories forwarded by the AT&T global security organization provide key AT&T personnel with details on virus warnings, new security patches and newly discovered vulnerabilities. The anti-virus vendor provides updates almost every business day as well as during virus outbreak emergencies; these updates are tested and then propagated automatically throughout the Corporation.

9.7 Security Status Checking and Vulnerability Testing

AT&T conducts regular tests and evaluations to ensure that security controls are maintained and are functioning in accordance with policy. These initiatives include Security Status Checking and Vulnerability Testing. Results from these activities are reviewed and tracked to ensure timely remediation and follow-up actions.

9.7.1 Security Status Checking

- Status Checking is performed on a regular basis to review and verify system security settings, computer resource security settings and status, and users having security administrative authority or system authority.
- Status Checking includes the testing of network elements to ensure the proper level of security patches, and to ensure that only required system processes are active.
- Validation of server compliance to AT&T security policy is conducted on a regular basis on AT&T servers.

9.7.2 Vulnerability Testing and Security Analysis

Vulnerability Testing is performed by authorized personnel to verify whether controls can be bypassed to obtain any unauthorized access.

- Vulnerability tests to evaluate the level of safeguards on network components are performed on a varying frequency based on the risk of compromise, utilizing authorized leading-edge testing tools.
- Vulnerability scans are conducted on networks, computer hosts and applications owned by AT&T at regular intervals as directed by AT&T's security policies using AT&T-developed tools and leading-edge scan tools from recognized commercial software providers.

Network or computer Security Analysis is commonly referred to as intrusion testing, penetration testing, sweeps, profiling, and vulnerability analysis. Performing security analysis of the AT&T networks or computers or applications is the responsibility of AT&T. Performance of security analysis by non-AT&T entities is expressly prohibited unless written approval has been obtained from AT&T global security organization management. See section 9.11 for additional information.

9.7.3 Security Status Reporting

Information regarding the security status of AT&T's infrastructure and services is managed and communicated on a need-to-know basis. Results of security health checking and vulnerability testing are tracked and reported by the security programs responsible for compliance management of those activities. Security status, as well as progress on security initiatives, is combined with threat intelligence gathered through trend analysis and reported to security organization executives.

Security program managers share security status information to ensure alignment of program objectives and prioritization of efforts. This disciplined sharing of security status information and reporting enables AT&T to achieve synergy and cooperation among security teams and appropriate management attention to AT&T's overall security posture.

9.8 Risk Management

AT&T's approach to identifying and mitigating network and application vulnerabilities is formalized in the Risk Management program. When vulnerabilities are identified, they are assessed as to severity, potential impact to AT&T and its customers, and likelihood of occurrence. Plans are developed, implemented and tracked to address vulnerabilities within prescribed timeframes according to security policy. When business needs preclude timely resolution, the risk level is documented and mitigating controls are put in place where practicable.

9.9 Security Advisory Program

AT&T utilizes an internal global program to acquire and distribute security advisories, coupled with review and compliance processes as a follow-up to these advisories. Security advisories predominantly consist of newly identified flaws to established network software, systems and equipment which could potentially allow unauthorized users to bypass access controls and/or gain access to data.

AT&T continually reviews bulletins, alerts and advisories regarding security issues, patches, vulnerabilities, and exploits from vendors and organizations (such as US-CERT) for all AT&T owned and managed components.

The advisory program follow up process oversees that security patches are applied to network systems in a timely manner. Each security advisory is categorized, assigned a severity rating and published by the AT&T global security organization, which in turn, dictates the timeframe within which the vulnerability must be resolved.

9.10 Security Incident Reporting and Management

AT&T uses a consistent, disciplined global process for the identification of security incidents and threats in a timely manner to minimize the loss or compromise of information assets belonging to both AT&T and its customers, and to facilitate incident resolution.

The AT&T global network operation centers maintain 24 x 7 near real-time security monitoring of the AT&T network for investigation, action and response to network security events. AT&T's Threat Management platform and program provides real-time data correlation, situational awareness reporting, active incident investigation and case management, trending analysis, and predictive security alerting.

In the event of a security incident, AT&T identifies the level of the potential impact and will attempt to notify the customer if the customer is at-risk.

Incidents are reported to AT&T's senior management to draw attention to the types of attacks reported by our incident response team as well as other noteworthy incident and vulnerability information.

9.11 Security Compliance Reviews

AT&T conducts regular internal reviews of operations and applications functions for compliance with AT&T Security Policy and Requirements (ASPR). AT&T considers such reviews as essential to evaluating the adherence to the established security procedures worldwide. Results of these reviews are reported to AT&T regional security managers and executive management. Results of routine internal reviews are not typically shared with customers, except as warranted by applicable auditing standards [see section 9.12].

Security reviews may be facilitated or conducted by the Chief Security Office; by a business area sponsor of a product, service, or supplier or partner relationship; or by an operations team responsible for life cycle service management. Business and operations areas are encouraged to perform self-reviews to verify compliance with published security requirements.

An internal review of compliance with security requirements is a comprehensive review of an organization's adherence to regulatory guidelines and internal policies, controls, and procedures, as applicable. Security auditors or assessors evaluate the strength and thoroughness of compliance. Assessors review security policies, user access controls and risk management procedures over the course of a compliance engagement and report the findings to all key stakeholders.

9.12 Internal and External Reviews and Audits

In addition to the security compliance reviews, AT&T conducts regular internal and external reviews to address compliance with regulatory, industry, corporate governance, and privacy requirements. The work-product, results and conclusions from these reviews are proprietary to AT&T and are not disclosed outside of the AT&T corporate family.

External audits and certifications are performed for specific services where business requirements merit third party attestations or compliance evaluation such as SSAE 16/ISAE 3402/SOC1 (formerly SAS 70), SOC 3 (formerly SysTrust), Payment Card Industry (PCI) Data Security Standard (DSS) or similar certifications or audits. AT&T has also undertaken an audit of its enterprise security policies, program and practices, resulting in formal certification to the ISO27001:2005 Information Security Management Standard including the latest certification which covers AT&T Services Inc. and its Affiliates as well as Hosting and Cloud Services. More information is available from your account team on request. The areas for such SOC and PCI audits include Managed Services & Managed Security Services, Hosting IDCs, Application Services and Cloud Services.

AT&T will engage in general security discussions with client executive representatives to address questions or concerns from their customers or the customer's auditors. However, security audits and testing conducted by AT&T customers or their representatives are only permitted under specific terms and conditions, including non-disclosure, and require express written authorization from AT&T concerning the scope and frequency; a fee may be charged as well to cover the cost. In particular, scans and vulnerability tests may only be conducted against systems and devices dedicated to the customer to ensure that such tests do not compromise the services or information of AT&T and its other customers.

9.13 Compliance with Standards and Regulations

AT&T complies with legal and regulatory data protection and privacy controls relevant to its general businesses. AT&T processes and programs are designed to support corporate compliance regulations (e.g., Sarbanes-Oxley), as well as with specific standards applicable to AT&T's commercial activities.

AT&T's Payment Card Industry Merchant Compliance program is comprised of a collection of assessment and remediation initiatives addressing major components associated with security compliance as they relate to the evolving Payment Card Industry Data Security Standard (PCI DSS). This program includes, but is not limited to, privacy masking of sensitive data elements; encryption; Security Enhanced Software Development Life Cycle; secure email; key management; and Application Firewall.

AT&T has a strong commitment to its customers' compliance obligations. In 2008, in its role as a Service Provider for its Managed Services and Managed Security Services portfolios, AT&T became the first carrier listed with the Payment Card Industry to offer a portfolio of business network services evaluated against PCI DSS. Presently, AT&T performs 25 unique assessments in this area. AT&T has successfully completed global certification to the ISO27001:2005 Information Security Management Standard including the latest certification which covers AT&T Services Inc. and its Affiliates as well as Hosting and Cloud Services. More information is available from your account team on request.

AT&T network services are available to support customer compliance with regulations in each applicable country. Examples include the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and security standards as specified through governing bodies such as the European Union. To the extent that AT&T personnel require access to information subject to privacy regulations, such information is used only for the purpose of rendering service to the customer, network management, service assurance, or as the customer has otherwise expressly authorized.

9.14 Change Management

To ensure that the integrity of the security infrastructure is not degraded, AT&T uses documented change management processes to submit, approve, and report change requests. A new change request initiates scheduling of a maintenance activity and approval processing. Change requests must receive the appropriate approvals prior to being performed.

The scope of AT&T’s change management program includes, but is not limited to:

- Installing, removing or modifying software
- Modifying configuration parameters including Operating System (OS) and application security logging and security parameters
- Upgrading to a new release level
- Installing patches or fixes
- Invasive system or process testing
- Changes to application software
- Changes to hardware
- Changes to the network or network elements

9.15 Business Continuity Management

AT&T is the first private sector company to receive certification under the Department of Homeland Security’s Private Sector Preparedness, or PS-Prep, program.

In addition to industry recognition, PS-Prep certification validates that AT&T is able to maintain or recover its own business operations in the face of an emergency or disaster, whether natural, man-made, or cyber in nature. AT&Ts preparedness measures include:

- Documenting and practicing strategies and procedures that reduce risk for people, property, and the business during and following a disaster
- Creating and practicing a comprehensive response, recovery, and restoration process that covers not only network and communications, but also general business operations, and
- Creation and maintenance of an incident command structure that provides strategic and tactical direction, coordination, and management of any emergency operations.

For more information regarding AT&T’s PS-Prep certification or other information regarding AT&T’s Business Continuity Management Program, please contact your Account Representative.

9.16 Network Disaster Recovery

AT&T's Network Disaster Recovery plan has three (3) primary goals:

1. Route non-involved communications traffic around an affected area.
2. Provide the affected area communications access to the rest of the world.
3. Recover the communications service to a normal condition as quickly as possible through restoration and repair.

AT&T through its Network Emergency Management (NEM) plan conducts annual accreditations and testing of its Command and Control, Damage assessment and Strike team recovery processes and capabilities. Quarterly disaster recovery tests are performed annually to review all aspects of emergency planning and response, and leverages investments in technology, equipment, and processes to support AT&T's Network Disaster Recovery capabilities throughout the world.

For more information, please visit http://www.corp.att.com/ndr/ or contact your AT&T Account Representative.

9.17 AT&T Corporate Management Engagement

AT&T management is engaged with the security program. Some of the situations where management in the service lines is engaged:

- Security incidents as they occur
- Progress from security initiatives
- Threat intelligence gathered by trend analysis
- Results of internal and external audits and reviews

In addition, the management chain of command receives consolidated reports on a regular basis outlining the results of the security programs and the key issues for their area of responsibility. These reports are delivered to the senior executives as well as their line management.

Senior executives are required to annually acknowledge their commitment to support corporate compliance. As a part of this requirement, senior executives attest that the areas within their responsibility are in compliance with the AT&T security requirements.

9.18 Strategy of Continuous Improvement

The world of networked computing - especially for today’s mobile, always-connected devices and applications, as well as cloud environments - is fast moving and highly dynamic. As a result, AT&T is continually improving security through active security research and development programs, influencing (via standards organizations) and tracking of industry development, and evaluation of new security technologies and products. New tools and systems are constantly deployed based on a cost/benefit analysis to deliver the most effective security safeguards.

9.19 Personnel Security

The AT&T Human Resources organization has controls in place to ensure that employees are properly screened and are aware of their responsibilities with regard to AT&T and customer assets in accordance with the AT&T Security Policy and Requirements and the AT&T Code of Business Conduct. The operating departments ensure that employees are properly trained and that only such employees perform company or customer related job functions.

The AT&T Supply Chain organization facilitates insertion of Asset Protection background check requirements into AT&T – supplier agreements. This action seeks to ensure that the personnel of suppliers granted physical access to AT&T and customer premises are properly screened and are aware of their responsibilities with regard to AT&T and customer assets.

9.20 Security Awareness and Education

The AT&T global security organization is charged with directing and coordinating security awareness and education across AT&T. The AT&T global security organization maintains an internal security awareness website, an internal awareness newsletter, all-employee and business unit-specific bulletins and communications, job-aids, technology conferences, employee security awareness events and expos, as well as, workshops and security courses to deliver general and targeted security awareness initiatives internally within AT&T. The program uses subject matter experts from the various security groups and disciplines for content development and to deliver webcasts and video productions. In addition, all AT&T personnel are required to annually acknowledge their responsibilities to adhere to AT&T's Code of Business Conduct and AT&T's information security policy.

9.21 AT&T Cyber Security Conference

AT&T Chief Security Office hosts the annual AT&T Cyber Security Conference (http://tawkster.att.com/securityconference) to enable open communications with our enterprise customers and the general security community on latest emerging threats and countermeasures in today's world. The conference showcases AT&T's security leadership, strategy, and advanced technology to further protect business customers utilizing AT&T network and systems. Since 2012 the conference is being held in New York City and keeps expanding with a multi-track agenda and outstanding speakers. Contact your AT&T account team for more information.

9.22 Security Executive Briefings and Roundtables

Security experts from the AT&T Chief Security Office frequently host Security Executive Briefings and Roundtables for AT&T customers, analysts and media to discuss the latest security trends and activities. They share expertise and offer guidance on the security issues they see for very large and dynamic environments – such as AT&T's own – and advise on the best practices in dealing with ever increasing threats in today's world. The executive briefings and roundtables take place at either the AT&T Customer Briefing Centers at various locations or at public venues in major cities, and enjoy excellent participation and feedback from attendees.

9.23 Security Training and Certifications

AT&T encourages its employees to obtain security training and to achieve accreditations and certifications. This training is conducted both within AT&T and through corporate training organizations such as:

- The International Information Systems Security Certification Consortium, Inc. (ISC)2
- Information Systems Security Association (ISSA)

- The SANS Institute
- Vendor and product-specific training and certification, such as, Cisco, Microsoft, Checkpoint and others.

Our large population of security professionals maintains certifications and credentials such as:

- Certified Information System Services Professionals (CISSP)
- Certified Information Systems Auditors (CISA)
- Certified Information Security Management (CISM)
- Certified Ethical Hacker (CEH)
- Global Information Assurance Certification (GIAC)
- RSA Certified Security Professional (CSP)
- Microsoft Certified Professional (MCP)
- Cisco Qualified Professional.

10 AT&T Security Research Center

The AT&T Security Research Center (http://src.att.com) was created within the AT&T Chief Security Office to invent the secure future of communications and computing, and create what may be impossible today and revolutionary for tomorrow. The researchers work on very large scale problems in dynamic areas such as mobility and cellular, cloud computing, networking, and data mining. In particular, they search for ways to leverage the power of the network for new security architectures and mechanisms.

11 AT&T Security Operations Center

The AT&T Security Operations Center (SOC) provides comprehensive security across the world's largest network infrastructure by deploying a pro-active defense-in-depth strategy of continuously including additional layers of security behind the network perimeter. The care and attention AT&T devotes to its own enterprise-wide network infrastructure when delivering critical security services and information can be acquired to protect and manage another organization's network.

The AT&T SOC is a 24x7 centralized command and control facility that includes seasoned expert staff, time-tested methodologies and AT&T Proprietary technology. The SOC can monitor and analyze traffic via AT&T's IP backbone, to provide near real-time and advance notification of different types of security events, and to produce daily, company specific security reports and alerts.

Using a global sensor network, AT&T's SOC supports the detection and mitigation of all security events across multiple devices and device types. The SOC provides correlation and alerting, situational awareness, incident response, along with proactive threat vulnerability analysis. It can manage threats and clean harmful traffic that may result in loss for a business.

12 AT&T Security Roles and Responsibilities

Support for AT&T security requirements and for compliance with the standards is required by all staff and management levels within AT&T.

12.1 Senior Executive

- Senior executives own the responsibility for network and information security within their organizations and are accountable to the AT&T Chief Security Officer.

12.2 Management

- Accountable for protecting assets under their ownership and control.
- Responsible to revoke logical and physical accesses owned by an employee based on his/her job reassignment or termination from employment.
- Responsible for the compliance of their staff with the requirements of the AT&T security policies.
- Responsible for conducting staff logical and physical access revalidation at regular intervals.
- Responsible for developing skills of staff necessary to support the security function.
- Responsible for annual review and acceptance of AT&T Code of Business Conduct with staff.

12.3 Staff

- Comply with AT&T security policies.
- Maintain and execute security status checking processes, security profile/signature upgrades, etc., on systems under their control.
- Validate their personal logical and physical accesses to systems and facilities on a regular basis.
- Comply with confidentiality requirements, customer privacy agreements, government policies where applicable and necessary, and office "clean desk" programs for securing confidential information.
- Comply with the AT&T Code of Business Conduct.

13 Customer Security Responsibilities

AT&T customers are responsible for safeguarding the security of their enterprise, their data, and any connection to the AT&T Global Network from loss, disclosure, unauthorized access or service disruption. The customer is expected to promptly notify AT&T of any actual or suspected security incidents or vulnerabilities relating to AT&T services of which the customer becomes aware. Prompt notification is required if the customer believes that an unauthorized party has obtained access to the customer's user identifications and passwords, personal identification numbers or tokens.

The customer should have a security policy defined and a security program in place to support the policy. The program should address, at a minimum, physical and logical security, and confidentiality of data. The customer should designate a member of its management team to be the owner of its security policy and program. The customer's security obligations include, but are not limited to:

- Responsibility for protecting the customer's confidential information from disclosure.
- Responsibility for the management of customer data, content and transaction information stored on or transmitted over the AT&T Global Network, e.g., backup and restoration of data, erasing data from disk space that the customer controls.
- Responsibility for the selection and use of appropriate services and security features and options to meet the customer's business and security requirements, such as encryption to protect privacy of personal information.
- Responsibility for 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 and managed networked devices and systems.
- For "Client Managed" customers who retain administrative control of their environment or portions thereof, sole responsibility for their own patch management, including the review, assessment, and application of patches. Under these circumstances, the customer assumes all risks due to vulnerability exploitation, including any additional usage charges due to such incidents. AT&T may disconnect a "Client Managed" customer from the network if AT&T finds them to be infected with a virus or other malicious code such that AT&T or its other customers could be placed at risk. If they choose, "Client Managed" customers may upgrade their service level to "AT&T Managed", in which case AT&T network and information security policies and procedures will then apply.
- Responsibility for the protection and physical security of devices and systems on the customer's premises, including preventing unauthorized sensors, sniffers and eavesdropping devices from being installed in the customer's premises.
- Responsibility to ensure no security testing or scanning, etc., sourced by the customer occurs on network or application components outside the responsibility and ownership of the customer.
- Responsibility to ensure that its end users comply with applicable laws and also with the AT&T Acceptable Use Policy (found at http://www.corp.att.com/aup/) in using any service offered by AT&T that is provided over or includes access to the Internet.
- Responsibility for the acts and omissions of the customer's end users of any service obtained from AT&T.

- Responsibility to notify AT&T promptly of any security breaches detected by the customer related to the services provided by AT&T.

Many country laws (for example, in the United States) prohibit unauthorized access to data transmitted over public network or commercial carrier (e.g., Internet) and unsecured transmission lines (e.g., cellular, radio or satellite). However, these open transmission services offer increased opportunity for unauthorized parties to discreetly obtain transmitted data. Consequently, all confidential traffic should be encrypted when transmitted across such networks or lines. Responsibility for encryption of data traffic is solely the responsibility of the customer data owner.

14 Summary

AT&T Inc. is one of the world's largest communications companies and is recognized as the leading provider of IP-based communications services to businesses. AT&T views security as a process, driven by management direction/directives and user awareness, and supported by expert skills and advanced technology. The security policies, programs and initiatives outlined throughout this document are administered by the AT&T Chief Security Office, worldwide.

This document provides an overview of AT&T's security policies and programs and how they are designed to safeguard AT&T's customers and their data while managed by AT&T or in transit on an AT&T network. This document also provides a summary of the customer's security responsibilities to protect their greatest assets, and heightens their awareness of why they should implement security measures.

For further information regarding AT&T, our security programs and services, please visit our website at http://www.att.com or contact your local AT&T account team.

APPENDIX

AT&T Security Products and Services

AT&T offers managed security products and services to its customers, designed to assess and protect their vital network infrastructure. Additionally, through our Security Analysis & Consulting Family of Services, that include Security Device Management (SDM), Security Event & Threat Analysis (SETA), and Security Consulting solutions, AT&T has the flexibility and expertise to custom design solutions to meet customer specific needs. AT&T Managed Security Products and Services include:

Security Analysis and Consulting Solutions range from security strategy development that help align security with business objectives, assessments that help evaluate security posture and meet compliance requirements and technical security assessments from a network and application perspective to keep abreast of the threat environment.

Security Event & Threat Analysis correlates information from multiple customer devices and device types, both on premises and embedded in the AT&T Network. This service provides a broad view of the customer network by correlating alerts from these devices across the entire organization and prioritizes security events based on threat and risk management methodologies. **AT&T**

Security Device Management provides a monitoring and management solution to implement customer security policies on new or existing security hardware and software on premises.

AT&T Firewall and Client Services include network-based, premises-based and personal firewalls, Web Application Firewall technology, and management services designed for maximum performance and business continuity. Proxy Services enhance AT&T Managed Firewall service, delivering fine-grained management and prioritization of browser-based traffic.

Email and Web Security Solutions include **AT&T Secure Network Gateway Service**, an integrated, turnkey security solution allowing customers to bundle AT&T Network-Based Firewall Service, AT&T Secure E-Mail Gateway Service, and AT&T Web Security Service on one convenient contract and bill. The service offers a single pricing schedule with multiple service and term discounts. **AT&T Web Security** offers URL blocking and application filtering of malware for Web traffic with real-time reporting of service results. **AT&T Secure E-Mail Gateway** offers anti-virus, anti-spam, and content filtering services for inbound and outbound e-mail messages, plus archiving and encryption options.

Threat Management services include **AT&T Internet Protect,** a security alerting and notification service offering advanced information regarding potential real-time attacks that are in the early formation stages; and **AT&T DDoS Defense,** a DDoS attack identification and mitigation capability within the AT&T network cloud providing increased protection from malicious traffic before it reaches customer's network.

Intrusion Management Services include **Managed Token Authentication**, for secure access to customer networks and applications through a two-factor authentication service; **Intrusion Prevention Services,** provides in-line network defense by detecting, containing and neutralizing or blocking known and unknown threats on the customer network, including worms, viruses, application threats and intrusion attempts. **Intrusion Detection Services** monitors customers networking infrastructure for potential misuse from internal and external sources.

AT&T Encryption Services provides fully managed standards-based PKI encryption to the PC/Blackberry and e-mail gateway, to individual and shared files and folders, via a web-based mail exchange portal and to electronic end-user statements.

These products and services may not be available in all regions. For more information on these and other products and services, please visit; **http://www.business.att.com/** or contact your AT&T account team.

AT&T Managed Services and Hosting and Cloud Services

AT&T Managed Services take advantage of the security of AT&T's global Internet Protocol/Multi Protocol Label Switching (IP/MPLS) network. MPLS technology enables the creation of feature-rich network-based services coupled with AT&T's management expertise, tools and automation. AT&T's network-based managed services include: AT&T Enhanced Virtual Private Network (EVPN) Service, AT&T Virtual Private Network (AVPN) Service and AT&T Managed Internet Service (MIS).

- **AT&T Virtual Private Network (AT&T VPN) Service** is a network-based IP VPN solution that provides a menu of transport capabilities. It combines the flexibility of IP access and inherent security with the reliability of frame relay and ATM. Customers can build an application-aware VPN to link global locations, enabling efficient transport of voice, data and video via a single connection. This solution supports customer managed routers and AT&T's managed firewall and intrusion detection services.

- **AT&T Enhanced Virtual Private Network (EVPN) Service** provides a fully meshed network that excludes having to configure numerous Permanent Virtual Circuits (PVCs). EVPN service bundles network transport with managed router and managed encryption capabilities. It interoperates with other AT&T security services such as managed firewall, managed authentication, anti-virus scanning, Internet Protect^{SM}, managed intrusion detection, and Private Intranet Protect to provide customers with a complete communications security solution.

- **AT&T Managed Internet Service (MIS)** helps customers consolidate management of their Internet applications with high-speed dedicated access, optimized performance and security. This service provides proactive 24x7 network monitoring, enhanced network security features, and maintenance of the communications links between customer locations and the AT&T network. Customers can select a completely AT&T-managed solution or can choose to self-manage components of their Internet solution.

Hosting and Cloud Services provide a variety of data center-based services that offer tailored or turnkey hosting solutions. The mix-and-match tailored solutions offer IT infrastructure, hardware and/or software components, reliable & secure data center facilities, value-added services (i.e., security, backup and restore, professional services, monitoring, portal/reporting, utility, and disaster recovery), server virtualization, and integrated client networking

AT&T Telepresence Solution® provides a fully managed videoconferencing solution including AT&T-owned equipment, installation, full monitoring and management, remote help desk service and equipment maintenance. Customers also have the option of providing their own equipment from a variety of vendors including Cisco, Polycom and LifeSize. AT&T can provide proactive management of customer-owned equipment or customers can provide their own management. AT&T Telepresence Solution reliability is built around AT&T’s high available and secure Multi-Protocol Label Switching (MPLS) VPN or enhanced VPN service and supports scheduled and reservationless business-to-business meetings.

Users are able to easily schedule and conduct meetings that are encrypted for business and security reasons, share videos and control access to a meeting by blocking additional endpoints from joining an established call. AT&T’s solution allows global companies to have access to AT&T Business Exchange, which allows multiple locations within and between companies to securely connect and collaborate with each other.