AT&T Information & Network Security Customer Reference Guide

January, 2010

Version 4.1

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,

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 management of security and the tools or processes utilized. 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, 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.

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 will, 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, as well as directory publishing and advertising services. AT&T operates one of the world's most advanced and powerful global backbone networks, carrying more than 18.7 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 over 50 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 is the driving force behind groundbreaking communications innovations that transform the way people work, live and play. Comprised of leading technical personnel from the former SBC Laboratories, BellSouth Laboratories and AT&T Laboratories, AT&T Labs today provides technology research and development to the subsidiaries of AT&T. 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 700 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 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 and workstations 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-managed assets and resources from security breaches by monitoring potential security threats, correlating network events, and facilitating compliance with legal and regulatory security requirements.

- Own and manage the AT&T security policies and standards for the 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

AT&T has developed and maintains a comprehensive set of security standards based in part to similar leading industry standards (COBIT, ISO/IEC 27001:2005, etc.). Given the dynamic environment that AT&T supports, the library of AT&T security standards 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 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.

9 AT&T Security Program

9.1 Confidentiality

To ensure confidentiality, information is accessible only to those authorized to access and view it. AT&T has implemented a three-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 customer information especially 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 requiring personnel to commit to a standard confidentiality policy on commencement of their employment, and a Code of Business Conduct that assigns severe penalties to violations of these commitments. AT&T personnel receive periodic training to reinforce the company's confidentiality standards.

AT&T employs information and data destruction and sanitization procedures to ensure that electronic and physical media containing proprietary data and information are physically destroyed or shredded, or properly 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 Privacy organization maintains AT&T's corporate privacy policy. Compliance with legal and regulatory privacy requirements is addressed in section 9.12 "Internal and External Reviews and Audits."

9.2 Access Controls

9.2.1 Physical Access Control

AT&T operates in a highly secured environment where physical access to staff office space, switching centers, global network and service management centers and other network facilities is strictly monitored and controlled. AT&T controls access to these assets by:

- Limiting access to authorized personnel and monitoring physical access to, and movement throughout, AT&T facilities through the use of physical monitoring and intrusion detection systems.
- Screening access through the use of trained security personnel and/or technical means such as automated card access systems and biometric screening systems.
- Conducting periodic in-depth Physical Security surveys and audits of its facilities and locations.

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, recognizing suspicious access attempts as security violations, and blocking access when access attempts exceed threshold settings.
- Requiring that all passwords for user authentication (employee, contractor, business partner, etc.) conform to established rules that 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 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 an authenticating server that validates and verifies user access, ensuring that only personnel currently responsible for managing these networks have access.
- Logging all access to the authenticating server and subsequent devices.
- Flagging repeated failed login attempts and blocking offending accounts.
- Changing passwords for routers at regular intervals and complying with AT&T internal password requirements.
- Reviewing passwords on routers, or their management applications, whenever an employee possessing such a password 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 managers are obligated to remove staff accesses, (physical and logical accesses) upon staff re-assignment or termination of employment. As a control measure, physical and logical accesses are revalidated regularly at defined time intervals. The owner or operator of the network elements or of the facility is obligated to conduct the revalidation of personnel accesses with the staff member's supervising manager 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 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.

9.5 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 propagated automatically throughout the Corporation.

9.6 Payment Card Industry (PCI) Compliance

AT&T is committed to privacy and security compliance in its role as a Merchant of Mobility and other telecommunications services. AT&T's Payment Card Industry Merchant Compliance program is a collection of remediation and assessment initiatives addressing major components of 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 sensitive data elements
- Encryption (data protection)
- Security Enhanced Software Development Life Cycle
- Secure Email
- Key Management
- Application Firewall

The Program also adheres to AT&T security standards as they pertain to security elements addressed during projects and/or assessments.

AT&T also has a strong commitment to its customers' compliance obligations in its role as a Service Provider of services from its Managed Services portfolio. In 2008, AT&T became the first carrier listed with the Payment Card Industry to offer a portfolio of business network services evaluated against the PCI DSS. Information is available from your account team upon request.

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 also includes the testing of network elements to ensure the proper level of security patches, to ensure that only required system processes are active, to ensure the existence and retention of activity logs, and to verify support personnel accesses.
- 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 9.12 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 Process

AT&T utilizes an internal global process 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 security patch and vulnerability announcements from vendors and organizations such as CERT for all AT&T owned and managed components.

The advisory process follow up 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 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 notifies 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 considers reviews of operations and applications functions for compliance to security requirements essential to evaluating the adherence to the established security procedures worldwide. Results of these reviews are reported to regional security managers and executive management. Results of internal reviews are not typically shared with customers.

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.

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 requirements such as corporate governance, Sarbanes-Oxley 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 SAS 70, SysTrust, Payment Card Industry (PCI) Data Security Standard (DSS) or similar certifications or audits. This information is available from the AT&T account team upon request.

AT&T complies with legal and regulatory privacy controls relevant to network services. AT&T network services are available to support customer compliance with regulations in each applicable country such as the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA) in the United States, and security standards as defined through governing bodies such as the European Union. However, most AT&T services do not process or access the customers' personal transactions or information. To the extent that AT&T personnel require access to information subject to privacy regulations, such information is used only for purpose for which it is collected, unless the customer consents to a different use.

AT&T is willing to engage in general security discussions with a customer or with security organizations representing a customer to address customer questions or concerns. However, security audits and tests conducted by AT&T customers or their representatives are only permitted under specific terms and conditions. Generally, such audits are subject to restrictions and approvals, require contractual agreements on scope and frequency, and require creation of non-disclosure agreements. In particular, scans and vulnerability tests can 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 Change Management

To ensure that the integrity of the security infrastructure is not degraded, AT&T uses change management processes to enter, approve, and report change requests. A new change request initiates approval processing and subsequent scheduling of maintenance activity for an ‘approved’ change request.

The scope of change management program includes but is not limited to:

- Installing or removing 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
- Changes to application software
- Changes to hardware

9.14 Business Continuity & Disaster Recovery

AT&T Corporate Business Continuity Planning (CBCP) provides technical consultation and program management expertise to address the business continuity, disaster recovery and managed security needs of both AT&T and its customers. Business Continuity Planning focuses on all aspects of business continuity required to protect business operations: availability, reliability, scalability, recoverability, performance and security. Working closely with internal and external customers, Business Continuity Planning develops a thorough understanding of business needs, applying its knowledge, expertise, and proven methodologies to implement customized solutions.

An integral element of AT&T's business continuity and disaster recovery program is the mandatory process of certifying and assigning assurance levels to critical business operations. The goal of this process is to ensure, through certification, that no critical deficiencies exist.

AT&T networks and services are designed with a level of redundancy and recovery capabilities that enable AT&T to meet contracted Service Level Agreements. Custom solutions with an additional level of redundancy or route diversity can be provided for unique customer needs under specific contractual agreements.

Disasters create chaos, turmoil and heartbreak, but they do not diminish AT&T's commitment to our customers. AT&T recognizes that when a community, town, city, or region is struck by a catastrophic event, the rapid recovery of communications is critical.

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.

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

AT&T conducts several major disaster recovery tests annually at different locations 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.

9.15 AT&T Corporate Management Engagement

AT&T management is engaged on a regular basis by various aspects of the security program and administration on a level and frequency commensurate with the criticality and impact of results of the programs or incidents as they occur. Following is a summary of 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 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 corporate executives are required to annually acknowledge their commitment to support corporate compliance. As a part of this requirement, senior executives attest that they and the areas within their responsibility are in compliance with the AT&T security requirements.

9.16 Strategy of Continuous Improvement

The world of networked computing and application security is fast moving and highly dynamic. As a result, AT&T is continually improving security through active security research and development programs, tracking of industry development, and evaluation of new security technologies and products. New tools are employed based on a cost/benefit analysis. The tools and systems selected are those that deliver effective security safeguards.

9.17 Personnel Security

The AT&T Human Resources and Vendor Management organizations have controls in place to ensure that employees, contractors, and subcontractors are properly screened, authorized to perform their job functions, properly trained, and aware of their responsibilities with regard to AT&T and customer assets.

9.18 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, 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 security policy.

9.19 AT&T Cyber Security Conference

AT&T Chief Security Office hosts the annual AT&T Cyber Security Conference to enable open communications with our enterprise customers and the general security industry community on emerging threats and countermeasures within the security industry. The conference promotes awareness of AT&T's strategy and direction to further protect business customers utilizing AT&T network and systems. Contact your AT&T account team for more information.

9.20 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 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. The following reviews these responsibilities from the most senior management level through to the entry level staff position.

10.1 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.

10.2 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.

10.3 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.

11 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 law 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 covertly accessing 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; ensuring that this protection is in place is the responsibility of the customer data owner.

12 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. Although AT&T does offer some customized services, by the nature of the design of shared infrastructure, AT&T cannot customize common security settings shared by other customers to unique settings for a particular customer. Contact your Account Manager to discuss customizations and alternative AT&T services that can help meet your needs. AT&T Managed Security Products and Services include:

AT&T Internet Protect is a suite of cloud-based security services designed to protect customers' networks and monitor their network traffic. The **AT&T Internet Protect** service is the keystone of the family of services and is a security alerting and notification service that offers advanced information regarding potential real-time attacks that are in the early formation stages.

The **AT&T DDoS Defense** option provides DDoS identification and mitigation within AT&T's backbone providing the customer with increased protection from malicious traffic before it reaches the customer's network. The **AT&T My Internet Protect** option provides customer specific event detection and alert notification. The **AT&T Private Intranet Protect** option provides proactive security alerts, traffic statistics, and reporting from customer's VPNs, including proactive alert notification. Contact your Account Manager to determine the **AT&T Internet Protect** service configuration to best suit your needs.

AT&T's Managed Intrusion Detection Service offers network-based and host-based Intrusion Detection Services.

AT&T Firewall Security Services including network-based, premises-based and personal firewall, Management Services designed for maximum performance and business continuity.

AT&T Endpoint Security Service helps customers overcome two critical Internet security challenges: deploying effective firewall policies and enforcing company security policies related to anti-virus and application use.

AT&T Token Authentication Service provides enhanced security, called two-factor authentication, to protect the customers' network and applications from access by unauthorized users and malicious hackers.

AT&T Encryption Services provide information confidentiality. The capabilities of this service include data file content confidentiality and email confidentiality to help prevent unauthorized parties from accessing critical messages and attachments. Also included is authentication of the e-mail sender, as well as non-repudiation: a validation of the integrity of the e-mail message and its contents that ensures the recipient that the message was not modified.

AT&T's Secure Email Gateway Service incorporates spam filtering, malicious code blocking, content management, email policy enforcement, message archiving, and disaster recovery for both inbound and outbound messages, all delivered through a global network of redundant data centers.

AT&T Vulnerability Scanning Service (VSS) is used to continuously and reliably assess networks for vulnerabilities, and provide timely, automatic reporting to enable effective remediation of any vulnerability or emerging threat before any possible exploitation.

AT&T Consultative and Engineering Security Services provide customized security solutions for businesses through consultative and engineering security services that are available to external customers on a "for fee" basis.

AT&T VPN Tunneling Services (AVTS) offer fully managed solutions that allow customers remote access to their corporate LAN using encryption and client-initiated tunneling technology.

AT&T Network Based IP VPN Remote Access (ANIRA) provides business customers with a single solution for remote access from an end-user's personal computer, or Local Area Network (LAN) to corporate LANs, intranets, and extranet(s), as well as the public Internet.

AT&T Government sector services for government agencies and organizations. An example in the United States is the AT&T Access Certificates for Electronic Service (ACES) program which provides PKI and digital certificates to various Federal government (GSA) agencies in addition to managing the internal digital certificates for AT&T.

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

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 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 Virtual Private Network (AVPN) 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 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 Services provide utility computing services that offer tailored or turnkey 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. A fully managed turnkey solution provides capacity on demand, managed firewall and network Intrusion Detection System (IDS) functionality, proactive alerting and patching, dedicated virtual servers, and total isolation of each client's data in a data center environment.

AT&T TelePresence Solution, a managed videoconferencing service provides AT&T-owned or customer-owned Cisco TelePresence equipment, installation, full monitoring and management, remote help desk service and equipment maintenance. 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.

Users are able to 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 exclusive TelePresence Solution allows global companies to have access to AT&T Business Exchange, which allows multiple locations within and between companies to securely connect to each other.