



# Network Security

customer reference **guide**

Version 2.0

May 17, 2004



# Table of Contents

To the Reader	1
Disclaimer	2
About AT&T	3
The AT&T Global Network	4
<b>Worldwide AT&amp;T Security Organizations</b>	5
Security Organization Mandate	6
Senior Executive Sponsorship	6
Management	7
Staff	7
<b>Security Program</b>	8
Physical Access Control Measures	8
Logical Access Control Measures	8
Access Validation Process	9
Confidentiality	9
Workstation Security Management	10
Security Status Checking and Vulnerability Testing	10
Security Status Checking	10
Vulnerability Testing	10
Security Advisory Process	11
Security Incident Reporting and Management	11
Security Status Reporting	12
Security Compliance Reviews	12
Internal and External Audits	12
Network Perimeter Protection	12
Intrusion Detection	13
Strategy of Continuous Improvement	13
<b>Security Awareness and Education</b>	14
Security Training and Certifications	14
<b>Business Continuity &amp; Disaster Recovery</b>	15
<b>Customer Security Responsibilities</b>	16
<b>Frequently Asked Questions (FAQs)</b>	18

# To the Reader

This document is designed for the use of AT&T customers and potential customers for transport services, managed services, hosting and related telecommunication service.

The document provides:

- An introduction to AT&T and its global security organization.
- An overview of AT&T security policy and program, focusing on the key elements and initiatives in data network security to safeguard AT&T's customers and their data while managed by AT&T or in transit on an AT&T network.
- A summary of the customer's security responsibilities to protect themselves, and
- Answers to frequently asked questions regarding AT&T's security program.

For further information regarding AT&T, visit our web site at <http://www.att.com> or contact your local AT&T sales representative.

# Disclaimer

This document provides only a summary overview of the AT&T security policy and program. The sheer nature of maintaining a high-level security posture dictates that AT&T cannot divulge in-depth details regarding the management of security and the tools/processes utilized. AT&T operates a common infrastructure shared by its customers and, as such, must safeguard customers equally on the shared network platform.

This document is provided as information only. It is not a contractual document and it shall not be construed by any person as giving rise to any representation or warranty of any nature whatsoever or any commitment, obligation or liability on the part of AT&T Corp. or any of its affiliates, or any other person. The contractual obligations between AT&T and its customer are set out exclusively in a written contract with the customer signed by both parties, and nothing in this document adds to, takes away from, amends or otherwise affects that agreement. AT&T reserves the right to alter the policies and procedures described in this document without notice to or consultation with any customer or other person. Any reliance that the reader places on the contents hereof shall be at the reader's sole risk; AT&T makes no representation or warranty whatsoever, whether express or implied, regarding the results of using the security procedures outlined in this document. Furthermore, AT&T customers are themselves responsible for maintaining security policies and programs appropriate to their enterprise.

# About AT&T

The AT&T Corporation is comprised of business and support organizations that provide services and functions to our customers. The following are those business organizations:

**AT&T Business** - AT&T Business is the corporation's business franchise, delivering network services and solutions to more than 4 million customers in the U.S. and around the world. AT&T Business develops and sells services including advanced long distance, Voice over IP, network data and IP services, network-based VPN (Virtual Private Network) service, managed network services, outsourcing, hosting and professional services.

**AT&T Consumer** - AT&T Consumer provides a variety of residential and small business communications services, including domestic and international calling plans, long distance, local voice, local-toll, WorldNet ISP services, Digital Subscriber Line (DSL) broadband access, transaction-based and online services.

**Global Networking Technology Services** - Global Networking Technology Services (GNTS) is responsible for designing, developing, deploying, managing and enhancing the AT&T global networks infrastructure, and for creating the technology and global architecture to achieve AT&T's vision of being the "World's Networking Company."

# 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 offerings. Many AT&T customers are multinationals with locations in multiple global regions. AT&T is responsible for managing this worldwide data network with presence on six continents.

The AT&T global network consists of multiple components, which are converging into a common Multi-Protocol Label Switching (MPLS) network:

- A global Internet Protocol Backbone network
- A circuit switched network
- Frame Relay and ATM private networks
- Internal Business and management networks.

# Worldwide AT&T Security Organizations

AT&T maintains comprehensive global security organizations at corporate and worldwide levels. These organizations are dedicated to the physical and logical security of the AT&T global network and its service offerings, and support a broad range of functions, from Security Policy management to customer-facing security solutions.

The AT&T global security organizations review and assess the company's security control posture to determine whether AT&T is keeping pace with industry security developments and meets regulatory and business requirements. Recommendations are made to the business on the technology solutions and critical skills that are to be developed or acquired to maintain the required security posture.

AT&T is actively participating in several global security organizations such as:

- Computer Emergency Response Team/Coordination Center (CERT/CC)
- Security activities within Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C)
- Forum of International Response and Security Teams (FIRST) Team.

Additionally, AT&T participates in the following government and quasi-government organizations in the United States:

- National Coordinating Center (NCC), which is part of Homeland Security, for Telecommunications
- Network Reliability and Interoperability Council (NRIC)
- National Infrastructure Protection Center (NIPC)
- Information Technology - Information Sharing and Analysis Center (IT-ISAC)
- Network Reliability Steering Committee (NRSC)
- The National Telecommunications and Information Administration (NTIA)
- National Communications System (NCS)
- National Security Telecommunications Advisory Committee (NSTAC)
- InfraGard
- Electronic Crimes Task Force.

## Security Organization Mandate

AT&T considers network security to be a cornerstone of the services that it delivers worldwide. By the security policy mandate of AT&T's CEO, 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 applicable to network elements, systems, applications and workstations owned or managed by AT&T. Execution of the policy is led by the AT&T Security organizations at the corporate and worldwide operational units, whose role is to:

- Own and manage the AT&T security standards and guidelines for the Corporation, and maintain ultimate responsibility for all aspects of network security within the Corporation
- Protect AT&T and AT&T managed assets
- Supply security guidance and strategic direction to the business, worldwide security and operations groups
- Ensure compliance to the network security program in a globally consistent manner
- Ensure that the AT&T security standards are implemented and practiced
- Ensure accountability of senior executives for security compliance in their business or region
- Coordinate a security review program to measure the degree of security compliance
- Maintain awareness of security industry changes and trends
- Develop and manage the global security education program within the corporation
- Deliver security alerts and advisories to the corporate and worldwide service organizations
- Provide security specialist support as required to the operations and security teams
- Monitor and facilitate compliance with legal and regulatory security requirements.

Security compliance is central to our culture and is a condition for employment. Each management and staff employee is aware of his or her responsibility and required to comply on an ongoing basis.

The following section outlines some of the security responsibilities of each AT&T employee:

### Senior Executive Sponsorship

- Senior executive sponsors own the mandate of network security within the organization sponsoring the security program and initiative, and are accountable to the CEO of AT&T.

## Management

- Accountable for protecting assets under their ownership and control
- Responsible to revoke logical and physical accesses owned by an employee on his/her job re-assignment or termination from employment
- Responsible for the compliance of their staff to the requirements of the AT&T security standards
- Responsible for conducting logical and physical access revalidation on 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 Conduct with staff.

## Staff

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

# Security Program

The best network security design and implementation must be continuously managed. AT&T views network security as a process, driven by management and user awareness, and supported by expert skills and advanced technology.

The security program implements the AT&T security policy through a rich set of initiatives, processes and procedures administered by the AT&T security organizations worldwide. These program initiatives are executed on an ongoing basis by each region and are supported by the global network security teams.

The goal of the program is to protect both AT&T and each customer's information and resources, including the protection of each customer from other customers within the AT&T network.

Our security program concentrates on the following internal processes:

## Physical Access Control Measures

AT&T operates in a highly secured environment where physical access to switching centers, global network and service management centers and other network facilities is strictly monitored and managed. AT&T employs many strategies to safeguard these assets and in particular AT&T's Network by:

- Limiting 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/locations.

## Logical Access Control Measures

Logical access controls are based on the principle of "Least Privilege". 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. The following control processes are used to manage the logical access:

- Authentication is the process of proving a claimed identity to the satisfaction of an access permission-granting authority.

All individual users must be positively and uniquely identified prior to granting access. Authentication of the user is achieved utilizing several methods such as: passwords, PINs (personal identification numbers) and tokens.

- The "Least Privilege" principle ensures that all access to computer resources is restricted to only the commands, data and systems necessary to perform the authorized functions.
- Security administration of access control measures restricts access to sensitive information by authorized personnel and system network processors, and limits the ability to set, modify or disable system security functions. Privileged access to systems and network elements is tightly controlled.
- Audit logging provides a record for each successful and unsuccessful access attempt. Suspicious access attempts are recognized as security violations and reported. Repeated failed attempts result in the blocking of access.
- All passwords used for authentication (employee, contractor, business partner, etc.) must conform to established rules that specify minimum number and types of characters, uniqueness from previous user passwords, uniqueness from user name or dictionary words, avoidance of repeated characters, limitations on sharing or group use, etc. The passwords must also be changed at regular intervals.

## Access Validation Process

Only those AT&T personnel with a current business need are authorized 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/operator of the network elements or of the facility is obligated to conduct the revalidation of personnel accesses with their supervising manager to ensure that the staff continues to have a legitimate business requirement for the access.

## Confidentiality

Sensitive customer information related to the provision and administration of AT&T services is accorded the same protections as AT&T proprietary information, including encryption 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 agreement on commencement of their employment.

## Workstation Security Management

The workstation security policies protect AT&T and customer information assets through a series of processes including verification of personnel workstation accesses, PC anti-virus protection, and protection of classified data and portable assets.

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 engages automatically through inactivity. Management at AT&T is responsible for ensuring compliance with these policies.

All 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. Furthermore, security advisories forwarded by the AT&T global security organization provide AT&T personnel with details on virus warnings, new security patches and newly discovered vulnerabilities.

## 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.

### 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 all AT&T servers.

### Vulnerability Testing

- Vulnerability Testing is performed by authorized personnel to verify whether controls can be bypassed to obtain security administrative authority or system authority/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.

- Weekly vulnerability scans are conducted on the worldwide AT&T Global Network components directly facing the Internet.
- Vulnerability scans are also conducted on a regular basis on all other network devices.

## Security Advisory Process

AT&T utilizes an internal global process to acquire and distribute security advisories, coupled with compliance and review processes as a follow-up to these advisories. The advisories originate from industry security organizations, and from equipment and systems suppliers. They predominately 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 like CERT for all managed components. The security integrity and advisory process ensures that security patches are applied to network systems in a timely manner.

Each security advisory is categorized and assigned a severity rating by the AT&T global security organization, which in turn, dictates the timeframe within which the vulnerability must be resolved.

## Security Incident Reporting and Management

AT&T uses a 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 our customers, and to facilitate the 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. Part of our security monitoring program incorporates proactive efforts based on trending and analysis.

Network related security incidents could involve network services provided by AT&T to AT&T entities (wholly owned AT&T, contracted, and partner entities) and AT&T customers. Upon occurrence of a security incident, AT&T identifies the level of the potential impact and notifies customers, if they are at risk, via the customer account representative.

Incidents are reported daily to 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.

## 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. Current status is shared on a cumulative basis with AT&T executives. 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. The disciplined sharing of security status information and reporting enables AT&T to achieve synergy and cooperation among security teams and appropriate management attention on our overall security posture.

## Security Compliance Reviews

AT&T considers security reviews essential to evaluating the adherence to the established security procedures worldwide. Results of these reviews are reported to regional security managers and executive management.

Security reviews are composed of the following elements:

- Review of the local network infrastructure
- Vulnerability scans of the network components and applications under review
- Review of current security processes and documentation
- Analysis of actions and improvement plans, and recommendations for security improvements
- Follow-up on the execution of improvement plans
- Reporting of results to regional and executive management.

## Internal and External Audits

In addition to the security compliance reviews, AT&T conducts regular internal and external audits to address compliance with regulatory requirements such as corporate governance, Sarbanes-Oxley and privacy requirements.

External audits and certifications are also performed for specific services where business requirements merit third party attestations such as SAS 70, SysTrust or similar certifications.

## Network Perimeter Protection

All 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 the security policy. In particular, Internet connections and Extranets are protected by firewalls and DMZs that block any direct network routing between the Internet and internal AT&T networks.

Connections of customer IP networks to AT&T management facilities are protected by access controls (such as ACL's or network based firewalls) that screen incoming and outgoing packets to ensure only authorized traffic.

## Intrusion Detection

AT&T employs a combination of internal and commercial tools to detect any attempts by non-authorized personnel to penetrate AT&T Global Network components. Although AT&T does not monitor individual customer connections for intrusions AT&T will promptly notify the customer via the customer-care representative if it believes that a detected intrusion attempt may impact the customer's service.

## Strategy of Continuous Improvement

The world of network security is fast moving and highly dynamic; 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 cost/benefit analysis; the tools and systems selected are those, which deliver effective security safeguards.

# Security Awareness and Education

The security organization within AT&T Labs is charged with directing and coordinating security awareness and education. The AT&T Security Awareness Program maintains a security awareness website, a quarterly newsletter, all-employee bulletins, technology conferences, workshops, and security course development to deliver general and targeted security awareness initiatives. The program uses subject matter experts from the various security programs and disciplines for content development, and partners with AT&T's education and training organization as well as Business Unit organizations for delivery channels. The security awareness program is reviewed with Security Organization Executives annually to gain concurrence and to ensure commitment of resources.

## Security Training and Certifications

AT&T encourages its employees to achieve security training, accreditation 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) <sup>2</sup>)
- Information Systems Security Association (ISSA)
- The SANS Institute
- Vendor and product specific training and certification, such as Cisco, Microsoft, Checkpoint and others.

# Business Continuity & Disaster Recovery

AT&T Business Continuity & Security Services (BCSS) 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. BCSS focuses on all aspects of business continuity required to protect business operations: availability, reliability, scalability, recoverability, performance and security. Working with the customer, BCSS 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 to meet contracted Service Level Agreements. Custom solutions with additional level of redundancy 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 (NDR) plan has three (3) primary goals:

1. Route non-involved communications traffic around an affected area.
2. Give 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 conducts several major disaster recovery tests annually at different customer locations to review all aspects of emergency planning and response, and is leveraging investments in technology, equipment, and processes to support AT&T's Network Disaster Recovery capabilities throughout the world.

# Customer Security Responsibilities

AT&T customers are responsible to safeguard the security of their enterprise, their data, and the connection to the AT&T Global Network from loss, disclosure, unauthorized access or service disruption. The customer must promptly notify AT&T of any actual or suspected security incidents relating to our services of which it becomes aware (e.g., prompt notification if it 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 to be the owner of its security policy and program. The customer's security obligations include but are not limited to:

- Responsibility for protecting customer's confidential information from disclosure, and 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 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 protection of 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 standards) on any customer provisioned and managed networked devices and systems.
- "Client Managed" customers who retain administrative control of their environment or parts thereof are solely responsible 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 security policies and procedures will then apply.

- Responsibility for physical security of devices and systems on the customer's premises, including preventing unauthorized sensors, sniffers and eavesdropping devices from being installed on customer's premises.
- Responsibility to ensure that its end users comply with applicable law and the AT&T Acceptable Use Policy (found at <http://www.ipservices.att.com/policy.html>) in using any service offered by AT&T that provides access to the Internet.
- Responsibility for the acts and omissions of 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 to discreetly obtain transmitted data. Consequently, all confidential traffic should be encrypted when transmitted across such networks or lines; this is the responsibility of the data owner.

# Frequently Asked Questions (FAQs)

## **1. Can AT&T share its security documentation with a customer?**

Internal processes and documentation are proprietary to the AT&T Corporation and may not be 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 customers. To protect the interests of AT&T's employees, shareholders and customers, AT&T does not provide more specific information regarding its network security programs or procedures. AT&T is always willing to engage in general security discussion with security organizations representing the customer.

## **2. Will AT&T share the results of security reviews and other security inspections performed on the AT&T Global Network with their customers?**

AT&T does not share the results of internal security inspections or reviews, as these are AT&T proprietary information. AT&T will make available for review, under a non-disclosure agreement, results of external certifications and audits such as SAS 70 or SysTrust.

## **3. How is support personnel access authenticated to the large population of AT&T Global Network routers in their worldwide network?**

Current industry tools are utilized for managing the authentication and approval of support personnel to access network routers.

## **4. What security measures are in place for access to the customer premises network equipment?**

Authorized personnel's access to customer premises network equipment is controlled and revalidated on a regular basis. Access is controlled by an authenticating server that validates and verifies user access, ensuring that only personnel currently responsible for managing the customer networks have access. All access to customer premises devices is logged. Repeated

failed login attempts are flagged and result in blocking of the offending accounts.

Passwords for routers are changed at regular intervals and comply with AT&T's internal password standards. Passwords on routers, or their management application, are also reviewed whenever an employee possessing such a password ceases to be employed or has been re-assigned. When strong authentication is required, two-factor token based authentication is available for access to customer's managed elements.

**5. What tools does AT&T use to perform their vulnerability testing? Are these tools provided by reputable scan tools providers?**

Leading-edge scan tools from recognized commercial software providers are used by AT&T for network and host-based scans.

**6. What alternative method do you provide when the network connections to the AT&T Network Management network fail?**

The preferred method for out-of-band access to Customer Premise Equipment (CPE) devices (for example during a network outage) is via secure modems in conjunction with Code Activated Switches (CAS). The available equipment on the client's premises typically determines the level of security for out-of-band access. Managed devices are normally configured to require authentication and authorization (e.g., through TACACS+) even for Out-of-Band access. If network problems prevent access to the TACACS server, the device will revert to its local access password. To access a CPE device out-of-band the user still needs to know the following:

- Dial-up number
- Modem password
- Device password.

For added out-of-band security, clients can opt at additional cost for modem devices capable of token-based or challenge response authentication, with added logging and control capabilities.

**7. What is the approach of AT&T regarding customers initiating security vulnerability testing on the AT&T Global Network?**

Network or computer security analysis is commonly referred to as intrusion testing, sweeps, profiling, and vulnerability analysis. Performing security analysis of the AT&T networks or computers is the responsibility of AT&T. Using external vendors or consultants to perform security analysis is expressly prohibited unless written approval has been obtained from AT&T Security management.

**8. Can AT&T implement unique filtering on common components in the AT&T Global Network?**

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.

AT&T offers a variety of solutions that can help a customer. Basic Managed connectivity services may be enhanced by Managed Security services that provide customer unique filtering with managed firewalls.

**9. What types of certifications do the Security Professionals within AT&T maintain?**

Our security professionals within AT&T maintain certifications and credentials such as:

- Certified Information System Security Professionals (CISSP)
- Certified Information Security Auditors (CISA)
- Certified Information Security Management (CISM)
- System Security Certified Practitioner (SSCP)
- Global Information Assurance Certification (GIAC)
- RSA Certified Security Professional (CSP)
- Microsoft Certified Professional (MCP) and related
- Cisco Qualified Professional and related.

**10. Does AT&T comply with privacy controls that are managed by governments?**

In the US, to the extent that AT&T personnel have access to information subject to privacy regulations, AT&T complies with all legal and regulatory privacy controls like The Health Insurance Portability and Accountability Act (HIPPA) and, Gramm-Leach-Bliley Act (GLBA). However, most AT&T services do not process or access customers' personal transactions or information.

**11. Is AT&T ISO17799/BS7799 certified?**

AT&T's security policies and standards are based on the same criteria as ISO17799 / BS7799 standards. In addition, AT&T regularly reviews its security standards, operating procedures, tools and other protective measures to ensure that high standards of security are observed throughout the company.





Cover art: "Bodiam Castle" – Christopher Plant, AT&T UK  
Copyright 2004 AT&T - All Rights Reserved

[www.att.com](http://www.att.com)