Network Security guide

customer reference

Version 1.1
April 24, 2001

AT&T

Global Network Services

Table of Contents

To the Reader

This document provides:

- An introduction to AT&T Global Network Services (known as AT&T Business Services Global Operations in the United States) and its international security organization.
- An overview of AT&T Global Network Services security policy and program, focussing on the key elements and initiatives of data network security that are implemented to safeguard its commercial customers and their data while traversing the AT&T Global Network.
- A summary of the customers' security responsibilities to protect themselves and a review of frequently asked questions regarding AT&T Global Network Services security program.

For further information regarding AT&T Global Network Services, visit our Web site at **www.att.com/globalnetwork** or contact your local AT&T Global Network Services sales representative.

Disclaimer

This document provides only a summary overview of AT&T Global Network Services security policy and program. The pure nature of maintaining a high-level security posture dictates that AT&T Global Network Services cannot divulge in-depth details regarding the management of security and the tools/processes utilized. AT&T Global Network Services 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 Global Network Services, AT&T Corp. or any of its affiliates, or any other person. The contractual obligations between AT&T Global Network Services 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, derogates from, amends or otherwise affects that agreement. AT&T Global Network Services 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 Global Network Services 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 Global Network Services customers are themselves responsible for maintaining security policies and programs appropriate to their enterprise.

About AT&T Global Network Services

AT&T Global Network Services provides world-class and managed network services to businesses in over 60 countries.

As a global organization that is part of the AT&T Corporate family, AT&T Global Network Services is responsible for managing a worldwide data network with presence on six continents. A large number of our customers are international in nature with locations in multiple global regions.

AT&T Global Network Services operates in the following global regions:

- North America, including Mexico and Canada
- Latin America
- Asia Pacific, including Australia
- Europe, the Middle East, and Africa

Global Security Organization

AT&T Global Network Services considers network security to be a critical cornerstone of the services that it delivers worldwide. Our senior executive sponsor holds ownership of the security mandate; fulfillment of the security obligations is driven by the global security organization and by the operational and security organizations in each of the global regions.

The following is an overview of the AT&T Global Network Services global security organization:

Senior Executive Sponsor

- Owns the mandate of network security within the organization sponsoring the security program and initiative, and accountable to the CEO of AT&T Global Network Services

Business Controls Department

- Coordinates the security review program to measure the degree of security compliance in the global regions

Regional Security Organization

- Ensures that the AT&T Global Network Services security standard is implemented and practised by regional service providers
- Regional senior executives are ultimately accountable for security compliance in their region

Global Network Security Group

- Maintains awareness of security industry changes and trends
- Supplies security guidance and strategic direction to the regional security and operations groups
- Develops and manages the network security policy and the network security standards
- Develops and manages the global security education program within the organization
- Owns the process to deliver security alerts and advisories to the regional security organizations
- Provides security specialist support as required to the regional security teams

AT&T Global Network Services, as a member of the AT&T Corporate family, maintains access to assistance from other AT&T security organizations. The mandate of these AT&T Security organizations includes:

- Responsibility for the protection of AT&T and the AT&T managed assets
- Ownership and management of the AT&T Corporate security standards and guidelines for the Corporation, and ultimate responsibility for all aspects of security within the Corporation

The key elements of the global security organizations including the strategic team, the regional network operators and security specialists meet at regular intervals (at least monthly and annually) to review security statuses, issues, security review results and ongoing initiatives. As well, the current security control posture is reviewed to assess whether AT&T Global Network Services is keeping pace with industry security developments. Recommendations are made to the organization on the next-generation solutions or business-critical skills that are to be developed or acquired.

In addition to the formal security organization, an informal virtual security team exists which consists of each and every employee as security compliance is central to our culture. Each management and staff employee is aware of their responsibility and challenged to deliver on an ongoing basis. The following outlines some of the security responsibilities of each employee at AT&T Global Network Services:

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 elements of the AT&T and AT&T Global Network Services security standards
- Promote the security culture within the organization, and the inclusion of security compliance as an objective on staff annual performance appraisals
- Conduct staff logical and physical access revalidation on regular intervals

Staff

- Responsible to comply with elements within the AT&T and AT&T Global Network Services security standards
- Maintain and execute security health checking processes 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

Security Policy

AT&T Global Network Services, as provider of worldwide network services and as required by the corporate security standards, will endeavor to protect from unauthorized access or disclosure of data residing on or passing through the AT&T Global Network, and will endeavor to protect the network infrastructure from unauthorized access and disruptions of service.

This security policy is applicable to network elements and workstations owned or managed by AT&T Global Network Services.

Security Program

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

The goal of the program is to protect each customer from those not in our customer network community, and to protect each customer from other customers within the customer network community.

The best network security design and implementation must be continuously managed; network security is a process, driven by management and supported by expert skills and advanced technology.

Essentially, the program provides a security posture through its consistent coverage worldwide and its depth of execution in each region, and with the guidance and support of the global security team to administer and coordinate execution of security initiatives.

Our security program concentrates on the following internal processes:

Physical Access Controls

Physical security is of fundamental importance in the protection of physical assets, data processing areas, and computer and network facilities. Inadequate physical access controls can render ineffective the most sophisticated logical access controls.

AT&T Global Network Services exercises physical access controls in its information-processing and network environments and facilities to prevent loss by theft or damage to computing resources, unauthorized disclosure or erasure of information.

Computing and network facilities are maintained in controlled access areas, separate from general office areas. Entry to these areas is restricted to only those authorized personnel with current business needs for access. Each controlled access area has an owner identified for determining those individuals to be granted access. Access to these areas is restricted via computer-controlled badge systems, physical locks or other locking mechanisms.

Logical Access Controls

Logical access controls require users with access to the systems of AT&T Global Network Services to have a current business need, to be allocated a unique identifier (a user ID), and to verify that they are who they claim to be (through a password). The following control processes are used to manage the logical access:

Identify and authenticate users:

- The process to ensure that a unique identifier can be associated with each potential user of a system

Define and protect resources:

- The process to ensure that each resource can be identified, that access to the resource can be allowed at the appropriate levels and that access can be denied for unauthorized users

Systems and security administration:

- The process to ensure that only authorized users can set, modify or disable system security functions

Log access attempts:

- The process to ensure that an audit record can be created for each successful or unsuccessful access attempt

Report access violations:

- The process to ensure that suspicious access attempts are recognized as security violations

At AT&T Global Network Services, our employees' passwords conform to established rules that specify minimum number of characters, uniqueness from previous user passwords, uniqueness from user name, avoidance of repeated characters, etc. The passwords must also be changed at regular intervals.

Access Validation Process

Only those AT&T Global Network Services personnel with a current business need are granted 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 failsafe, physical and logical accesses are revalidated on defined time periods. The owner/operator of the network elements or of the facility is obligated to conduct the revalidation of accesses, held by personnel, with their supervising manager to ensure the staff continue to have a legitimate business need for the access.

Confidentiality

Information managed by AT&T Global Network Services is further protected by requiring personnel to commit to a standard confidentiality agreement on commencing their employment with us.

Workstation Security Management

Information, whether electronic or hardcopy, is a valuable asset and must be protected. Classified information is protected by securing it from access or viewing except by those with a valid business need.

The workstation security process protects AT&T Global Network Services and customer information assets through a series of initiatives including verification of personnel workstation accesses, PC anti-virus protection, and protection of classified data and portable assets.

AT&T Global Network Services employs a "clean desk" policy that requires classified material to be secured in locked cabinets following the end of the workday.

Additionally, portable computing equipment (i.e., laptop computers) must be cabled to fixed furniture during office hours, and securely stored in locked cabinets at the end of the workday. Securing of the personal computer while in use is further managed by the requirements for power-on passwords, hard drive passwords where possible, and a keyboard or screen lock that engages through inactivity. Management at AT&T Global Network Services is responsible for ensuring compliance with these policies.

AT&T Global Network Services workstations are required to have "anti-virus" software active on their personal computers. In addition, our anti-virus software vendor regularly provides virus detection file updates. Furthermore, security advisories forwarded by the internal global security organization provide AT&T Global Network Services personnel with details on virus warnings.

Security Status Checking

Security status checks are regularly conducted to ensure that security controls are maintained in place and are functioning in accordance with plan. These initiatives include *health checking* and *vulnerability scanning*. Results from these activities are reviewed by each region for closure and for any required follow-up actions.

Health checking

- Health checking is performed on a regular basis, involving the review and verification of system security settings, operating system resource security settings and status, and users having security administrative authority or system authority.

- Health checking also includes the verification of network elements to ensure the proper level of security "fixes" is maintained, to ensure only those system processes required are active, to ensure the existence and retention of activity logs, and to verify support personnel accesses.

- The local service providers and security personnel perform security status checking on an ongoing basis. During security reviews, the review team conducts status checking as part of the review process.

Vulnerability scanning

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

- Vulnerability scans to test the level of safeguards on network components are performed on a varying frequency based on the risk of compromise, utilizing authorized leading-edge scanning tools.

- Weekly vulnerability scans are conducted on the worldwide AT&T Global Network directly facing the Internet (i.e., OpenNet).

- Quarterly vulnerability scans are conducted on the portion of the worldwide AT&T Global Network infrastructure which does not directly face the Internet (i.e., the network protected from the Internet via firewalls).

Security Integrity and Advisory Process

The security integrity and advisory process ensures that security fixes are applied to network systems in a timely manner.

Data network systems based on "open" network protocols such as TCP/IP are inherently more vulnerable than legacy protocols such as SNA which have strong security measures built in. TCP/IP, by its nature of facilitating communication of "anyone to anyone," has less security measures embedded in the protocol. Given the increasing sophistication of hacking and electronic compromise techniques, this security environment is very dynamic and undergoing constant change as new vulnerabilities are identified and as countermeasures are devised.

AT&T Global Network Services utilizes a global process to acquire and distribute security advisories, and 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 systems and equipment which could potentially allow unauthorized users to bypass access controls and/or gain access to data.

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

Security Incident Reporting

AT&T Global Network Services utilizes a global process for the identification of security incidents in a timely manner to minimize the loss or compromise of customer assets and facilitate the incident resolution.

Upon occurrence of a security incident, AT&T Global Network Services identifies the level of the potential impact and notifies customers if they are at risk, via the customer account representative.

Security Status Reporting

Regional security organizations of AT&T Global Network Services report status on their security activities, both routine and unique, on a regular basis within the Global Network Security organization.

Security Compliance Reviews

AT&T Global Network Services considers data network security reviews essential to evaluating the adherence to the established security procedures worldwide. Additionally, as the results of these reviews are educational, other regions benefit from the techniques utilized in a particular region to bolster their own security posture, strengthening the global security procedures and posture through the knowledge gained. Results of these reviews are reported to regional and executive management.

Security reviews are composed of the following elements:

- Review of the local network infrastructure
- Vulnerability scans of the network under reviewee's control
- Review of current security processes and documentation
- Analysis of actions and improvement plans based on the review results
- Identification of recommendations for security improvements
- Follow-up on the execution of improvement plans
- Reporting of results to regional and executive management

Business Continuity and Disaster Recovery

Following industry design practices for highly available and reliable networks, the AT&T Global Network infrastructure contains strategic redundancy and the ability to dynamically re-route around failed nodes. In addition, AT&T Global Network Services has the capability to operate and manage the networks from multiple geographic locations.

If a customer identifies that a portion of the AT&T Global Network is vital to one or more of their business processes and requires greater redundancy, then a custom solution for that customer can be designed and developed at the customer's expense.

Intrusion Detection

AT&T Global Network Services employs a combination of tools to perform intrusion detection to determine whether any initiatives by non-authorized personnel to penetrate AT&T Global Network components have been attempted.

If a particular customer is identified to be at risk of an intrusion, AT&T Global Network Services will notify the customer via the customer representative.

Key Competencies and Initiatives

Education and Workshops

AT&T Global Network Services engages in ongoing security education through the resources of the global security organization. Security workshops at the technical level are delivered as required to our service providers and security teams within the global regions.

Strategy of Continuous Improvement

The best network security design and implementation must be continuously managed and improved.

The world of network security is fast moving and dynamic; AT&T Global Network Services is continually improving security through a number of security initiatives and evaluation of new security developments, in addition to maintaining existing programs.

Our tools evaluation process is based on cost/benefit analysis; the tools and systems selected are those that deliver effective security safeguards.

Customer Security Responsibilities

AT&T Global Network Services 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 should promptly notify us 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).

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 the management of customer data 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 needs and security requirements;
- 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 complying with prudent security standards);
- protection of customer's confidential information from disclosure;
- responsibility to ensure that its end users comply with applicable law and the AT&T Acceptable Use Policy (found at www.ipservices.att.com/policy.html) in using any service offered by AT&T Global Network Services that provides access to the Internet or e-mail services; and
- responsibility for the acts and omissions of customer's end users of any Service that it obtains from AT&T Global Network Services.

FAQs
Frequently Asked Questions

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

By the nature of the design of shared infrastructure, AT&T Global Network Services cannot customize common security settings shared by other customers to unique settings for a particular customer.

2. Can AT&T Global Network Services share its security documentation with a customer?

Internal processes and documentation are proprietary to AT&T Global Network Services and may not be disclosed to any organization or entity external to the AT&T Corporate family. Maintaining this information confidential is, in itself, a facet of our security program that protects customers.

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

AT&T Global Network Services does not share the results of any security inspections or reviews as these are AT&T proprietary information.

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

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

5. How are customer networks protected from the AT&T Global Network?

The network access equipment on the customer premises, linking the customer network with the AT&T Global Network, is on a separate network segment from the internal AT&T Global Network Services support network. Only authorized personnel are permitted to access (physically and logically) those traffic segments that contain customer premises routers.

Within AT&T Global Network Services, customer premises routers are accessible only from specified network management hosts, and only by authorized support personnel. Network support personnel access to these management hosts is controlled and revalidated on a regular basis, ensuring that only personnel managing the customer networks have access to these management hosts. Further to this, access to the customer routers from the network management host is controlled by an authenticating server which validates and verifies user accesses. "Telnet" and "SNMP" traffic to the customer router is allowed but only from the Network Management server hosts.

Hence, for AT&T Global Network Services support personnel to access a customer premises router, their only access means is to first logon to the network management host with user ID and password. From this management server host, the authorized user would attempt to Telnet to the customer premises router. The customer premises router would not initially accept the Telnet but would redirect the Telnet logon request to an authenticating server. After entering user ID and password on the authenticating server, the support personnel's access to the router is verified and the Telnet request to the router is approved and logged. If the logon and/or authentication are not approved, then no Telnet session is allowed.

AT&T Global Network Services staff do not have direct access (via "Telnet", "Finger", "Sniff" functions or protocols) to customer premises routers from their desktops. Access is only permitted to defined users from the Network Management host and only after successful signon and verification at the authenticating servers.

Passwords for routers are changed at regular intervals and comply with our internal password standards. Passwords on routers are also changed whenever an employee possessing such a password ceases to be employed or has been re-assigned by AT&T Global Network Services or its agents.

6. What defence does AT&T Global Network Services employ against "denial of service" attacks?

AT&T Global Network Services utilizes a protocol rate limiting process to reduce the effect of many types of "denial of service" attacks. Both host- and network-based intrusion detection tools are utilized within the network.

7. What tools does AT&T Global Network Services use to perform vulnerability scanning? Are these tools provided by reputable scan tools providers?

Leading-edge scan tools from a widely recognized commercial software provider are used by AT&T Global Network Services. We are continuously evaluating alternative tools for performance and additional functions.

8. What is the approach of AT&T Global Network Services 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.

Global Network Services

www.att.com/globalnetwork

04/01