

Public Security Guide

(Final)

**TUNIX keeps your
security up !**

Owner: Leo Willems
Department: Directie
Project: TUN/TUN=Directie

This document has been audited by Ronald Pikkert at 02-02-2008.
The information in this document is valid through: 01-01-2010.

Version: 1.11
Formatted: 14-11-2008
Copyright 2008 TUNIX Internet Security & Training



1. Public Security Guide

1.1 Introduction

This document is designed for TUNIX customers and potential customers for managed services and hosting services. TUNIX appreciates that security and awareness thereof is not a single product or service but a ongoing process and way of thinking. This document illustrates the TUNIX security processes.

The document provides: An introduction to TUNIX and its security organization. An overview of TUNIX's security policy and program, focusing on the key elements and initiatives in data network security to safeguard TUNIX's customers and their data while managed by TUNIX or in transit on a TUNIX network. A summary of the customer's security responsibilities to protect themselves. For further information regarding TUNIX, visit our web site at <http://www.tunix.net> or contact your TUNIX sales representative.



2. Disclaimer

This document provides only a summary overview of the TUNIX security policy and program. The sheer nature of maintaining a high-level security posture dictates that TUNIX cannot divulge in-depth details regarding the management of security and the tools/processes utilized in a public document.

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 TUNIX or any other person. The contractual obligations between TUNIX 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 such an agreement. TUNIX 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; TUNIX makes no representation or warranty whatsoever, whether express or implied, regarding the results of using the security procedures outlined in this document. Furthermore, TUNIX customers are themselves responsible for maintaining security policies and programs appropriate to their enterprise.



3. TUNIX Security Organization

TUNIX is participating in or monitoring several global security organizations such as:

- CERT/CC
- Cert/NL (govcert.nl)
- Security activities within Internet Engineering Task Force (IETF)
- SANS
- The World Wide Web Consortium (W3C)
- Forum of International Response and Security Teams (FIRST) Team.

Security Organization Mandate

TUNIX considers network security to be a cornerstone of the services that it delivers worldwide. By the security policy mandate of TUNIX's management, TUNIX 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 TUNIX. Execution of the policy is led by the TUNIX Security Organization whose role is to:

- Own and manage the TUNIX security standards and guidelines, and maintain ultimate responsibility for all aspects of network security within the company.
- Protect TUNIX and TUNIX managed assets.
- Supply security guidance and strategic direction to the business.
- Ensure compliance to the network security program in a consistent manner.
- Ensure that the TUNIX security standards are implemented and practiced.
- Ensure accountability of senior executives for security compliance.



- Coordinate a security review program to measure the degree of security compliance.
- Maintain awareness of security industry changes and trends.
- Develop and manage the security education program within the company.
- Deliver security alerts and advisories to the service organization.
- 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 TUNIX employee:

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 TUNIX 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 regular review and acceptance of the TUNIX Acceptable Use Policy (code of conduct) with staff.

Staff:

- Comply with the TUNIX 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 TUNIX Acceptable use Policy.



4. Security Program

The best network security design and implementation must be continuously managed. TUNIX 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 TUNIX security policy through a set of initiatives, processes and procedures administered by the TUNIX Security Organization. The goal of the program is to protect both TUNIX and each customer's information and resources. Our security program concentrates on the following internal processes:

Physical Access Control Measures

TUNIX operates in a secured environment where physical access to service management centers is monitored and managed. TUNIX employs many strategies to safeguard these assets and in particular TUNIX's Network by:

- Limiting and monitoring physical access to, and movement throughout, TUNIX facilities through the use of physical monitoring.
- Screening access through the use of security personnel and/or technical means such as automated card access systems.
- Conducting periodic 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 TUNIX's and customers' security systems must have a current business requirement, must be allocated a unique identifier (a special operator ID, not the usual 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.

Access Validation Process

Only those TUNIX personnel with a current business need are authorized physical and logical access to security 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 TUNIX services is accorded the same protections as TUNIX proprietary information, including encryption when stored or transmitted on untrusted networks.

Customer Information managed by TUNIX is further protected by requiring personnel to commit to a standard confidentiality agreement on commencement of their employment or thereafter.

Workstation Security Management

The workstation security policies protect TUNIX 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 and hard drive passwords where possible, and password-protected keyboard or screen-locks that engages automatically through inactivity. Management at TUNIX is responsible for ensuring compliance with these policies.

All TUNIX workstations are required to have active, up-to-date *anti-virus* software. TUNIX's anti-virus software vendor regularly provides virus signature updates, which are propagated automatically to workstations. Furthermore, security advisories forwarded by the TUNIX Security



Organization provide TUNIX personnel with details on virus warnings, new security patches and newly discovered vulnerabilities.

Security Status Checking and Vulnerability Testing

TUNIX 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 Checking.

Security Advisory Process

TUNIX utilizes an internal process to acquire and distribute security advisories, coupled with compliance and review processes as a followup 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. TUNIX 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 TUNIX Security Organization, which in turn, dictates the timeframe within which the vulnerability must be resolved.

Security Incident Reporting and Management

TUNIX uses a 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 TUNIX and our customers, and to facilitate the incident resolution.

The TUNIX network operation centers maintain 24 x 7 real-time security monitoring of the TUNIX and customers networks for investigation, action and response to 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 TUNIX to TUNIX entities (wholly owned TUNIX, contracted, and partner entities) and TUNIX customers. Upon occurrence of a security incident, TUNIX identifies the level of the potential impact and notifies customers if they are at risk. 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 TUNIX'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 TUNIX executives. Security status, as well as progress on security initiatives, is reported to the Security Officer.



Security Compliance Reviews

TUNIX considers security reviews essential to evaluating the adherence to the established security procedures. Results of these reviews are reported to 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 executive management.

Network Perimeter Protection

All TUNIX 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 TUNIX networks. Connections of customer IP networks to TUNIX management facilities are protected by access controls (such as ACL's and firewalls) that screen incoming and outgoing packets to ensure only authorized traffic.

Intrusion Detection

TUNIX employs tools to detect any attempts by non-authorized personnel to penetrate TUNIX network components. TUNIX will promptly notify customers via the network operation center 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; TUNIX 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.



5. Security Awareness and Education

The TUNIX Security Organization is charged with directing and coordinating security awareness and education. The TUNIX bi-monthly meeting and newsletter have a dedicated security paragraph. The program uses subject matter experts from the various security programs and disciplines for content development from TUNIX's education and training organization.

Security Training and Certifications

TUNIX encourages its employees to achieve security training, accreditation and certifications. This training is conducted both within TUNIX and through company training organizations such as:

- The International Information Systems Security Certification Consortium, Inc. ((ISC) 2)
- The SANS Institute
- Vendor and product specific training and certification, such as Cisco, Microsoft, Tippingpoint, F5 and others.



6. Business Continuity & Disaster Recovery

TUNIX provides technical consultation and program management expertise to address the network part of business continuity, disaster recovery and managed security needs of both TUNIX and its customers. TUNIX focuses on all aspects of business continuity required to protect business operations: availability, reliability, scalability, recoverability, performance and security with regard to networking. Working with the customer, TUNIX develops a thorough understanding of business needs, applying its knowledge, expertise, and proven methodologies to implement customized solutions.

TUNIX 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 TUNIX's commitment to our customers. TUNIX recognizes that when a customer's business is struck by a catastrophic event, the rapid recovery of communications is critical.



7. Customer Security Responsibilities

TUNIX customers are responsible to safeguard the security of their enterprise, their data, and the connection to the TUNIX network from loss, disclosure, unauthorized access or service disruption. The customer must promptly notify TUNIX 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 TUNIX 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.
- 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 companies Acceptable Use Policy (e.g. at <http://www.cbpweb.nl>)
- Responsibility for the acts and omissions of customer's end users of any Service obtained from TUNIX. Responsibility to notify TUNIX promptly of any security breaches detected by the customer related to the services provided by TUNIX

Many country laws 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.

