LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
CO-OPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

ICT FIREWALL POLICY

20 February 2012

Version Control

Version	Date	Author(s)	Details
Draft 1.1	**22/11/2011**	**Sam Mantlaka**	**New policy**
Draft 1.1	**20/02/2012**	**Sam Mantlaka**	**Incorporation of inputs after circulation to all staff members**
Final	**27/02/2012**		**Adopted by Labour Management Forum**

Contents

1. Introduction

Firewalls are an essential component of any organization information systems security infrastructure. Firewalls are defined as security systems that control and restrict both Internet connectivity and Internet services. Firewalls establish a parameter where access controls are enforced

2. Terms and definition

Authentication: a systematic method of confirming the identity of an individual or system

Database: is a collection of information that is organized so that it can easily be accessed, managed and updated

Data: Information that has been translated into a form that is more convenient to move or process

Coghsta: Cooperative Governance, Human Settlement and Traditional Affairs

Exploitation: The process of obtaining intelligence information from any source and taking advantage of it

FTP (File Transfer Protocol): a standard Internet protocol that allows users to transfer files from one computer to another over a network

HTTP (Hypertext Transfer Protocol): set of rules for transferring files (text, graphic images, sound, video and other multimedia files) on the World Wide Web

ICT: Information Communication Technology

Inbound Traffic: Traffic coming into Local Area Network

IT Security Requirements: describe functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an IT system.

Network security: refers to any activities designed to protect network, especially the usability, reliability, integrity and safety of the network and data

Network Security Architecture: a subset of network architecture specifically addressing network security.

Outbound Traffic: Traffic going out of Local Area Network

Perimeter Firewall: a Firewall installed between a private network and public networks, such as the Internet

Proxy server: is a computer that acts as a gateway between a local network and a large –scale network such as the Internet. Proxy servers provide increased performance and security

Remote Access Points (RAPs): provide secure always-on network access to corporate enterprise resources from remote locations.

Security device: Hardware or software that provides security services.

Security Functionality: are the security-related features or functions employed within an information system or the infrastructure supporting the system.

Service: is a long-running executable that performs specific functions and which is designed not to require user intervention

VPN (Virtual Private Network: A virtual private network (VPN) is a network that uses a public telecommunication infrastructure and their technology such as the Internet, to provide remote offices or individual users with secure access to their organization's network

TCP/IP: a set of protocols (including TCP) developed for the internet in the 1970s to get data from one network device to another

Threat: is a possible danger that might exploit a vulnerability to breach security and thus cause possible har

Traffic: is data in a network. In computer networks, the data is encapsulated in packets

Vulnerability: is a weakness which allows an attacker to reduce a system's information assurance

3. Legal Framework

5.1 ISO 17799

5.2 Information Security Forum (Code of good practice for Information Security)

5.3 Minimum Information Security Standards

5.4 Limpopo Information Security Policy

5.5 Protection of Information Act

5.6 International Standard for Risk Assessment

5.7 COBIT Audit Framework

5.8 Departmental ICT Password Management Policy

4. Purpose

The purpose of this ICT Firewall Policy is to allow or block a network or Internet devices and services sending traffic or receiving traffic over a network. To define standards for provisioning security devices owned and/or operated by Coghsta. To prevent exploitation of insecure services, restrict inbound/outbound traffic from unregistered devices, control inbound/outbound access to/from specific services or devices and monitor traffic volumes.

5. Scope

This policy defines the essential rules regarding the management and maintenance of Firewall at Coghsta and it applies to all users that use computers and the network of Coghsta.

6. Policy statement

Coghsta operates perimeter firewalls between the Internet and the department network in order to establish a security environment for the department's Information Technology resources. Coghsta perimeter firewalls are a key component of the overall department's Network Security Architecture. This ICT Firewall policy governs how the perimeter Firewalls will filter Internet traffic to mitigate risks and possible losses associated with security threats to the networks and information systems.

7. Requirements

7.1 The Firewall system shall control all traffic entering and leaving the Coghsta Internal network.

7.2 Coghsta Firewall shall block all incoming and outgoing traffic by default.

7.3 Only authorized incoming and outgoing traffic shall be allowed to pass through Coghsta Firewall.

7.4 Traffic with invalid source or destination addresses shall always be blocked.

7.5 Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid "external" address) shall be blocked at the network perimeter.

7.6 Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) shall be blocked at the network perimeter.

7.7 Outbound traffic with invalid source addresses shall be blocked.

7.8 Incoming traffic with a destination address of the firewall itself shall be blocked unless the firewall is offering services for incoming traffic that require direct connections.

7.9 Traffic from outside the network containing broadcast addresses that are directed to inside the network shall be blocked.

8 Operations

8.1 Only Firewall system administrators shall be permitted to logon to Firewall hosts. Access to Firewall hosts shall be tightly controlled. Only Firewall system administrators are allowed to have user accounts on Firewall hosts. Firewall system administrators shall have personal accounts; i.e. no group logins are allowed.

8.2 All changes to Firewall access rules shall be made through a single approved interface. The Firewall shall have a trusted path for its management e.g. a physically secure dedicated management process with a password-based identification and authentication system.

8.3 Only personnel with the appropriate authorisation shall make changes to the Firewall access rules, software, hardware or configuration. All changes shall be as a result of a request recorded in an ICT Change Management System although emergency modifications can be requested by phone, with a follow up email and change request. Only authorised personnel must be able to implement the changes and an audit log must be retained as per the Departmental ICT Change Management Policy.

8.4 Logging and audit facilities provided by the Firewall system shall be fully utilised. All significant traffic through the Firewall shall be logged. The Firewall shall provide sufficient audit capacity to detect breaches of the Firewall's security and attempted network intrusions. Firewall System Administrators shall examine logs on a regular basis and also set up mechanisms to respond to alarms.

8.5 Logs shall be kept for a minimum period of one year, before the overriding function overrides the previous logs.

9. Configuration

9.1 The perimeter Firewall system shall be configured to deny any service unless it is expressly permitted. If there are no rules defined for the department network address, then traffic to or from that address shall be denied. Access to the department network shall be blocked during the start-up procedure of the Firewall.

9.2 The Firewall operating system shall be configured for maximum security. The underlying operating system of Firewall hosts shall be configured for maximum security, including the disabling of any unused services.

9.3 The Firewall product suite shall reside on dedicated hardware. Applications that could interfere with, and thus compromise, the security and effectiveness of the Firewall products, shall not be allowed to run on the host machine.

9.4 The initial build and configuration of the Firewall shall be fully documented. This provides a baseline description of the Firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state.

9.5 Security shall not be compromised by the failure of any Firewall component. If any component of the Firewall fails, the default response will be to immediately prevent any further access, both outbound as well as inbound. A Firewall component is any piece of hardware or software that is an integral part of the Firewall system. A hardware failure occurs when equipment malfunctions or is switched off. A software failure can occur for many reasons e.g. bad maintenance of the rules database on the Firewall or software which is incorrectly installed or upgraded.

9.6 There shall be regular reviews to validate the Firewall system meets the needs of the business regarding information security. The configuration of the Firewalls shall be regularly checked to ensure they still match the business requirements regarding the security. It may be necessary to implement separate Firewall modules to protect against the vulnerabilities of certain services. An example would be a package to scan email for viruses or other malicious software. The Firewall must also be regularly tested for vulnerabilities. Applications on internal hosts that handle incoming services will need to be checked for known vulnerabilities.

10. Audit and compliance

10.1 Regular testing of the Firewall shall be carried out. The Firewall shall be regularly tested for;

- Configuration errors that may represent a weakness that can be exploited by those with hostile intent.
- Consistency of the Firewall rule set.
- Secure base system implementation.

10.2 The Firewall system shall have an alarm capability and supporting procedures. When an agreed specified event occurs, an alarm shall be sent to the security team. Documented procedures shall exist to permit an efficient response to such Firewall security alarms and incidents. In the event that the Firewall itself is the subject of malicious attempts to penetrate it and the Firewall

has the capability, delivery of services should be terminated rather than permit uncontrolled access to the department network.

10.3 There shall be an active auditing/logging regime to permit analysis of Firewall activity both during and after a security event. An audit trail is vital in determining if there are attempts to circumvent the Firewall security. Audit trails must be protected against loss or unauthorized modification. The Firewall system must be able to provide logging of specific (or all) traffic when suspicious activity is detected.

11. Responsibilities

GITO will be the sole responsible entity for putting in place firewalls and the management thereof. The monitoring will be done by GITO and reported to Risk and Security management if any breach attempts are detected.

12. Change control

With any Firewall it is very important to have change control. When rules are introduced there should be a well-defined method for documenting these and in the case of temporary rules, the removal date for the rule should be added in a comment field. The only way of checking if the Firewall is actually enforcing the agreed policy is to either verify it with an Intrusion Detection System, or to do a manual verification using a penetration test or a Firewall review by third party.

13. Monitor stability

A Firewall is like any other infrastructure component and should be managed as such. It should be monitored for availability to ensure maximum uptime. If a Firewall isn't stable people will find ways of avoiding the Firewall that leads to a low level of security.

14. Administration of the Policy

GITO is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

15. Consequences for Non-Compliance

Non-compliance of this policy may lead to disciplinary actions, legal liability as well as dismissal.

16. Policy Review

This policy shall be reviewed annually.

17. Effective Date

This policy comes into effect from the date of approval.

COMPILED BY

06/03/2012

SENIOR MANAGER: **DATE**

INFORMATION TECHNOLOGY

ACKNOWLEDGED BY:

Adoption and approval of ICT firewall policy is recommended.

06/03/2012.

GENERAL MANAGER: **DATE**

GOVERNMENT INFORMATION TECHNOLOGY OFFICE

ACKNOWLEDGED BY:

Supported for approval.

08/03/2012.

SENIOR GENERAL MANAGER: **DATE**

SHARED SERVICES

ADOPTED /NOT ADOPTED:

Adopted

HEAD OF DEPARTMENT **DATE** 28/03/2012

APPROVED/~~NOT APPRO~~VED

HONOURABLE MEC **DATE** 28/03/12