LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

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

IP Address Management Policy

Version: 1

Version Control

Version	Date	Author(s)	Details
1.0	21/06/2012	Samuel Mantlaka	Original draft IP Address Management Policy
2.0 Final	12/03/2014	Samuel Mantlaka	Adopted by Labour Management Forum

Table of Contents

Version Control 2

I. Acronyms and Abbreviations 4

II. Clarification of Terms 5

1. Preamble 8

2. Purpose and objectives 8

3. Scope of Allocation 8

4. Legal Framework 8

5. Administration of the policy 9

6. Policy Contents 9

7. Default 11

8. Inception Date 11

9. Policy Review 11

10. Enquiries 11

I. Acronyms and Abbreviations

COBIT	Control Objectives for Information Technology
CoGHSTA	Co-operative Governance, Human Settlements and Traditional Affairs
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ICT	Information Communication Technology
ISO	International Standards Organization
IP	Internet Protocol
IETF	Internet Engineering Task Force
MAC	Media Access Control
RFC	Request for Comment
SITA	State information Technology Agency
VLAN	Virtual Local Area Network
VOIP	Voice over Internet Protocol

II. Clarification of Terms

Active Directory

Electronic database that stores all network information about a Microsoft network infrastructure

Appliance Device

An electronic device that performs a special function on a network, the software is encoded in the device itself to form a single computer system.

COBIT

ICT Governance Framework

DHCP

Protocol for issuing hosts devices with IP addresses on a network.

DNS

Protocol in a network for resolving hostnames to IP addresses

Default Gateway: Network device that routes network traffic from one network to the other

Hostname

Name assigned to devices on a network that uniquely identifies the device.

IP

Network protocol used for routing network traffic from one location to another on network

IP Address

Network address used to uniquely identify device on a network

MAC address

A unique address hard coded on a network interface card on a network device.

Network

Is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information

Network interface card

A device attached to a network device used to connect the network device to the network

Private IP Address

IP addresses that are not visible to the Internet, they are used by organization to assign host within an organization private network

RFC

A memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems

Router

Network device that routes network traffic from one network to the other

Resource Record

Record in a DNS server that maps network device name in to an IP address

Subnet

A small logical portion of a network that is assigned a network ID

Static IP address

An IP address that is assigned manually

Three Factor Authentications

An approach to security authentication, which requires that the user of a system provide more than one form of verification in order to prove their identity and allow access to the system

VLAN

A technology used to segment a network into smaller manageable pieces for performance and security purposes.

VOIP

Protocol used to transmit voice over data networks.

1. Preamble

IP Address management requires proper allocation and administration of IP addresses throughout an organization. It ensures users and systems are allocated with consistent and secure access to a network, reducing the risk of assigning conflicting addresses, thereby affecting availability of the network.

2. Purpose and objectives

The purpose of this policy is to establish standards and directives for the allocation, administration and usage of IP Addresses throughout the CoGHSTA network infrastructure.

3. Scope of Application

This policy is applicable to those responsible for the management of CoGHSTA ICT Network Infrastructure and Security including service providers. The policy further applies to all officials and other stakeholders. This policy covers IP Address Inventorying, Dynamic Address Service Management as well as IP Name Service Management.

4. Legal Framework

The following publications govern the execution of this policy and were taken into consideration during the drafting of this policy.

4.1. CoGHSTA ICT Security Policy
4.2. SITA Act 88 of 1998
4.3. ISO 17799
4.4. Information Security Forum (Code of good practice for Information Security)
4.5. Minimum Information Security Standards
4.6. Limpopo Information Security Policy
4.7. Protection of Personal Information Act 4 of 2013
4.8. International Standard for Risk Assessment
4.9. COBIT Framework

5. Administration of the policy

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

6. Policy Contents

All ICT network devices, computer equipment and systems approved by GITO management must be allocated an approved IP address to connect to CoGHSTA network infrastructure. The allocation and management of IP addresses must conform to the standards and directives laid throughout this policy and other CoGHSTA related policies.

6a General

6a.1 Only Private IP addresses that conform to RFC (1918) standard allocated by SITA and Private IP addresses approved by GITO management should be used to allocate approved devices to connect to network.

6a.2 All IP address information should be documented on a spread sheet and must include, but not limited to the following:

6a.2.1 Subnet information

6a.2.2 VLAN assignments

6a.2.3 Device Static IP assignments

6a.2.4 Device related information

6a.2.5 VOIP Ranges

6a.2.6 DHCP Scopes

6a.2.7 DHCP exclusions

6a.2.8 DHCP reservations

6a.2.9 DHCP pools

6b Configurations

6b.1 DHCP Server

6b.1.1 DHCP server should be configured with IP address scopes, pools, exclusions, and reservations in order to assign IP addresses as required.

6b.1.2 All sites separated by routers should have own DHCP server or relay agent installed.

6b.1.2 DHCP servers should be authorized through Microsoft Active Directory.

6b.1.3 DHCP servers should be capable of dynamically updating DNS server resource records for every assigned IP address.

6b.1.4 DHCP sever options should be configured with the Domain Name, Default gateway and DNS server IP address.

6b2 DNS Servers

6b2.1 DNS servers should be configured on the network and must allow dynamic updates from DHCP servers.

6c IP Address Allocation

6c.1 All CoGHSTA Servers, Routers, Switches, Security device and other appliance devices shall be assigned with manual IP addresses.

6c.2 Client computers including desktops, laptops, and smart phones shall be assigned dynamic addresses through DHCP servers.

6d Network Access Control

6d.1 Network access shall be controlled through Network Access Control system and no device that has not registered its MAC address shall be allowed to connect to the network.

6d.2 Devices that have outdated software patches and Anti-Virus software shall be redirected to a remediation server before allowed connecting to the network.

6d.3 Wireless Devices shall be authenticated with three factor authentication before access to CoGHSTA network is provided.

6e Administration and Change Management

6e.1 ICT Change management form should be completed and approved by GITO management prior to any IP address changes be made on the network except for DHCP assigned IP addresses.

6e.2 Excel spread sheet documentation should be updated to reflect changes made on any system on the network.

6e.3 the spread sheet documentation should be stored on a central shared folder accessible to only authorized GITO personnel.

6f Fail-Over and Availability

6f.1 IP address database and DHCP server database must be backed up as part of the normal CoGHSTA backup processes.

6f.2 DHCP servers should be configured in a fail-over configuration to provide redundancy in an event one DHCP server fails.

6g Tracking, Monitoring and Reporting

6g.1 An electronic system should also be implemented and be used to monitor and manage IP addresses throughout the CoGHSTA network.

7. Default

Non-compliance of this policy shall constitute violation of the policy and shall be treated in terms of the Departmental Disciplinary Code and Procedure Policy.

8. Adoption of the Policy

This policy shall be considered and adopted by the Labour Management Forum.

9. Inception Date

This policy comes into effect from the date of approval by Member of Executive Council.

10. Policy Review

This policy shall be reviewed bi-annually.

11. Enquiries

Enquiries about the policy should be directed to the Government Information Technology Office

Document Title	**IP Address Management Policy**
Compiled by :	**Government Information Technology Office** **Senior Manager** **(ICT Infrastructure and Systems)** 19/03/2014 **Date**
Acknowledge by :	 **General Manager (GITO)** 20/03/2014 **Date**
Recommended by:	 **Senior General Manager** **(Corporate Services)** 01/04/14 **Date**
Adopted by :	p **Head of Department** 03/04/2014 **Date**
Approved by :	 **Member of the Executive Council** 10/04/2014 **Date**