**Network Security Policy**

**Security Classification: Restricted**

**Document Ref. ISMS19005**

**Version: 1.0**

**Draft 1**

**Document Author: Cybersecurity Unit**

**Document Owner: NCS / TMP**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Change Number** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document Review**

|  |
| --- |
| **Date of Next Scheduled Review** |
|  |

Distribution

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

**Contents**

[1 Introduction 5](#_Toc379819270)

[1.1 Risks Addressed 5](#_Toc379819271)

[1.2 Scope 5](#_Toc379819272)

[1.3 Related Documents 5](#_Toc379819273)

[1.4 Purpose 5](#_Toc379819274)

[2 Network Security Policy 6](#_Toc379819275)

[2.1 Network Security Design 6](#_Toc379819276)

[2.1.1 Requirements 6](#_Toc379819277)

[2.1.2 Defence in Depth 7](#_Toc379819278)

[2.1.3 Network Segregation 7](#_Toc379819279)

[2.1.4 Perimeter Security 7](#_Toc379819280)

[2.1.5 Public Networks 8](#_Toc379819281)

[2.1.6 Wireless Networks 8](#_Toc379819282)

[2.1.7 Physical Security 8](#_Toc379819283)

[2.1.8 Remote Access 9](#_Toc379819284)

[2.1.9 Network Intrusion Detection 9](#_Toc379819285)

[2.1.10 Network Security Standards 9](#_Toc379819286)

[2.2 Network Security Management 10](#_Toc379819287)

[2.2.1 Roles and Responsibilities 10](#_Toc379819288)

[2.2.2 Logging and Monitoring 11](#_Toc379819289)

[2.2.3 Network Changes 11](#_Toc379819290)

[2.2.4 Network Security Incidents 12](#_Toc379819291)

[3 Conclusion 13](#_Toc379819292)

# Introduction

## Risks Addressed

This document describes a control that was identified in [ISMS06004 Information Security Risk Treatment Plan](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\06.%20Planning\ISMS06004%20Information%20Security%20Risk%20Treatment%20Plan.doc) to address the following risks:

|  |  |
| --- | --- |
| **Reference** | **Description of Risk** |
|  |  |
|  |  |
|  |  |

## Scope

This control applies to all systems, people and processes that constitute the organisation’s information systems, including board members, directors, employees, suppliers and other third parties who have access to PMO systems.

## Related Documents

The following policies and procedures are relevant to this document:

* [ISMS12002 Mobile Computing Policy](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A6.%20Organisation%20of%20information%20security\ISMS12002%20Mobile%20Computing%20Policy.doc)
* [ISMS12003 Teleworking Policy](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A6.%20Organisation%20of%20information%20security\ISMS12003%20Teleworking%20Policy.doc)
* [ISMS12004 Bring Your Own Device Policy](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A6.%20Organisation%20of%20information%20security\ISMS12004%20Bring%20Your%20Own%20Device%20Policy.doc)
* [ISMS18004 Change Management Policy](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18004%20Change%20Management%20Policy.doc)
* [ISMS18008 Software Policy](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18008%20Software%20Policy.doc)
* [ISMS18010 Anti-Malware Policy](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18010%20Anti-Malware%20Policy.doc)

## Purpose

This document sets out the organisation’s policy on how it will design, manage, and support computer networks. Its intended audience is IT and information security management and staff who will implement and maintain the organisation’s defences.

# Network Security Policy

The use of networks is an essential part of the day-to-day business of the PMO. Networks not only connect many of the components of business processes together internally, but they also link the organisation with other government agencies (OGAs), stakeholders, and the outside world.

The PMO networks have evolved over time, to become the circulatory system of the Nigeria Customs Service, transporting information to where it needs to go and enabling trade to be carried out effectively.

But the fact that so much information runs through our networks makes them a target for those who would try to steal that information and disrupt our services. Therefore, these networks need to be protected to ensure that the confidentiality, integrity, and availability of our vital information is assured at all times.

The effective protection of our networks requires that we adopt best practices in information security covering the design, implementation, operation, and management of them and that we ensure that everyone involved follows these practices.

This policy sets out the PMO rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure.

## Network Security Design

The design of networks is a complicated process requiring a good knowledge of network principles and technology. Each design is likely to be different, based on a specific set of requirements that are established early in the process. This policy does not attempt to specify how individual networks should be designed and built but provides guidance for the standard building blocks that should be used.

### Requirements

A network design should be based on a clear definition of requirements which should include the following security-related factors:

* The classification of the information to be carried across the network and accessed through it.
* A risk assessment of the potential threats to the network, taking into account any inherent vulnerabilities.
* The level of trust between the different components or organisations that will be connected.
* The hours of availability and degree of resilience required from the network.
* The geographical spread of the network
* The security controls in place at locations from which the network will be accessed.
* Security capabilities of existing computers or devices that will be used for access.
* The list of components that make up the network.

Requirements should be documented and agreed before design work starts.

### Defence in Depth

A “Defence in Depth” approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network. For example, network firewalls should be supplemented by host-based software firewalls on servers and clients to provide several levels of firewall protection.

At key points in the network a “defence diversity” approach should also be taken so that vulnerabilities are minimised. For example, this should involve using firewalls from different vendors in series so that if a vulnerability is exploited in one device, the other will not be subject to it. This will be extended to the use of more than one network virus scanner at the perimeter for the same reason.

### Network Segregation

The principle should be adopted that a network should consist of a set of smaller networks segregated from each other based on either trust levels or organisational boundaries (or both).

For the Nigeria Customs Service network, this will be achieved using separate domains, particularly where separate campus networks are being linked. An appropriate level of trust will be configured at the domain level and domain perimeters will be secured using a firewall where appropriate.

Within networks, Virtual Local Area Networks (VLANs) will be used to segregate organisational units.

### Perimeter Security

At all perimeters between the internal network and an external network (such as the Internet) effective measures will be put in place to ensure that only authorised network traffic is permitted. This will usually consist of at least one Next-generation firewall and for major links with the Internet an appropriate firewall will be used. For connections such as broadband at smaller locations a Packet Filtering firewall may suffice, depending on the results of a risk assessment.

Servers that are intended to be accessed from an external, insecure network (such as web servers) should be in a DeMilitarised Zone (DMZ) of the firewall in order to provide additional protection for the internal network.

### Public Networks

Where information is to be transferred over a public network such as the Internet, strong encryption via SSL/TLS must be used to ensure the confidentiality of the data transmitted.

Servers that will be accessed from devices on the public network will be located in the DMZ of the firewall.

### Wireless Networks

Wireless networks should be secured using WPA2 encryption. WEP and WPA should not be used.

Wireless networks should be treated as insecure even if WPA2 is used as the encryption method and a firewall is installed between the wireless network and the main LAN.

A guest wireless network may be provided for visitors. This should be physically separate from all internal networks (including internal wireless networks) and secured using a firewall.

Wireless access points can be configured to broadcast their SSID, but configured to not allow secure connection using WPS (Wi-Fi Protected Setup) via physical access to the access point itself.

Wireless access point administrator logon passwords should always be changed from the default.

### Physical Security

Remote network equipment will be housed in secure cabinets which will be always locked. Only authorized personnel will have access to the key to each cabinet.

Backbone and centralised network equipment will be housed in appropriate lockable cabinets or racks in a secure server room to which only authorised personnel will have access.

Wireless access points located in public areas should be hidden from view where possible and should be placed in positions where access by the public is difficult e.g. in or near the ceiling. A lockable protective casing should be installed where an access point is in an unprotected public area e.g. a car park.

### Remote Access

Where there is a requirement for remote access to the internal network the following controls will be used:

* A Virtual Private Network (VPN) will be used providing session encryption using SSH.
* Multi factor authentication at the client where appropriate.
* Secure authentication using a RADIUS server.
* Network Access Control (NAC) will be used to restrict access to remote clients that do not meet minimum requirements e.g. malware control.

Remote access should be granted on an “as required” basis rather than for all users by default.

### Network Intrusion Detection

A Network-based Intrusion Detection System (NIDS) will be installed at the network perimeter and at all key points within the network e.g. on critical servers.

For networks with high security requirements, an Intrusion Prevention System (IPS) will be considered, although its implementation should be approached with caution to avoid a high degree of false positives with corresponding disruption to service to users.

### Network Security Standards

The following standards will be adopted with respect to network configuration and security.

#### Network Hardware

Where possible a single supplier policy will be used for network hardware. An exception will be made where the use of multiple vendor hardware may increase the level of security provided e.g. in a dual network-based firewall configuration.

Network routing will be based on approved routers. High-end switches will be used as standard for connectivity. Switch ports, including diagnostic ports will be configured to be administratively disabled until required. Hubs will not be used due to their inherent security weaknesses.

Cat 6 UTP or fibre optics will be used for network cabling unless specific circumstances (such as excessive interference) preclude its use. The network topography used will be Ethernet or fibre optics, according to the IEEE 802.3 and 802.8 family of standards.

#### IP Addressing

IPv4 will be used on internal networks. However new network devices purchased should support IPv6 in preparation for the future.

The internal IP address range used will be determined and the assignment and use of subnets will be monitored carefully.

IP addresses and associated network information for desktop and laptop clients will be controlled using DHCP and static. Internal and external DNS servers will be used if required.

#### Network Protocols

The protocol used on all networks will be TCP/IP. UDP will be used where appropriate, but other OSI layer 4 network protocols should not be used.

Only protocols and ports required on a specific server should be enabled by default in order to reduce the attack surface. This is especially true for servers within the DMZ of the firewall(s).

## Network Security Management

Once networks have been designed and implemented based on a clear set of security requirements, there is an ongoing responsibility to manage and control the secure networking environment to protect Nigeria Customs Service information in systems and applications. This will be achieved via controls in the following areas.

### Roles and Responsibilities

Roles and responsibilities for the management and control of networks should be clearly defined. To provide effective segregation of duties, the operation of networks is managed separately from the operation of the rest of the infrastructure such as servers and applications.

This segregation of duties is detailed in the following table.

|  |  |  |
| --- | --- | --- |
| **Manager Role** | **Team** | **Main Responsibilities** |
| Networks Manager | Network and Communications Management | Design and implementation of new and changed networks  Installation and removal of networking equipment  Configuration of networking equipment  Third line incident management |
| Network Operations and Security Manager | Network Operations | Network availability monitoring  Network intrusion monitoring  Second line incident management  Configuration backups  Patching and updates  Setup and management of remote access users |
| Servers and Cloud Operations Manager | Servers and Cloud Operations | Server and application backups  Job scheduling  Infrastructure monitoring  First line incident management |

### Logging and Monitoring

Logging levels on network devices will be configured in accordance with Nigeria Customs Service policy (see [ISMS18002 Procedure for Monitoring the Use of IT Systems](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18002%20Procedure%20for%20Monitoring%20the%20Use%20of%20IT%20Systems.doc)) and logs will be monitored on a regular basis.

Firewall logs will be monitored for signs of excessive port scanning which may be a precursor to a remote attack. Where installed, a Network-based Intrusion Detection System will be configured to alert the Network Operations team of this activity.

Network monitoring for availability will be achieved using an appropriate SNMP-based network management tool and recovery actions automated where possible.

Alerts from the Network Access Control (NAC) system must be addressed immediately to ensure that clients that do not meet minimum security requirements are only allowed access to a quarantined subset of systems on the network.

### Network Changes

All changes to network devices will be subject to the change management process (see [ISMS18005 Change Management Process](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A12.%20Operations%20security\ISMS18005%20Change%20Management%20Process.doc)) and appropriate risk assessment, planning and backout methods put in place. The Configuration Management Database (CMDB) must be updated whenever such changes are carried out so that a current and accurate picture of the network is maintained at all times.

### Network Security Incidents

Events which are deemed to be network security incidents must be recorded and managed according to the incident management process (see [ISMS22002 Incident Management Process](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A16.%20Information%20security%20incident%20management\ISMS22002%20Incident%20Management%20Process.doc)).

Major network outages should be managed via the Major Incident Management Process (see [ISMS22003 Major Incident Management Process](file:///C:\Users\Umar%20Farouk\OneDrive\Documents\TMP\ISO%2027001%20Information%20security%20management%20systems\ISO-27001-2013-V5R1\A16.%20Information%20security%20incident%20management\ISMS22003%20Major%20Incident%20Management%20Process.doc)) which provides for the invocation of aspects of the business continuity plan where appropriate.

# Conclusion

Network security is a cornerstone of PMO defences against many of the threats with which we are faced. Only by designing effective security into every new system and network from the very beginning can effective control be maintained, and risk minimised. Further to this, additional controls must be implemented which ensure that proper segregation of duties is achieved and changes to the network environment happen in a managed way.

Combined with watchful monitoring of the network itself and the tools put in place to manage it, this should ensure that the number and severity of network security incidents is minimised and our exposure from those that do occur is not as great as it otherwise might have been.