

February 2025

INTERNAL

# Network Security Policy

FUNDS  AXIS

<b>Policy title:</b>	Network Security Policy
----------------------	-------------------------

<b>Issue</b>	1.0
<b>Approved by:</b>	Trevor Dempster
<b>Approval Date:</b>	February 2025
<b>Next Review Date:</b>	February 2026

<b>Scope:</b>	The policy applies to Funds-Axis Limited and all contractors and other people working on behalf of the company.
<b>Associated documentation:</b>	<ul style="list-style-type: none"> <li>\ Mobile Device Policy</li> <li>\ Remote Working Policy</li> <li>\ Anti-Malware Policy</li> </ul>
<b>Responsibility for Implementation &amp; Training:</b>	<p>Day to day responsibility for implementation: ISO</p> <p>Day to day responsibility for training: ISO</p>

<b>Distribution methods:</b>	<p>Methods used to communicate this policy:</p> <ul style="list-style-type: none"> <li>\ Training</li> </ul>
------------------------------	--

## 1. Introduction

The use of networks is an essential part of the day-to-day business of Funds-Axis. Networks not only connect many of the components of business processes together internally, but they also link the organisation with its suppliers, customers, stakeholders and the outside world.

The organisations networks have evolved over a period of time to become the circulatory system of the company, transporting information to where it needs to go and enabling business 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 business. Therefore, these networks need to be protected to ensure that the confidentiality, integrity and availability of our vital information is always assured.

The effective protection of our networks requires that we adopt good 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 Funds-Axis's rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure. Its intended audience is IT and information security management and support staff who will implement and maintain the organisations defences.

As a cloud service provider (CSP), this policy also applies to the methods used to design and create the physical and virtual networks used to deliver service to our cloud customers.

This control applies to all systems, people and processes that constitute the organisations information systems, including board members, directors, employees, suppliers and other third parties who have access to Funds-Axis systems.

The following policies and procedures are relevant to this document:

- \ Mobile Device Policy
- \ Remote Working Policy
- \ **Change Management Process**
- \ **Software Policy**
- \ Anti-Malware Policy

## 2. Network Security Policy

### 2.1 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.

#### 2.1.1 Requirements

A network design must 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.

Requirements must be documented and agreed before design work starts.

#### 2.1.2 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 may be supplemented by host-based software firewalls on servers and clients in order to provide several levels of firewall protection.

At key points in the network a “defence diversity” approach must also be taken so that vulnerabilities are minimised. For example, this may 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 may be extended to the use of more than one network virus scanner at the perimeter for the same reason.

## **2.13 Network Segregation**

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

For a large network this may be achieved using separate domains, particularly where separate organisations' networks are being linked. An appropriate level of trust must be configured at the domain level and domain perimeters must be secured using a firewall where appropriate.

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

In a cloud environment, it is important that requirements for segregating networks to achieve tenant isolation are defined and the cloud service provider's ability to meet these requirements is verified.

Where Funds-Axis is acting as a CSP, it is important to enforce segregation between our multi-tenant clients and also between the cloud service customer environment and our own internal networks.

### **2.1.4 Perimeter Security**

At all perimeters between the internal network and an external network (such as the Internet) effective measures must be put in place to ensure that only authorised network traffic is permitted. This will usually consist of at least one Stateful Inspection Firewall and for major links with the Internet an Application (or Application Gateway) firewall must 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) must be location in a DeMilitarised Zone (DMZ) of the firewall in order to provide additional protection for the internal network.

### **2.1.5 Cloud Networks**

Where virtual infrastructure services are configured within a virtual private cloud, the same principles must be used as for the security of physical networks. These will include the use of network segmentation, firewalls (for example the use of AWS security groups), access control lists and log monitoring (for example the use of AWS CloudWatch).

## **2.1.6 Public Networks**

Where information is to be transferred over a public network such as the Internet, strong encryption via 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.

## **2.1.7 Wireless Networks**

Wireless networks must be secured using WAP2 encryption. WEP and WPA must not be used.

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

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

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

Wireless access point admin logon passwords must always be changed from the default.

## **2.1.8 Physical Security**

Remote network equipment will be housed in secure cabinets which will always be locked. Only support staff 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 support staff will have access (except for local facilities staff for reasons of health and safety).

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

## 2.1.9 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 TLS
- \ Multifactor 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. virus control

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

## 2.1.10 Network Intrusion Detection

A Network-based Intrusion Detection System (NIDS) must 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) may 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.

## 2.1.11 Network Security Standards

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

### 2.1.11.1 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 **Cisco routers using OSPF. Cisco Gigabit 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 will be used for network cabling unless specific circumstances (such as excessive interference) preclude its use. The network topography used will be Ethernet according to the IEEE 802.3 family of standards.

## 2.1.11.2 IP Addressing

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

The internal IP address range used will be **XXX.XXX.X.X – XXX.XXX.X.X**, the assignment and use of subnets must be monitored carefully.

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

## 2.1.11.3 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 will be enabled by default in order to reduce the attack surface. This is especially true for servers within the DMZ of the firewall(s).

## 2.2 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 the organisation's information in systems and applications. This must be achieved via controls in the following areas.

### 2.2.1 Roles and Responsibilities

Roles and responsibilities for the management and control of networks must be clearly defined. In order 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
--------------	------	-----------------------

Network Manager	Michael McKinley – Cyber Security	Design and implementation of new and changed networks Installation and removal of networking equipment Configuration of networking equipment Third line incident management
Network Operations Manger	Sarim Jamal – Cyber Security	Network availability monitoring Network intrusion monitoring Second line incident management Configuration backups Patching and updates Setup and management of remote access users
Computer Operations Manager	TBC	Server and application backups Job scheduling Infrastructure monitoring First line incident management

Table 1: Roles and responsibilities

## 2.2.2 Logging and Monitoring

Logging levels on network devices must be configured in accordance with organisation policy ([see Logging and Monitoring Policy](#)) and logs 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 must be configured to alert the Network Operations team of this activity.

Network monitoring for availability may be achieved using an appropriate SNMP-based network management tool ([such as Nagios or WhatsUp Gold](#)) 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.

## 2.2.3 Network Changes

All changes to network devices will be subject to the change management process ([see Change Management Process](#)) and appropriate risk assessment, planning and back-out methods put in place. Configuration records must be updated whenever such changes are carried out so that a current and accurate picture of the network is always maintained.

## 2.2.4 Network Security Incidents

Network events which are deemed to be security incidents must be recorded and managed according to the Cyber Security Incident Response Procedure.

### 3. Conclusion

Network security is a cornerstone of Funds-Axis's 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 reduced. 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.