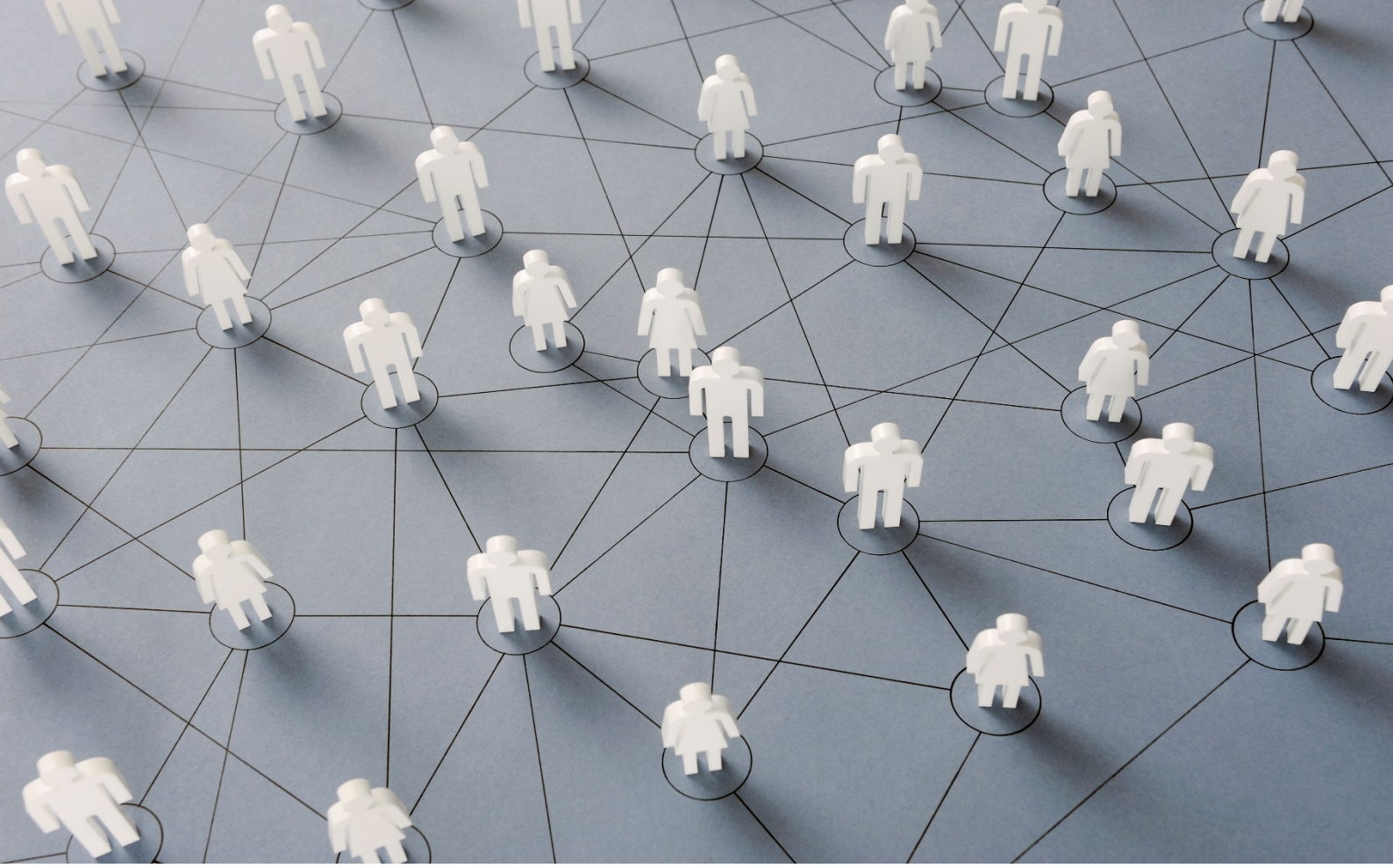

Network Security Policy

Reference: FPD0131-2022

Version: 1

Owner: James Pobgee

First Issued Date:

Revision Issued Date:

To outline FISCAL Technologies' requirements for security of the network infrastructure and associated networks.

Prepared for:
All Employees, select Contractors,
Partners and Customers

Prepared by:
James Pobgee

FISCAL Technologies Ltd
448 Basingstoke Road,
Reading, RG2 0LP
Tel: 0845 680 1905

FISCAL TECHNOLOGIES

1 CONFIDENTIALITY

Table of Contents

2 DOCUMENT CONTROL

Item	Description
Document Title:	Network Security Policy
Associated Controls:	B.5.10 B.5.14 B.5.15 B.5.18 B.5.2 B.5.23 B.6.4 B.7.11 B.7.12 B.7.5 B.7.8 B.8.14 B.8.15 B.8.16 B.8.17 B.8.2 B.8.20 B.8.21 B.8.22 B.8.3 B.8.5 B.8.6 B.8.7 B.8.9
Reference ID:	FPD0131-2022
Version:	1
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	25/09/2023
Revision Issued Date:	
Reference Documents:	Linked Policies: Linked Procedures: Linked Records:

2.1 DOCUMENT PUBLICATION HISTORY

(All revisions made to this document must be listed in chronological order, with the most recent revision at the bottom)

Version	Date	Author
1		James Pobgee

3 PURPOSE AND SCOPE

3.1 PURPOSE

The purpose of this policy is to ensure that all staff understand their role regarding the security of the network infrastructure and the acceptable use of information systems which they have access to for their day-to-day tasks. Its other purpose is to provide assurance that FISCAL Technologies systems and networks are maintained, secure, efficient, and effective.

3.2 SCOPE

This policy is applicable to all information and IT assets (including networks, systems, and infrastructure), information processing facilities, personnel as well as all third-party personnel within the scope of FISCAL's Information Security Management system.

4 NETWORK SECURITY MANAGEMENT

4.1 NETWORK CONTROLS

Network controls ensure information communicated through the network will be protected and maintain the confidentiality, integrity and availability of the information shared. The following should be considered when implementing robust network protocols and services:

- Equipment needs to be maintained and patched regularly.
- IPS / IDS must be enabled where applicable and available.
- RADIUS infrastructure or equivalent shall be implemented where applicable and available.
- Authentication systems must be in place to access and configure network devices.
- All non-FISCAL devices, including Personal, customer and guest devices must not use company network Wi-Fi or plug in to the network via cable. Non-FISCAL devices must use the guest WIFI network only.
- Management and sensitive traffic must be segmented from other network traffic.
- Vulnerable network protocols must be disabled.

4.2 SECURITY OF NETWORKS AND SERVICES

Employees are not given administration rights for servers unless this task forms part of their job role, or there are justifiable reasons for doing so. Authority for granting administrator rights for staff other than those who are designated administrators will be controlled, monitored, and reviewed by the IT Team and authorised by the Director of IT and Security. All requirements of network services are identified by Management, including services agreements whether in-house or outsourced.

To ensure security of the network and its associated services:

- Networks must be documented including network diagrams and configuration files for devices e.g., routers, switches, etc.
- Gateway rules should be limited to the minimum required ports both for inter-VLAN traffic and external traffic (inbound and outbound).
    - Firewalls or equivalent should protect network borders.
    - Ports should be limited to minimum required for activities.
    - All gateway rules must be documented with valid justification and sign off prior to implementation.
- Systems supporting utilities should only be connected to the internet when need or only in a secure manner e.g., Door System (server can be connected to receive updates, though shouldn't be otherwise and the connected door controllers should not have any external access).

- Where a network is critical, resilience should be implemented e.g., network backup lines, UPS', multi-pathing for cables, multiple devices, etc.
    - Resilience of equipment can also come in the form of support / service agreements, spare equipment or under capacity of equipment to enable failover in event of a failure.
- Devices or software that is no longer supported / receiving patches must be segmented to a separate network segment and restricted access to the internet and other networks.

Where possible network equipment must be secured in data rooms with limited access:

- Access to Cabinets and patch panels should be locked and accessible via key.
- Where possible data cables should be separated from power.
- Physical sweep of ports in an office at least annually for unauthorised devices being attached to cables or ports.

4.3 CONFIGURATION OF NETWORK ASSETS

- Employees must adhere to recommended best practices and guidance provided by the manufacturer of all hardware and software.
- Whenever feasible, standard templates from reputable organisations such as CIS, NIST, or NCSC should be employed.
    - The versioning of standard templates in use must be reviewed at regular intervals to ensure compliance.
    - Exceptions to these policies should be documented with justifications for any exceptions.
    - Configuration checks should be conducted whenever possible to identify deviations and rectify them to align with assigned policies.
- Unnecessary accounts, functions, and services must be disabled.
- All systems must synchronize their clocks with the specified NTP (Network Time Protocol) source.

*Licensing requirements and other relevant considerations are to be covered under the **acceptable use policy**.*

4.4 UNSECURE NETWORKS

There are many risks associated with unsecure networks including: Unencrypted networks, WIFI Snooping and sniffing, Man in the middle attacks, Malware distribution, and malicious hotspots. To reduce the risks to FISCAL devices and data wherever possible employees should not use unsecure networks or hotspots.

If you must utilise an unsecure network e.g., a hotel WIFI:

- Validate that the WIFI is the hotels hotspot.
- Avoid accessing any sensitive information and reduce any data used while on the network.
- Ensure all sites you visit are encrypted.
- When using FISCAL systems use the FISCAL VPN.
- Do not set the connection to auto-connect.
- Do not set your network discovery to enabled.
- Turn off file sharing and do not share files.
- Use multi-factor authentication.
- Remember to disconnect and log out of your device following completing the required activity.

- If you must access sensitive information in public areas, consider requesting a privacy screen for your laptop.

If you believe there is an issue or your device has become compromised, raise it with the helpdesk immediately.

4.5 SECURITY MONITORING

Fiscal Technologies will ensure that there is continuous monitoring of their network, for any and all potential security breaches and threats.

Network monitoring systems shall be in place where appropriate and will monitor all inbound and outbound traffic, modification of network configuration, security events from IDS / IPS and other security systems on devices and perimeter, utilisation of resources.

All blocked traffic events should be logged as well as all performance capacity.

4.6 NETWORK SEGREGATION

FISCAL Technologies shall ensure that, where possible, segregate their computing networks into sub-networks based on the level of sensitivity, criticality, and type of network.

FISCAL Technologies will restrict the flow of traffic between these different sub-networks to ensure the confidentiality, integrity, and availability of information on critical sub-networks.

FISCAL Technologies will ensure that cloud service providers are able to meet these requirements.

The following requirements will be implemented for network segmentation:

- Networks must be segmented by appropriate network technologies e.g., VLAN's, Subnets, etc.
- Networks must be segmented environment type, sensitivity of environment and potential risks e.g.
    - Production / test, servers / clients / Wi-Fi, Internal / external, compliant, and uncompliant.
- Where network segments bridge access controls should be put in place to limit the traffic and ports between networks to purely those required to reduce surface and risk.

5 INFORMATION TRANSFER

Security is maintained of any information transferred using FISCAL Technologies' network, both internally and/or externally.

Information transfer policies and procedures are in place to protect the transfer of information through the use of all types of communication systems. Please refer to ***Mobile Device Policy*** and ***Information Management Policy.***

Agreements for the transfer of information between FISCAL Technologies and external parties are covered in contractual agreements, including service agreements. Please refer to ***Supplier Security Policy*** and ***Information Management Policy.***

Electronic messaging is appropriately protected, and best practice principles are adopted with regards to monitoring this service. Please refer to ***Acceptable Use Policy*** and ***Information Management Policy.***

6 ENFORCEMENT AND VIOLATIONS

6.1 ENFORCEMENT

All divisions & employees of the organisation must comply with the requirements of this policy. Management is responsible for ensuring that the policy is implemented within its area of responsibility.

FISCAL Technologies expects all users to comply with the terms of this policy and all other policies, procedures, guidelines, and standards published in its support.

6.2 VIOLATIONS

Violations of this policy shall result in disciplinary action / legal ramifications by the organisation. Disciplinary action will be consistent with the severity of the incident as determined by an investigation and as deemed appropriate by Management and HR.

Compliance with this policy will be reviewed by the organisation's Internal Audit Team.