©(ORGANISATION NAME)

NETWORK SECURITY POLICY

Subject: Network Security Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 7	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 INTRODUCTION

Networks form the basic means of electronic communication within and outside of the Organisation. Therefore, the Organisation should deploy appropriate measures to protect these assets. Furthermore, interaction with external networks such as the Internet and other third-party networks introduces the risk of potential compromise to the Organisation's information asset.

Reference	Description of Risk
SAFETag	Network Access
SAFETag	Network Scanning and Traffic Analysis
SAFETag	Hardening of Network Devices

1.2 OBJECTIVES

The objective of this policy is to ensure the:

- overall security of the Organisation's network devices and all computing equipment used on the network.
- Organisation permits only authorised traffic in and out of its network.

2. POLICY STATEMENTS

- Formal procedures shall exist to approve any service request through the Organisation network perimeter devices; every service request shall have an approved business objective.
- A risk-based approval process shall exist to identify additional risks introduced to the Organisation by the service.
- The internal network shall be efficiently and effectively segmented.
- All Network Devices (routers, switches, etc.) shall be secured with passwords in line with the Organisation's password policy.
- All default/generic accounts on network devices shall be disabled. However, for default/generic accounts with business exigencies:
    - their passwords shall be changed.
    - the Organisation's password policy shall be enforced.
    - the default/generic account shall be assigned to a responsible stakeholder who will be responsible and accountable for the usage of the default/generic account.
- Wireless devices shall be securely passworded. The password for accessing the wireless environment shall be changed at every <<to be defined by the Organisation>>. The visibility of the wireless devices shall be secured to determine how far the Organisation's wireless network extends beyond a controlled area.

- The network devices shall be running on current/non-vulnerable firmware/iOS/Operating systems.
- The internal network shall be separated from the external network by a network security perimeter. This separation shall be established through a secure Demilitarized Zone (DMZ).
- Network perimeters shall be configured by default to prohibit all that is not explicitly allowed; permitted connections and protocols through the perimeter shall be explicitly defined. Any connection or protocol not explicitly defined and permitted shall be prohibited by the network perimeter.
- Network perimeters shall be monitored for policy violations; the configuration of a network perimeter shall be such that it is able to detect unauthorised access attempts.
- Confidential and restricted data shall be encrypted when sent over external networks. External networks refer to networks that are not directly managed by the Organisation. This includes the Internet and third-party/vendor network.
- A log of all operational network activities shall be maintained.
- The network activity logs shall be reviewed by the IT Department (or other responsible stakeholder assigned to the function)
- User passwords shall be encrypted when transmitted over internal networks. Other data sent over internal networks shall be encrypted based on risk assessment.
- Remote access to the Organisation shall be through authorised secured VPN connectivity. This shall be subject to the approved stakeholders (CISO, CIO/Head of IT)

3. RECOMMENDATIONS/ADVISORY ON NETWORK FIREWALLS

Organisations with 1 – 5 Staff	**Organisations with 6 – 20 Staff**	**Organisations with more than 20 Staff**
▪ Consider the use of Windows Firewall on workstation for host-based network protection. https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/ https://learn.microsoft.com/en-us/windows/security/operating-	▪ Consider the use of Windows Firewall on workstation for host-based network protection. https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/ https://learn.microsoft.com/en-us/windows/security/operating-	▪ Consider the use of Windows Firewall on workstation for host-based network protection. https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/ https://learn.microsoft.com/en-us/windows/security/operating-

system-security/network-security/windows-firewall/rules ▪ Consider the use of Access List/MAC Address filters on Wireless Routers and Wi-Fi/Hotspot devices. ▪ Consider the use of Windows VPN for remote access. Windows VPN	system-security/network-security/windows-firewall/rules ▪ Consider the use of Access List/MAC Address filters on Wireless Routers and Wi-Fi/Hotspot devices. ▪ Consider the use of Windows VPN for remote access. Windows VPN	system-security/network-security/windows-firewall/rules ▪ Consider the use of Access List/MAC Address filters on Wireless Routers and Wi-Fi/Hotspot devices. ▪ Consider the use of Windows VPN for remote access. Windows VPN ▪ Consider the use of open source-firewall devices. https://www.pfsense.org/ https://www.ipfire.org/ https://opnsense.org/ ▪ Consider the use of proprietary firewall solutions. https://www.sophos.com/en-us https://www.sonicwall.com/