©(ORGANISATION NAME)

TRAVEL POLICY (Remote Access/VPN)

Subject: Travel Policy (Remote Access/VPN)		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 11	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

Remote access to our Organisation’s network is essential to maintain our team's productivity, but in many cases, this remote access originates from networks that may already be compromised or have a significantly lower security posture than our Organisation’s network.

The risks associated with unauthorised access to the Organisation's Network can be significant and far-reaching. Some of the major risks include:

Reference	Description of Risk
SAFETag	Loss of sensitive or confidential data
SAFETag	Intellectual property theft
SAFETag	Reputation damage
SAFETag	Malware infections
SAFETag	Regulatory Compliance Violations
SAFETag	Service disruption
SAFETag	Financial losses

1.1 SCOPE

This policy applies to all employees, contractors, vendors, and other authorised parties who require remote access to Organisation's internal network and resources.

1.2 RELATED DOCUMENTS

The following policies and procedures are relevant to this document:

- Encryption Policy
- Acceptable Use Policy

1.3 PURPOSE

The purpose of this policy is to define rules and requirements for connecting to an Organisation's network from remote locations through Remote Access Virtual Private Network (VPN) connections. These rules and requirements are designed to minimise the potential exposure to Organisation from damages which may result from unauthorised use of organisational resources, while also providing guidelines for secure remote access to the Organisation’s network.

2.0 POLICY

2.1 RULES

2.1.1 It is the responsibility of Organisation employees, contractors, vendors, and agents with remote access privileges to the Organisation's network to ensure that their remote access connection is given the same security consideration as their on-site connection to the Organisation.

2.1.2 General access to the Internet for recreational use through the Organisation's network is strictly limited to Organisation employees, contractors, vendors, and agents (hereafter referred to as "Authorised Users").

2.1.3 When accessing the Organisation's network from a personal computer, Authorised Users are responsible for preventing access to any Organisation's computer resources or data by non-Authorised Users.

2.1.4 Performance of illegal activities through the Organisation's network by any user (Authorised or otherwise) is prohibited.

2.1.5 The Authorised User bears responsibility for and consequences of misuse of their access. For further information and definitions, see the Acceptable Use Policy.

2.1.6 Authorised Users will not use the Organisation's networks to access the Internet for any personal business interests.

2.2 APPROVED REMOTE ACCESS METHOD

- The only approved remote access method to the Organisation's network is Virtual Private Network (VPN) using the Organisation's VPN client software.
- Unauthorised remote access methods, such as remote desktop sharing tools or file transfer utilities, are strictly prohibited.

2.3 VPN REQUIREMENTS

Approved users may utilize the benefits of the VPN service, which is a "user-managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

2.3.1 All remote access to the Organisation’s internal network must be established using the Organisation’s VPN client software. VPN connections must use strong encryption protocols and authentication mechanisms, as specified by the IT department.

2.3.2 VPN access is restricted to Authorised personnel only, and user accounts will be provisioned based on the principle of least privilege. VPN credentials must be kept confidential and never shared with unauthorised parties.

2.3.3 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For further information, see the Acceptable Encryption Policy and the Password Policy.

2.3.4 It is the responsibility of users with VPN privileges to ensure that unauthorised users are not allowed access to Organisation's internal networks.

2.3.5 VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

2.3.6 When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.

2.3.7 VPN gateways will be set up and managed by Organisation's network operational groups.

2.3.8 All computers connected to Organisation's internal networks via VPN must use the most up-to-date anti-virus software and operating system patches.

2.3.9 VPN users will be automatically disconnected from the Organisation network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

2.3.10 Users of computers that are not Organisation-owned equipment must configure the equipment to comply with Organisation's VPN and Network policies.

2.3.11 Only Security-approved VPN clients may be used.

2.3.12 By using VPN technology, users must understand that their machines are a de facto extension of the internal network and, as such, must not use the connection for any purpose other than providing technical support.

2.4 REMOTE ACCESS SECURITY

2.4.1 Sensitive data accessed remotely must be handled in accordance with Organisations data classification and handling policies.

2.4.2 Remote access sessions must be terminated when not in use to prevent unauthorised access.

2.4.3 All remote access connections and activities may be monitored and logged for security and compliance purposes. Logs will be reviewed periodically for potential security incidents or policy violations.

2.4.4 Authorised users must ensure that their remote access devices (e.g., laptops, smartphones) are secure, up to date with the latest security patches, and equipped with antivirus/antimalware software.

2.4.5 Authorised Users shall protect their login and password, even from family members.

2.4.6 While using an Organisation-owned computer to remotely connect to Organisation 's corporate network, Authorised Users shall ensure the remote host is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of an Authorised User or Third Party.

2.4.7 Use of external resources to conduct Organisation business must be approved in advance by Information Security and the appropriate business unit manager.

2.4.8 All hosts that are connected to Organisation's internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.

2.4.9 Personal equipment used to connect to Organisation’s networks must meet the requirements of Organisation owned equipment for remote access.

3.0 SUPPLIERS OBTAINING ACCESS TO ORGANISATION’S SYSTEMS

3.1 PROCEDURE FOR SUPPLIERS TO OBTAIN REMOTE ACCESS TO ORGANISATION’S SYSTEMS.

3.1.1 All requests for access must be logged by the supplier with the Service Desk by providing the following details:

- Name, company, and contact details of person requesting access.
- Reason for access, quoting the relevant IT Service Desk Call reference (if the access is not in relation to a logged incident, they must provide the name of the staff member who requested access to the system.
- The access password for the appropriate supplier

3.1.2 The IT Service Desk will then verify the access request by:

- checking that the password given is correct for that supplier.
- checking the call reference given on the Service Desk system
- checking with an appropriate staff member if the access is not related to a Service Desk call.

3.1.3 If the request is verified:

a) Enable the VPN link.
b) enable the support user account on the relevant system.
c) Log the fact that access has been given on the relevant Service Desk call.

3.1.4 Once access is verified, contact the supplier using the details provided to inform them that they can connect.

3.1.5 When the task requiring access is completed, the supplier will contact the IT Service Desk to inform them of this fact. The IT Service Desk will then:

a) disable the VPN link.
b) disable the support user account.
c) add a note to the relevant Service Desk call to indicate that the supplier has disconnected.

3.1.6 As a further precaution, all connections will be terminated at 6pm each weekday evening. If the supplier needs access beyond this time, they must inform the IT Service Desk

3.2 OTHER CONSIDERATIONS

3.2.1 Remote access to the Organisation's systems by suppliers must be tightly controlled.

3.2.2 Any changes to the supplier's connections must be immediately reported to the IT Service Desk so that access can be updated or ceased.

3.2.3 All permissions and access methods must be controlled by the IT Service Desk.

3.2.4 Partners or third-party suppliers must contact the IT Service Desk before connecting to the Organisation's network and a log of activity must be maintained.

3.2.5 Remote access software must be disabled when not in use.

4.0 CHANGES TO SYSTEMS

Supplier and employee are required to adhere to the following rules:

4.1 Any changes that need to be carried out by supplier support staff on the Organisation's systems must first be defined and raised as a change request.

4.2 This will be achieved by contacting the IT Service Desk who will ask for the relevant information and submit the change request for approval on the supplier's behalf. They will ask for the following details:

- One-line Summary of Change
- Details of change
- Users affected (particularly if a system outage is required)

- Support and Testing plan.
- Contingency plan (how can the change be backed out?)
- Communication plan (who needs to be informed and when?)

4.3 The Service Desk will submit the change request to the Change Management office, where it will be assessed, and if acceptable, it will be authorised. Change requests will be assessed and processed in a timely manner to minimise delays.

- The Service Desk will inform the supplier when the change has been authorised.
- Once authorised, the change may be implemented by the supplier.
- The success or otherwise of the change must be communicated by the supplier to the Service Desk, and the supplier must also inform the Service Desk if the remote connection is no longer required.
- The Service Desk will inform the Change Manager of the success or otherwise of the change.

5.0 RESPONSIBILITIES

5.1 Users are responsible for ensuring compliance with this policy and reporting any suspected security incidents or policy violations.

5.2 The IT department is responsible for implementing, managing, and maintaining the remote access and VPN infrastructure, as well as providing guidance and support to users.

6.0 RECOMMENDATIONS/ADVISORY ON TRAVEL (REMOTE ACCESS/VPN)

Organisations with 1 – 5 Employees	Organisations with 6 – 20 Employees	Organisations with more than 20 Employees
• Use a Secure VPN Solution: NordVPN https://nordvpn.com/ or ExpressVPN https://www.expressvpn.com/, or open-source VPN server like OpenVPN https://openvpn.net/ within your network. • Enforce two-factor authentication for all VPN connections to add an extra layer of security beyond just passwords. Google Authenticator https://google.com/landing/2step/ or Authy https://authy.com/ • Deploy antivirus software like Bitdefender, https://www.bitdefender.com/ or Malwarebytes https://www.malwarebytes.com/ • Consider using a password manager like LastPass, https://www.lastpass.com/or KeePass https://keepass.info/ to generate and store strong passwords. • Make use of Microsoft bit locker for disc volume encryption and encryption of USB removable storage	• Make use of Windows VPN Connectivity for remote Access to Server https://support.microsoft.com/en-us/windows/connect-to-a-vpn-in-windows-3d29aeb1-f497-f6b7-7633-115722c1009c# • Implement logging and monitoring mechanisms to track all remote access activities. Tools like Splunk https://www.splunk.com/ or ELK Stack https://www.elastic.co/elk-stack • Deploy endpoint protection solutions like Bitdefender. https://www.bitdefender.com/, Sophos https://www.sophos.com/, or open-source like ClamAV https://www.clamav.net/ to protect remote devices from malware, viruses, and other cyber threats. • Make use of Microsoft bit locker for disc volume encryption and encryption of USB removable storage	• Make use of Windows VPN Connectivity for remote Access to Server https://support.microsoft.com/en-us/windows/connect-to-a-vpn-in-windows-3d29aeb1-f497-f6b7-7633-115722c1009c# • Implement logging and monitoring mechanisms to track all remote access activities. Tools like Splunk https://www.splunk.com/ or ELK Stack https://www.elastic.co/elk-stack • Deploy endpoint protection solutions like Bitdefender. https://www.bitdefender.com/, Sophos https://www.sophos.com/, or open-source like ClamAV https://www.clamav.net/ to protect remote devices from malware, viruses, and other cyber threats. • Make use of Microsoft bit locker for disc volume encryption and encryption of USB removable storage

devices https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ • Make use of open-source encryption solutions https://www.7-zip.org/ https://gnupg.org/	devices https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ • Make use of open-source encryption solutions https://www.7-zip.org/ https://gnupg.org/	devices https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ • Make use of open-source encryption solutions. https://www.7-zip.org/ https://gnupg.org/ • Implement enterprise-endpoint protection and management solutions like Microsoft Endpoint Manager https://www.microsoft.com/en-us/security/business/microsoft-intune Symantec Endpoint Protection https://www.broadcom.com/products/cybersecurity/endpoint or open-source like OPSI https://www.opsi.org/