**Virtual Private Network (VPN)**

**Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author/Editor** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

**PURPOSE 4**

**SCOPE 4**

***POLICY* 4**

**ENFORCEMENT 5**

1. **PURPOSE**

The purpose of this document is to provide policies for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Organization corporate network.

1. **SCOPE**

This ***policy*** applies to all Organization employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Organization network. This ***policy*** applies to implementations of VPN that are directed through a VPN Gateway.

1. ***POLICY***

Approved Organization employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are 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. Further details may be found in: -

* + - 1. *Remote Access Policy*
      2. *Enterprise Network Security Architecture Policy*
      3. *Policy On General Systems Security and Controls On IDs and Passwords*

Additionally,

* + - 1. It is the responsibility of authorized personnel with VPN privileges to ensure that unauthorized users are not allowed access to Organization internal networks.

* + - 1. 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 pass phrase.
      2. 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.
      3. Dual (split) tunnelling is NOT permitted; only one network connection is allowed.
      4. VPN gateways will be set up and managed by Organization network operational groups or other authorized parties.
      5. All computers connected to Organization internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (refer to IT Security); this includes personal computers.
      6. VPN users will be automatically disconnected from Organization’s network after fifteen minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
      7. The VPN gateway is limited to an absolute connection time of 24 hours.
      8. Users of computers that are not Organization-owned equipment must configure the equipment to comply with Organization's VPN and Network policies.
      9. Only IT Security-approved VPN clients may be used.
      10. Clientless VPN technology may be used after approval from IT Security.
      11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Organization's network, and as such are subject to the same rules and regulations that apply to Organization-owned equipment, i.e., their machines must be configured to comply with Organization’s security policies.

1. **ENFORCEMENT**

# *All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.*

# *Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.*

* 1. ***Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.***
  2. ***Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.***