timeTec

VIRTUAL PRIVATE NETWORK (VPN) POLICY

Document Name:	**Virtual Private Network (VPN) Policy**		
Current Version:	V1.0		
Prepared by:	Barry Chai, COO	**Signature:**	
Approved by:	Daryl Choo, CTO	**Signature:**	
Last Updated:	1st August 2017		
Confidentiality Level	Confidential		

Virtual Private Network (VPN) Policy

1. Purpose

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to the TimeTec Cloud corporate network.

2. Scope

This policy applies to all TimeTec Cloud employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the TimeTec Cloud network. This policy applies to implementations of VPN that are directed through anyone of these: IPSec, L2TP and OpenVPN.

3. Policy

Approved TimeTec Cloud 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 coordinating installation and installing any required software. Further details may be found in the *Remote Access Policy*.

Additionally,

1. This policy is applicable to OpenVPN, IPSec, and L2TP.
2. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to TimeTec Cloud internal networks.
3. VPN use is to be controlled using either a one-time password authentication with a strong passphrase.
4. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel.
5. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
6. VPN gateways will be set up and managed by TimeTec Cloud’s IT Operation Team.
7. All computers connected to TimeTec Cloud internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard.
8. Users of only company issued computers can have the access to the VPN facilities.
9. Only IT Operation Team’s VPN clients may be used.

4. Policy Compliance

5.1 Compliance

The IT Operation team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, internal and external audits, and feedback to the CTO.

5.2 Exceptions

Any exception to the policy must be approved by the CTO in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Version	**Date of Change**	**Prepared by**	**Summary of Change**
1.0	1st August 2017	Barry Chai	1st Baseline