Virtual Private Network (VPN) Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

This policy provides guidelines for remote access connections to ABC Company’s Information Systems.

# II. Purpose

This policy is established to help protect the integrity, availability and confidentiality of information, to prevent loss of service, and to comply with legal requirements.

# III. Scope

This policy applies to all Staff that administer, monitor, maintain, or remotely use ABC Company’s Information Systems.

# IV. Policy

Approved ABC Company Staff may remotely connect to Company’s Information Systems. Virtual Private Network (VPN) technology provides an encrypted tunnel so that information transmitted to and from Company’s systems are not easily readable by unauthorized parties.

ABC Company Staff are responsible for selecting and providing an Internet Service Provider (ISP), coordinating the installation of Company approved VPN software through the IT Department, installing any required software, and paying associated fees.

It is the responsibility of Staff with VPN privileges to ensure that unauthorized users are not allowed access to ABC Company internal networks from the Staff member’s remote location.

IT Staff shall ensure that VPN use is controlled using either a one-time password authentication, such as a token device, or a public/private key system with a strong passphrase.

When actively connected to ABC Company’s Information Systems, IT Staff shall ensure that implementations force all traffic to and from the user workstation through the VPN tunnel. All other traffic shall be dropped.

Dual (split) tunneling is NOT permitted and only one network connection is allowed. VPN gateways shall be set up and managed by ABC Company’s IT Department.

All computers connected to ABC Company’s Information Systems via VPN or any other similar remote technology must use up-to-date anti-malware software as stated in ABC Company’s Anti-Malware Policy.

VPN users shall be automatically disconnected from ABC Company’s Information Systems network after a period of inactivity. The VPN user must then logon again to reconnect to the network. Pings or other artificial network processes shall not to be used to keep the connection open.

Users of computers that are not ABC Company owned equipment must configure the equipment to comply with ABC Company’s policies. By using VPN technology with personal equipment, VPN users must understand that their machines are an extension of ABC Company's network, and as such are subject to the same rules and regulations that apply to ABC Company owned equipment.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO12.02, APO12.07, APO14.07, BAI02.05, BAI10.07, DSS01.05, DSS05.07, DSS06.08

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv), 164.312(d), 164.312(e)(2)(ii)

ISO 27001:2013 8.3, 9.1, A.6.2.2, A.8.1.3, A.9.1.2, A.9.2.2-3

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AC-2-3, AC-6, AC-17, CM-5, PE-17, PL-4

NIST Cybersecurity Framework PR.AC-3, DE.CM-1, DE.DP-2

PCI 2.3, 7.1-3, 8.1.5