Remote Access 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

The purpose of this policy is to define standards for connecting to ABC Company's network from any remote location. These standards are designed to minimize the potential exposure to ABC Company from damages which may result from unauthorized use of ABC Company Information Resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, and damage to critical ABC Company Information Systems.

# II. Purpose

This policy applies to all ABC Company Staff with a computer used to connect to the ABC Company network from a remote location. This policy applies to remote access connections used to do work on behalf of ABC Company, including reading or sending e-mail and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to, high speed Internet connectivity, Virtual Private Network (VPN), Secure Shell (SSH) and other forms of electronic connectivity to Information Systems.

# III. Scope

This policy applies to all Staff that access ABC Company’s Information Resources from a remote location.

# IV. Policy

Staff shall contact the IT Department for approved methods to remotely connect to ABC Company's Information Systems. Staff shall review ABC Company’s Securing Information Systems Policy for details on protecting information when accessing the corporate network via remote access methods. Staff shall review the Acceptable Use Policy for the acceptable use of ABC Company's Information Systems.

It is the responsibility of Staff with remote access privileges to ABC Company's Information Systems to ensure that their remote access connection is given the same consideration as the user's on-site connection to ABC Company.

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong password/phrase see the Password Policy. At no time should any ABC Company Staff member disclose their login or e-mail password to anyone.

When accessing ABC Company’s Information Resources from a remote location, Staff shall ensure:

* ABC Company’s policies and procedures are followed.
* Friends and relatives do not have access to ABC Company’s systems and assets.
* Staff do not connect to other networks (excluding the Internet and an in-house personal network) at the same time they are connected to ABC Company’s systems.
* Only ABC Company e-mail accounts are used for business related communications.
* All computers, mobile devices, etc. use up-to-date anti-malware software and an activated firewall (if available). Please refer to the Anti-Malware Policy and Mobile Device Policy for more information.

Personal equipment used to connect to ABC Company's networks must meet or exceed the requirements of ABC Company owned equipment for remote access. Staff who wish to implement non-standard remote access solutions to ABC Company Information Systems must obtain prior approval from the IT Department.

# 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 APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.310(b)

ISO 27001 A.7.2.1, A.8.1.2-3

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AC-1-3

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

PCI 2.3, 7.1-3, 8.1.5