Internet Connection 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 has components of a user compliance policy and an internal IT policy. The user compliance section specifies how users are allowed to connect to the Internet and provides for IT Department approval of all connections to the Internet or other private network. It requires all connections such as connections by modems or wireless media to a private network or the Internet be approved by the IT Department and what is typically required for approval such as the operation of a firewall to protect the connection.

This policy requires users to use the Internet for business only and requires users to avoid going to malicious web sites which could compromise security. It informs the users that their Internet activity may be logged and monitored and defines whether user activity on the network will be logged and to what extent. It specifies what system will be used to prevent unauthorized viewing of sites and what system will log Internet usage activity. Defines whether a proxy server will be used for user Internet access. It defines how the network will be protected to prevent users from going to malicious web sites.

# II. Purpose

This policy is designed to protect Information Resources against intrusion by malware that may be brought into the network by users as they use the Internet. It is also designed to prevent unauthorized and unprotected connections to the Internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

# III. Scope

This policy applies to all Staff that have access to ABC Company’s Information Resources.

# IV. Policy

All physical Internet connections or connections to other private networks shall be authorized and approved by the IT Department. Most users will access the Internet through the connection provided for their office by the IT Department. Any additional connections must be approved by the IT Department. These additional connections include but are not limited to:

* A computer or communication device which may allow a connection to the network.
* Any multipurpose printing and FAX machines which have both a phone and network connection must be examined and approved for use by the IT Department.
* Wireless access points or devices with wireless capability are not allowed unless approved by the IT Department. If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to the network unless it is approved for wireless operation by the IT Department when connected to the network. Refer to the Wireless Access Policy for more information.
* Any additional Internet connections not provided by the IT Department must be reviewed and approved by the IT Department. Typically any additional connections from the organizational network to the Internet or other private network will require.
* An IT Department approved firewall operating at all times and properly configured. Refer to the Firewall Policy for more information.
* Some communications may require encryption. Contact the IT Department and/or refer to the Encryption Policy for more information.

An Internet control and logging system shall provide the following capabilities:

* The system will require a login ID or it will use the current network login to identify users.
* The system will prevent users from visiting inappropriate, pornographic, or dangerous web sites. This same system will not require an additional login ID and will use Active Directory to identify Internet users. The system shall be able to log the time of Internet activity, duration of the activity, the website visited, any data downloaded and the type of data downloaded. The system will cache web pages.
* Refer to the Logging Policy for more information.

# 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 Staff members with access to ABC Company’s Information Resources.

**Policy History**

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

**References:**

COBIT APO01.04, APO13.04, BAI09.04, BAI10.10, DSS01.04, MEA01.04

GDPR Article 25, 30, 32

HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)

ISO 27001:2013 A5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29

NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2

PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8