Network Address 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 IT Department is responsible for planning, developing, implementing and maintaining ABC Company's network. The use of Internet Protocol (IP) and network addresses is included in this responsibility.

# II. Purpose

Internet Protocol and network addresses are numeric labels assigned to each network device. The address serves two principal functions, to identify a host or network interface and to identify a location. The purpose of this policy is to ensure network addresses are properly assigned and managed.

# III. Scope

This policy applies to IT Department Staff responsible for managing ABC Company networks.

# IV. Policy

The IT Department Network Administrators are assigned the responsibility of managing ABC Company’s IP and network addresses.

Addresses may be assigned to a device either at the time of startup (dynamic), or permanently assigned (static) by a fixed configuration of its hardware or software. The IT Department shall maintain procedures for implementing, maintaining, and terminating IP and network addresses.

Where possible, Network Administrators shall centrally manage the addresses without having to specifically configure each device on the network as a manual procedure. Dynamic IP addresses can be configured on LANs and broadband networks by Dynamic Host Configuration Protocol (DHCP) servers. This avoids the administrative burden of assigning specific static addresses to each device on a network. It also allows many devices to share limited address space on a network if only some devices are connected at a particular time. Dynamic IP configuration shall be enabled by default so that a user does not need to manually enter settings to connect to a network with a DHCP server.

Systems requiring access to the Internet shall be configured with public (global) IPv4 or IPv6 addresses.

IP or network addresses that are not in use for a period of three months shall be brought to the attention of the Director of IT for resolution.

Network administrators may elect to implement host access controls based on network address. Network addresses may be grouped into subnets of a reasonable size taking into account the types of devices, uses, quantities, physical layout of the network, and ease of network management.

Network Administrators may allocate network addresses within a particular subnet or VLAN. VLANs are generally allocated with one subnet per VLAN for all devices connected to the network. Network Administrators shall maintain a register of VLAN names and address ranges.

# 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 the IT Department Staff.

**Policy History**

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

**References:**

COBIT APO01.03, APO03.06, APO12.02, APO12.07, APO13.07, DSS06.08, MEA01.05

GDPR Article 25, 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 A.5.1.1, A.8.1.1, A.8.2.2

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 CM-8, SC-2, SC-7, SC-21

NIST Cybersecurity Framework ID.AM-5, ID.BE-4, ID.RA-6, ID.SC-1, PR.PT-4, DE.DP-2

PCI 1.3.7