Router Security 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

Routers and switches are networking devices that send and receive data packets between computer networks and devices.

# II. Purpose

This policy describes router security configurations to help minimize and control risks related to the connectivity and availability of ABC Company’s Information Resources.

# III. Scope

This policy applies to all Staff that manage ABC Company’s network and communications systems.

# IV. Policy

Every router and switch deployed in the ABC Company network must be appropriately configured and meet configuration and security requirements.

Access controls shall be used to provide separate authentication, authorization, and accounting services.

Configurations shall prohibit direct public access between public networks (e.g. Internet) and any Information Resource containing sensitive information. Configurations, access control lists, and other network filtering technology must be used to limit network access to devices that store sensitive data. Configurations shall restrict all traffic, inbound and outbound, from untrusted networks (including wireless) and hosts and specifically deny all other traffic except for necessary protocols.

Local user accounts shall not be configured on the router. To prevent unauthorized changes, the device shall be protected using a password available from the IT Director. Access rules shall be implemented and maintained per business needs and as approved by the IT Director.

Unless otherwise approved by the IT Director, routers shall be configured to disallow the following:

* IP directed broadcasts.
* Incoming packets at the router sourced with invalid addresses.
* TCP small services.
* UDP small services.
* All source routing.
* All web services running on router.

Each router must have the following statement posted in clear view: UNAUTHORIZED ACCESS PROHIBITED. Staff must have explicit permission to access or configure this device. All activities performed on routers shall be logged.

Unless there is a secure tunnel protecting the entire communication path, Telnet shall not be used to manage a router. When routers are remotely configured, Secure Shell (SSH) is the preferred management protocol.

IT security Staff shall ensure:

* Formal router hardening procedures are in place.
* Formal testing procedures are followed whenever configurations change.
* Router passwords are long and complex. Default passwords and configurations are changed on all routers.
* Routers are patched and updated in a timely manner. Documentation and procedures ensure that software updates and maintenance procedures are performed by authorized personnel.
* Routers are under support contract with appropriate response time guarantees and/or replacement routers are immediately available.

# 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 IT Staff that manage ABC Company’s routers and switches.

**Policy History**

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

**References:**

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(4), 164.312(a)(1)

ISO 27001:2013 6.1.3(b), A.9.1, A.9.4.1, A.12.1, A.12.4, A.12.6, A.13.1.3

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 AC-4, RA-3, RA-5, SC-7, SI-2, SI-5

NIST Cybersecurity Framework ID.RA-1, PR.AC-3, PR.AC-5, PR.DS-1-2, DE.DP-2, RS.RP-1

PCI 1.1-3, 1.5, 11.1