Domain Controller 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

ABC Company’s Information systems are critical to the continued operations of essential business processes. Domain Controllers (DC) are an essential component of ABC Company’s network.

# II. Purpose

Domain controllers, as well as backup domain controllers, are central to the security of all devices on that network and must be protected. The actions necessary to secure domain controllers are listed in this policy.

# III. Scope

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

# IV. Policy

The domain controller function is incompatible with other functions such as web server, mail server, ftp server, or mail client that can increase the risk of compromise to an unacceptable level. As a result, domain controllers shall be established on a dedicated device.

Domain controllers shall have restricted Internet access. In addition, the domain controllers shall have limited communications with specific devices (or an IP range if not practical to individually list the devices) on the ABC Company network.

Domain controllers shall deny access to unknown machines on the Internet and network using either filtering, firewall, or non-routed network addressing.

# V. Enforcement

Any Staff member 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 responsible for installing, maintaining, and securing domain controllers.

**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 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.310(d)(1)

ISO 27001 A.11.2, A.12

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 AC-3, AC-4(2), AC-5, CA-3, SC-2, SC-3, SC-20

NIST Cybersecurity Framework ID.AM-1-2, ID.BE-4, ID.GV-1, ID.RA-1, ID.RM-1, DE.DP-2

PCI 6.1-4, 6.7, 7.1-2, 8.1