# Domain Controller Policy

## Overview

Domain controllers perform mission critical authentication and directory services tasks for the enterprise and are an essential component of the [LEP] network. Domain controllers as well as backup domain controllers are central to the security of all devices on the network and must be isolated and protected.

## Purpose

Isolating services and functions on specific server instances serves to increase reliability and security for mission critical business functions. Domain controllers (regardless of primary or backup designation) perform critical directory service, role-based security, and authentication services for [LEP]. This policy limits the services that can be co-mingled on domain controller systems.

3. Scope

This policy applies to all [LEP] staff, users, and contractors that create, deploy, or support domain controllers and network services.

## Policy

Domain controllers shall be single function servers within the [LEP]. Because they house security account databases, group policy configurations, and role-based group security, their function is mission critical to the organization. All regular server hardening procedures as well as the following additional processes shall be followed when installing and configuring these specialized servers:

* Domain Controllers (DC) shall be established on a dedicated device or virtual machine.
* DC non-essential services, ports, and protocols shall be hardened and minimized to increase security and server stability. It is acceptable to collocate network services such as DNS, DHCP, and WINS on domain controllers based on their complimentary functions within the directory, name resolution, and authentication structure.
* A DC shall have restricted internet access to protect its account and security databases.
* A DC shall have limited communications with specific premise devices (or an IP range if not practical to individually list the devices) as dictated by the network architecture.
* All DC’s shall deny access to unknown machines on the private or public networks using either filtering, firewall, or non-routed network addressing.
* All local, remote and physical domain access shall be secured and changed with only limited access to network service staff for support

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP] internal processes and procedures. Examples of appropriate controls and documentation are:

* Documented DC server build processes and images.
* Internal DC configuration and asset management documentation, protocols and procedures.
* Patch logs containing DC name, patch installed, and date.
* GPO documentation showing hardening and security measures employed across the enterprise.

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff using information resources.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/04/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |