503 VPN Use And Security

503 VPN USE AND SECURITY

503.1 Use of ISP:

Employees with an approved VPN shall use their own internet service provider (“ISP”) for access to the Archdiocesan network.

Procedure:

A) The user is responsible for paying any fees associated with the user’s ISP.

B) A broadband ISP service with 256K speed or greater is recommended.

C) VPN access via America Online or dial-up services is not supported, due to technological and speed limitations.

503.2 Automatic Disconnections:

The Archdiocesan network will automatically disconnect VPN users after thirty minutes of inactivity. Pings or other artificial network process shall not be used to avoid disconnection.

503.3 Connection Limit:

VPN access may not extend beyond a 24-hour connection limit.

503.4 Expiration of VPN Access:

If a VPN account is not used for a period of six months the account will expire and no longer function.

Procedure:

VPN access is considered an “as needed” privilege, and account activity is monitored. If VPN access expires and is subsequently required, the user must make a new VPN request as described above.

503.5 Unauthorized Users:

Employees with VPN privileges must ensure that unauthorized users are not allowed to access the Archdiocesan network

503.6 Internet Access Prohibited:

To protect the Security of the Archdiocesan network, access to the Internet is strictly prohibited while connected to the VPN. To gain access to the Internet, a user must log out of the VPN connection.

503.7 Compliance with Computer Use and Internet Policy:

VPN users must read and follow the Division of Information Technology’s Computer Use and Internet Policy, available here.