Remote Access Tools Policy

1. Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include Skype, GoToAssist, TeamViewer, TightVNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the Diocese network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on Diocese computer systems.

2. Purpose

This policy defines the requirements for remote access tools used at The Catholic Diocese of Columbus.

3. Scope

This policy applies to all remote access where either end of the communication terminates at a Diocese computer asset

4. Policy

All remote access tools used to communicate between Diocese assets and other systems must comply with the following policy requirements.

4.1 Remote Access Tools
The Diocese provides mechanisms to collaborate between internal users, with external partners, and from non-Diocese systems. The approved software list can be obtained from the Technical Services Department. Because proper configuration is important for the secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

   a) All remote access tools or systems that allow communication to Diocese resources from the Internet or external partner systems must require authentication.
   b) Remote access tools must support the Diocese application layer proxy rather than direct connections through the perimeter firewall(s).
   c) Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Diocese network encryption protocols policy.
   d) All Diocese antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard Diocese procurement process, and the information technology group must approve the purchase.

5. Policy Compliance

5.1 Compliance Measurement
The Technical Services team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru's, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Technical Services Team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies, and Processes

None.