

# Remote Access Policy

## 1. Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases, this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of The Catholic Diocese of Columbus' policy, we must mitigate these external risks the best of our ability.

## 2. Purpose

The purpose of this policy is to define rules and requirements for connecting to Diocese networks from any host. These rules and requirements are designed to minimize the potential exposure to the Diocese from damages which may result from unauthorized use of Diocese resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Diocese internal systems, and fines or other financial liabilities incurred as a result of those losses.

## 3. Scope

This policy applies to all Diocese employees, contractors, vendors and agents with a Diocese-owned or personally-owned computer or workstation used to connect to the Diocese network. This policy applies to remote access connections used to do work on behalf of Diocese, including reading or sending an email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Diocese networks.

## 4. Policy

It is the responsibility of Diocese employees, contractors, vendors and agents with remote access privileges to Diocese corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Diocese.

General access to the Internet for recreational use through the Diocese network is strictly limited to Diocese employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the Diocese network from a personal computer, Authorized Users are responsible for preventing access to any Diocese computer resources or data by non-Authorized Users. Performance of illegal activities through the Diocese network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Diocese networks to access the Internet for outside business interests.

For additional information regarding Diocese's remote access connection options, including how to obtain a remote access login, antivirus software, troubleshooting, etc., contact the Technical Services department.

## 4.1 Requirements

- 4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.
- 4.1.2 Authorized Users shall protect their login and password, even from family members.
- 4.1.3 While using a Diocese-owned computer to remotely connect to Diocese's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- 4.1.4 Use of external resources to conduct Diocese business must be approved in advance by the Technical Services department and the appropriate business unit manager.
- 4.1.5 Personal equipment used to connect to Diocese's networks must meet the requirements of Diocese-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to Diocese Networks*.

## 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 inspection, and will provide feedback to the policy owner and appropriate business unit manager.

### 5.2 Exceptions

Any exception to the policy must be approved by Remote Access Services and 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

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods and acceptable use of the Diocese network:

- *Acceptable Encryption Policy*
- *Acceptable Use Policy*
- *Password Policy*
- *Third Party Agreement*
- *Hardware and Software Configuration Standards for Remote Access to Diocese Networks*