**Report on Installation of VPN Connections for Achieve PCs**

**Objective:**

The goal of this installation project was to establish VPN connections across various systems in the Achieve office environment by ensuring proper networking and connectivity from different devices to the VPN server. This included computers, iMacs, laptops, and network infrastructure components.

**Installation Overview:**

The process involved a combination of physical infrastructure work, including the installation of Ethernet cables, network adapters, Fiber optic connections, and the configuration of devices to ensure VPN access. The key steps in the installation were as follows:

**1. Ethernet Cable Installation:**

* **Location:** Camera Room to Computers in Achieve Area
* **Work Performed:**
  + Laid Ethernet cables from the camera room to each computer within the Achieve area. These cables were intended to provide wired network access, essential for stable VPN connections.
  + Ensured that each computer had a direct wired connection to the internal network, which would be routed through the VPN gateway for secure external communication.

**2. Network Adapter Installation in Archive Computers:**

* **Location:** Archive Section
* **Work Performed:**
  + Installed additional network adapters into the desktop computers in the Archive section. These adapters were necessary to connect the second Ethernet cable that would facilitate VPN connections.
  + Connected the second Ethernet cable from the newly installed network adapter to the VPN gateway, enabling secure communication with the external network.

**Images**

**3. USB Network Adapters for iMacs and Laptops:**

* **Location:** Office Workstations
* **Work Performed:**
  + Connected USB network adapters to the iMacs and laptops. These adapters were essential for providing an additional Ethernet port to support the second connection for VPN.
  + Routed the second Ethernet cable from the USB adapters to the VPN network switch, ensuring that these devices could also access the VPN.



**4. Fiber Optic Setup:**

* **Location:** Server Room and Production Area
* **Work Performed:**
  + **Identifying Fiber Ports:** Identified the Fiber ports on the patch panel that were running from the production area to the Fiber home in the server room.
  + **Fiber to Ethernet Conversion:** Connected Fiber patch cables from the Fiber home to the Fiber converter, which converted the Fiber optic signal to Ethernet for compatibility with the VPN switch.
  + **VPN Switch Connection:** The Ethernet cables from the Fiber converter were then connected to the VPN switch, establishing the secure VPN network to handle traffic.

Images

****

**5. Fiber Home to Production and Camera Room Link:**

* **Work Performed:**
  + The Fiber optic connection from the Fiber home in the server room runs directly to the production Fiber patch panel.
  + Another Fiber converter was connected at this location, converting the Fiber signal back into Ethernet for integration with the internal network.
  + The Ethernet connection from the Fiber converter was routed to the camera room to ensure that all locations within the network had access to the VPN service.

**6. Testing and Validation:**

* Testing is not yet done

**7. Conclusion:**

The installation of VPN connections for Achieve PCs was successfully completed. All required devices, including desktop computers, iMacs, laptops, and network infrastructure, were connected to the VPN with secure and reliable Ethernet and Fiber optic connections. The VPN switch is now functioning as expected, enabling secure communication for all connected devices across the network.

The installation team ensured that all components, both hardware and software, were configured appropriately to handle the new VPN infrastructure. The work was completed within the specified time frame, and the network is now fully operational.

**8. Recommendations:**

* Regular monitoring of VPN performance is recommended to ensure optimal bandwidth and connection stability.
* Periodic checks on the Fiber converters and network adapters will help maintain consistent performance.
* It is advised to conduct routine security audits to ensure that the VPN network remains secure against any potential vulnerabilities.