Remote Access Requirements

Revised: March 2025

As part of the offerings of the AoA IT department, remote access into the organization's network is provided to Chancery employees, consultants, independent contractors and volunteers who would like to take advantage of working from outside of the office. Whether or not the access includes working with AoA proprietary data, all remote work must be approved by the user's management. Prior to being granted this access, there are several requirements that employees will need to acknowledge and accept:

Personal Equipment / Infrastructure used to gain access to the Chancery systems must meet certain criteria. Both AoA-issued equipment along with any personal equipment used to gain remote access must meet the following minimum requirements:

- Desktop Computer or Laptop with the following minimal operating systems:
    - Windows 11 Pro. If another version of Windows 11 is being used (i.e. Windows 11 Home), a paid-version of an anti-virus program must be loaded onto the system in use and kept updated with the latest signature files. Examples of such programs would be Webroot; TrendMicro, ESET, etc. Only AV modules are necessary – no extended versions containing add-ins like VPS or firewalls are required.
    - Windows 10 (any version). The above separate paid-versions of an AV program being loaded would apply to any version of Windows 10. Please note, Windows 10 will no longer be supported after September 2025.
    - Apple-based desktop or laptop with an operating system running on version macOS 12 (Monterey) or later. Paid-versions of an AV program are also required to be loaded on a macOS device.
- The operating system on the device being used (above) is being continually updated with the latest patches distributed by Microsoft (or Apple).
- High speed internet with minimal transfer speeds of 100 Mb down and 50 Mb + up. This can be checked by performing a SpeedTest from your browser at https://www.speedtest.net/
- Internet/network connection MUST be secured (especially if Wi-Fi). This pertains to home as well as shared access (i.e. WiFi connection at a coffee house; airport; etc.) If connecting to a public WiFi (with a password – no open access), using a personal VPN service is preferred. Examples would be NordVPN, ProtonVPN, EspressVPN, etc.
- Actual device hardware specifications should meet or exceed the following:
    - CPU i5 or better
    - RAM 8GB (16GB or higher preferred)
    - 500GB hard drive or larger (SSD or NVMe preferred)
    - Network capability (minimal WIFI - though cabled ethernet RJ-45 is always preferred)
    - Webcam etc. (for virtual meetings)

Note: You may be asked to prove these requirements are in place at any time by producing your equipment or submitting a screenshot.

Safe and private computing procedures should be followed at all times while accessing or handling AoA-based data. These procedures include (but are not limited to) the following:

- Access will be limited only from the device or devices approved and referenced in the above section. Local passwords on the equipment should be enforced and AoA-based information should never be left on-screen while device is unattended.
- Printing of documents, if not disabled, is prohibited on printers outside of the Chancery unless approved by the department director.
- Personal e-mail accounts (i.e. Gmail; Hotmail; Yahoo; etc.) are never to be used to disseminate AoA-based data or information. Only archatl.com based e-mails should be used.

    Note: The use of personal email accounts could potentially be subpoenaed and searched during the discovery process of a litigious event.

Links with additional information:

Guidelines for working remotely

https://archatl.zendesk.com/hc/en-us/articles/360050288531-Guidelines-for-Working-Remotely

***Remote Access Guidelines** (AoA Employee Policy Manual)*

https://www.paperturn-view.com/us/archdiocese-of-atlanta/2020-archdiocese-of-atlanta-employee-policy-manual-september-2020?pid=MTE112592&p=49&v=13.1

If you have any questions, please feel free to contact the IT Department by submitting a helpdesk ticket at https://help.archatl.com/. Otherwise, by my signature, I agree to the policies and procedures contained within this document.