THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

Remote Access Requirements

Revised: January 2023

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 Windows 10 or above. If an Apple-based desktop or laptop is being used, it must contain an operating system running on version macOS 12 (Monterey) or later.
- The operating system on the device being used (above) is being continually updated with the latest patches distributed by Microsoft (or Apple). *Example: Windows 10 version 21H2 or later.*
- The device has at least 8GB RAM along with ample hard drive storage available
- High speed internet. A recommended minimum would be 200 Mb + down, 100 Mb + upload speed (NO dial up or DSL)
- 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, Surfshark, etc.
- A paid-version of an anti-virus program must be loaded, in use and updated with the latest signature files. Examples would be Webroot; TrendMicro, ESET, etc.

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, should not be performed on printers outside of the Chancery.
- Personal e-mail accounts (i.e. Gmail; Hotmail, 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

By completing the section below and submitting this document, both the user (consultant, contractor or volunteer) and supervisor are acknowledging that the user has fulfilled the minimal requirements necessary to access the AoA network/services remotely understanding that there may be possible penalties for not adhering to these requirements.

> **NOTE:** For those users who are unable to create/use the Digital ID feature for the fields requiring a signature, you are encouraged to simply print this document, complete it by hand and submit a scanned (legible) copy back through a help desk ticket.
>
> You can find more information and instructions for creating Digital IDs on

Signature: ____

Name (Please Print): ____________________________________ Date: ____________

Phone Number: __________________________

Supervisor's Signature: ____

Supervisor' Name (Please Print): ________________________________ Date: _________

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