AREA AGENCY ON AGING OF PASCO-PINELLAS, INC.

POLICY:	**Email Encryption Policy**	**POLICY #:**	**ADLAN-1131**
DEPARTMENT:	**ADMINISTRATION**	**PROGRAM:**	**LAN**
DEVELOPED DATE:	**02/13/2026**		
REVISION DATE:			

Purpose

The purpose of this policy is to ensure that all sensitive and confidential information transmitted via email is protected from unauthorized access. This policy outlines the mandatory procedures for encrypting emails sent from our Office 365 environment to both internal and external recipients.

Scope

This policy applies to all employees, contractors, and third-party agents who send emails containing sensitive, proprietary, or confidential information on behalf of [Company Name] (hereinafter referred to as "AAAPP")

Policy

AAAPP utilizes Microsoft's native email encryption built into the Office 365 environment. All emails are transmitted over encrypted connections. However, to ensure the content of the email cannot be read if intercepted, senders must apply specific encryption methods based on the sensitivity of the data and the recipient.

Encryption Methods

Automated Encryption (Default Method)

To ensure ease of use and compliance, AAAPP has enabled automated encryption triggers. The automated encryption is to be used when sending Protected Health Information (PHI), Personally Identifiable Information (PII), or financial data externally. To trigger the encryption, users should include the word ENCRYPT in the subject line of the email. The system will automatically apply Microsoft 365 Message Encryption to the email before it is sent.

Manual Encryption Options

For greater control over the security of the message, senders must manually select the appropriate sensitivity label in Microsoft Outlook.

> ***AAAPP – Encrypt Only*** is to be used when the email is being sent outside of the AAAPP network and requires standard encryption to protect the data from being read by anyone other than the intended recipient. To trigger the inscription, users should select the "Sensitivity" button and choose AAAPP-Encrypt Only option. The email will appear directly in the inbox with a padlock icon and a label indicating it is encrypted for

Microsoft Users (Outlook/Hotmail/Office 365). **Non-Microsoft Users (Gmail, Yahoo, etc.)** will receive a notification email with a link to a secure web portal. The identity of the user to be verified with a one-time passcode sent to their email address. The user can access the email once verification is complete.

AAAPP – Confidential (Read-Only) is to be used when sending sensitive information to any recipient (internal or external) where user needs to deter the recipient from distributing the content further. To trigger this inscription, users should select the "Sensitivity" button and choose AAAPP-Confidential (Read-Only). The AAAPP – Confidential (Read-Only) label enforces additional usage restrictions such as: 1. The email cannot be forwarded; 2. The content cannot be printed; 3. The email cannot be copied and pasted; 4. The email is blocked from being shared via screen capture applications.

Compliance and Exceptions

It is the responsibility of the sender to classify the information correctly and apply the appropriate encryption.

- Failure to encrypt sensitive data is a violation of this policy and may result in disciplinary action.
- If a user believes an email requires encryption but the automated trigger did not work, the user must exercise the manual labeling options described above.
- Users should **not** send sensitive information (such as Social Security numbers or bank details) in the body of a standard, unencrypted email.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.