Allegany College of Maryland

ELECTRONIC SIGNATURE GUIDELINES AND PROCEDURES

Adopted date 8/16/2021
Revised Date 10/3/2022
Approved by Board of Trustees Date 8/16/2021
Implementation Date 8/16/2021
Type of Policy: Operational

BACKGROUND AND PURPOSE

To establish procedures for using electronic signatures (e-signatures) in connection with Agreements and other documents (i.e., proposals, grants, contracts, statements, notices, resolutions, memoranda of understanding, licenses, etc.) used to conduct official Allegany College of Maryland (ACM) activities. These guidelines implement the ACM Policy Regarding Electronic Signatures.

I. APPLICABILITY

As organizations move away from paper documents with ink signatures, the ability to sign electronic transactions and documents for business, financial, or other reasons is important, if not essential. The guidelines and procedures described herein apply to all users seeking to utilize e-signatures in connection with official ACM agreements, contracts, approvals and other documents.

II. General Guidelines

1. As set forth in the Policy, to use an e-signature, an individual must have the authority to undertake the action made by the e-signature. Only specific individuals identified by ACM have authority to sign agreements, contracts and other documents on behalf of ACM. Only those individuals and their authorized designees have authority to affix e-signatures on agreements, contracts and other documents within the signatory's authority.

2. A user's right to use an approved method to create signing documents and to build associated workflows for accepting e-signatures does not of itself grant signature authority to the user. Therefore, no such user may sign agreements, contracts or other documents on behalf of ACM unless they otherwise have authority to do so.

3. All parties involved in an e-signature transaction must consent to the use of an electronic record prior to a signing event.

4. The President will designate "signature authority" to the Vice Presidents who can in turn delegate based on operational necessity. However, even in these cases if the agreement is for something new or involves a high dollar amount, the Vice President would need to give express approval for signature.

5. Adobe Sign will be used as the primary method for obtaining electronic signatures. Other methods can be used if approved by the department Dean, or Vice President and vetted by the Information Technology Department.

6. All College employees accepting legally-binding documents from another party are accountable for properly and appropriately ensuring signature authenticity and determining the reliability of the documents. This includes ability to retain the e-signature and associate it with the transaction (document or record) it authenticates.

7. These guidelines will be revised to reflect changes in e-signature policy and procedures as transactions, or processes for accepting and using e-signatures change.

III. Signature Management

An e-signature may be used with the same force and effect as a signature affixed by hand, unless specifically provided otherwise by College policy, State or Federal law. A signature on a document identifies the signer and signifies that the signer and/or the entity authorizing the signature understands and intends to carry out whatever is stipulated in the signed document or record. The act of signing alerts the signer that they may be making a legally-binding commitment.

In order for an e-signed document or record to be considered valid, it must satisfy the following signing requirements:

- The method of signature must be authorized and accepted by law and policy.
- The identification and authentication of the signer must be possible based on the e-signature.
- The signer must intend to sign the document or record.
- The e-signature must be reliably associated with the document or record.
- The signed document or record must have integrity (e.g., legibility, no indication of alteration, securely and reliably stored, and with limited access by authorized persons).

Acceptable methods used to create an electronic form of signature that may be used by a signer includes, but is not limited to:

- The signer logs into a College resource (e.g., Colleague, Self-service, etc.) and clicks an agreement button or checks an agreement box.
- The signer types their name or enters a unique identifier which ties them to a transaction.
- The signer utilizes a graphical image of their handwritten signature that is affixed to an electronic document or record.
- The signer utilizes a custom signature (e.g., a typed signature converted to cursive using an appropriate font) to sign an electronic document or record.
- The signer signs using a computer input device such as a digital pen or pad.

As a general rule, signatures must be the act of a specific person. To be enforceable, there must be proof that the signer actually signed the document or record. The level of confidence required by a given identification and authentication process should be based on the level of business impact or loss if the alleged signer later denies their involvement in the transaction. Actions should be taken to preserve the accuracy and completeness of all e-signed documents and to ensure that no unauthorized alterations
are made to these records either intentionally or accidentally.

IV. Responsibilities

The President, Vice Presidents, or designees are responsible to:

1. Approve “signature authority” for the use of e-signatures.
2. Act on requests for the use of e-signatures and when necessary, approve documents that can be signed electronically.

Operational Units (departments) are responsible to:

1. Ensure that only individuals with signature authority are signing documents with e-signatures on behalf of the College.
2. Ensure that use of an e-signature complies with law and College policies.
3. Guide users within the unit in creating and maintaining document templates.
4. Assist Senders in establishing signatories, routing, and document management.
5. Properly store, secure and maintain electronic documents and records.

Information Technology is responsible to:

1. Review and recommend tools for e-signature activities.
2. Provide technical guidance for resolving e-signature issues.
3. Manage select e-signature software, updates, security, licensing and other
4. related technology duties.

V. Assessment and Risk Analysis

The following factors must be considered when determining whether to permit the utilization of an e-signature:

1. Potential efficiencies of the use of e-signatures.
2. Potential risks of the use of e-signatures.
3. Ability to correctly maintain documents or records.
4. Ability to accurately tie an e-signature(s) to a transaction and person(s).
5. Applicable College policies, State or Federal laws.

VI. Restrictions

E-signatures may not be used or accepted for any of the following types of transactions:

- Willed body agreements.
- Transactions which require a notarized signature, sworn signature, witnessed signature, an apostille, or a recorded document.
- Assumption of risk and release of liability documents for high risk transactions or situations.
- Administrative or academic documents held to a stricter standard for signatures as identified by a department's operating procedures.
- For purposes forbidden by State or Federal law.

VII. Record Retention

The E-Sign Act requires an organization to maintain electronic records accurately reflecting the information contained in applicable contracts, notices or disclosures and that they remain accessible to all persons who are legally entitled to access for the period required by law in a form that is capable of being accurately reproduced for later reference. Operational units using e-signatures must understand document retention requirements for the kinds of documents used by the department to conduct College business.

Documents that reach end-of-life can be properly disposed of. Electronic documents containing PII require special care and should be permanently deleted (shredded if paper copies exist). When disposing of documents be sure to search for copies of the document and delete them as well. When removing electronic documents, they can end up in a wastebasket and may be retained for a period of time. Be sure to clear the trash after document deletion.

VIII. Exceptions

Exceptions to these guidelines and procedures must be approved in writing by the President of the College, an area Vice President (VP) or designee. The request must be signed/e-mailed to the approver by the Department Head or designee.

IX. Violation and Sanctions

Employees or Affiliates who do not comply with these Guidelines and Procedures may be subject to disciplinary action, lose the privilege of using e-signatures, or have ACM fiscal authority terminated.

X. Process Owner

The office of the Dean of Information Technology, in consultation with The Vice President of Finance and Administration, shall be responsible for maintaining these guidelines and procedures.

XI. Procedures

1. How to Access Adobe sign

a. To Login, CTRL click or paste in browser: https://secure.echosign.com/public/login
b. The user will be directed to the "Login to Adobe sign" page.
c. Enter in the Email and Password.
d. Click the "Sign In" button.
e. The user will arrive at their Adobe sign home page.

2. Adobe sign Security Roles

a. **Signer** - All Adobe sign users have basic Signer rights. A Signer has the ability to open, view and sign any Adobe sign document that has been sent to them.

In order to receive the right to have additional functionality with Adobe sign documents, the user must be assigned one of four "security roles": i.e. either "Sender," "Group Admin," "Account Admin", or "Privacy Admin".

b. **Sender** - A Sender has the ability to upload any document and configure it for Adobe sign. A Sender also has the ability to send the document for review, data input, and e-signature by authorized signers.

c. **Group Admin** - Group Admins have the authority to override the account level settings and configure the group they are in to better reflect the work product of the group. This includes most account level settings, including branding, default signature and verification settings, workflows, templates, etc.

d. **Account Admin** - Account admins control the settings at the account level. Account level settings are automatically inherited by all groups in the account unless the group level admin overrides them. At the account level, admins can configure settings like federated sign in, Account level branding, templates, and workflows.

e. **Privacy Admin** - The Privacy Admin is an extension of the Account admin role. Privacy admins must first be an Account admin to add the additional toolset. The privacy admin has the authority to fully delete agreements and userIDs from the Adobe Sign servers (per GDPR requirements).

Further information and training for all security roles can be found on the Adobe sign help portal. Adobe sign webpage.

3. How to Receive an Enhanced Security Role

a. In order to be assigned a higher-level security role, the user must do the following:

i. Complete the Adobe sign Online Training. https://helpx.abobe.com/sign/how-to/customer-success-resources.html
ii. Click "WATCH TUTORIALS"
III. Select "BEGINNER" or "EXPERIENCED"
iv. Senders – Complete Sending & Signing for new users
v. Admins – Complete Sending & Signing Plus Administration for new admins.

b. Complete and submit to Helpdesk a request for Adobe Sign Security (Sender or Admin).
c. The request must be approved by the requester's supervisor and the area Dean or VP.

4. **How to Create a New Template**

   a. The user can follow along with the "Create a shared document template" tutorial for template creation instructions. The below link will provide access to this tutorial.
      i. https://helpx.adobe.com/sign/tutorials.html
   b. Information Technology may, upon request, help with template creation on behalf of an Operational Unit. In order to request such assistance, the Operational Unit must do the following:
      i. Submit a Helpdesk request for assistance.
      ii. If required, provide a prototype document for upload in DOCX or PDF format.
   c. If HIPAA, FERPA, or personally identifiable information will be included in the template, ITD will conduct additional review and may request additional information from the requester.
   d. A copy of any template created by a user must be approved by the Department Head, Dean, or area VP prior to use.

5. **Definitions and Terms**

Operational Units - Departments, and affiliates of ACM.

Authorized Affiliate Employee - Person employed by an entity that has a relationship with ACM authorized by the Board of Trustees or by law, and other affiliated foundations, recognized incorporated alumni associations, recognized affiliated business entities. An Authorized Affiliate Employee is responsible for the administration and reporting of ACM resources.