

**Policy Number/Title:** 1.3.1.02 Electronic Records and Signature Policy  
**Effective Since:** 04/05/2020  
**Last Revision Approved:** 04/01/2020  
**Responsible Office:** General Counsel; Office of the President

---

## 1. Scope:

This campus-wide policy applies to all Winthrop-affiliated employees, whether temporary or permanent, paid or unpaid, as well as students, associates, volunteers, and/or anyone conducting electronic business, transactions, or other official activities for, or in association with, the University.

## 2. Definitions:

**Computer Program.** A set of statements or instructions used directly or indirectly in an information processing system to bring about a certain result.

**Digital Signature.** Digital signatures are a subset of electronic signatures and use the PKI (Personal Key Infrastructure) where you create a public and private key and you have a digital certificate assigned to you by a certificate authority. Approved University electronic signatures use this format to ensure validity of signatures.

**Electronic.** Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

**Electronic Record.** A record created, generated, sent, communicated, received, or stored by electronic means.

**Electronic Signature.** An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Digital Signatures are a type of electronic signature.

**Individual.** A single natural person; one human being.

**Information.** Data, text, images, sounds, codes, computer programs, software, databases, or other forms for the communication or reception of knowledge.

**Information Processing System.** An electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.



Person. An individual, corporation, business trust, estate, trust, partnership, Limited Liability Company, association, joint venture, governmental agency, public corporation, or other legal or commercial entity.

Record. Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form

Transaction. An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Wet Signature. Any physical mark on a document created by a person. The traditional handwritten application of a signature, or other self-identifying mark, with ink to a document.

### **3. Policy:**

Winthrop University adopts the use of electronic agreements and signatures as allowed by the South Carolina Uniform Electronic Transactions Act (“UETA”) (2004 S.C. Code Ann. §06/26/2010 et seq.) for the conduct of business and academic operations.

#### **Electronic Records:**

Except as specifically excluded by the UETA or this policy, all related procedures, forms, and guides that the University is required to maintain under the South Carolina Public Records Act (S.C. Code Ann. §01/30/2010 et seq.) or any other provision of State law may be stored and maintained in an electronic format, provided that all State laws, rules, regulations, and guidance of particular application to each type of class of records are observed by the data retention office of the university.

#### **Electronic Signatures:**

There are four elements to a valid **electronic signature**:

Use of a signature unique to the signer

Parties agree to conduct transactions by electronic means

A clear intent to sign

Association of the signature with the signed record.

When determining if the conditions are present, the University will examine the authentication of the signer, non-repudiation by the signer, and integrity of the **record**.



## Standards for **Electronic Signatures**

General Rule: **Electronic signatures** accepted by the University must meet the standards contained in this policy in addition to any other standards that may be imposed by a law of specific application to the particular **record** that is being signed.

Use of signature unique to the signer:

The **electronic signature** must uniquely identify the signer, be under the reasonable control of the signer, and be unlikely of use by any unauthorized entity.

Using a secure University information system with proper and valid credentials, will serve as an **electronic signature** in most cases for internal documents that can only be accessed through that system. This electronic signature service is to be used by only those with signature authority.

Employees which need to electronically sign documents which have an external party will need to apply a specific type of **electronic signature** known as a digital **signature** through an authorized vendor.

The party using the **electronic signature** bears the responsibility for maintaining control and security of the relevant “sign, symbol, or process” signifying the signature.

The party using the **electronic signature** shall not share access credentials with any other party at any time. In the event the access credentials, or the electronic signature, are compromised, the party using the Electronic Signature must immediately provide notification of such compromise.

Security over the methodology for assigning the means of creating the **electronic signature**, and for maintaining the confidentiality of the **electronic signature** received reside with the Department of Computing and Information Technology with approval from Information Security.

Intent to Sign: The act of applying the **electronic signature** to a record must be intentional.

Intent will be inferred by the contents of the document or **record** and the facts and circumstances surrounding the **transaction**.

The University requires a prior **agreement** with the signer or clear and unambiguous notification in, or accompanying, the transactional document or subject **record** stating that the execution of the **transaction** or transactional document or subject **record** stating that the execution of the **transaction** or authentication of the **record** can or must be



effected by an **electronic signature**.

Certain types of documents are required to be kept in a paper format or are required to have wet signature.

The use of **electronic signatures** or **electronic records** is not allowed when in contradiction with Winthrop policies and procedures, or prohibited by federal or state laws or regulations.

Specific documents for which electronic documents or signatures are prohibited as the official record of the University.

Resolutions approved by the Board of Trustees

Any documents or reports required for institutional accreditation purposes or accreditation reports.

Any documents related to long-term donor gifts to the University.

Any deed related to the acquisition or disposal of real property.

Documents that need to be notarized.

The final approval of any **electronic signature** method will be by the President, with the recommendation of the Vice President for Finance and Business and General Counsel.

**Electronic signature** documents must follow the same retention policy as set forth in the General Records Retention Schedule for State Colleges and Universities as determined by the South Carolina Department of Archives and History.

**Records** must remain accessible in a form that can be reproduced by anyone entitled to access the **record**.

#### **4. Procedures:**

##### **A. University Documents for which electronic signatures are currently prohibited:**

1. Any document for which the use of an electronic signature is prohibited by law.
2. Resolutions approved by the Board of Trustees
3. Any documents or reports required for institutional accreditation purposes or accreditation reports.



4. Any documents related to long-term donor gifts to the University.
5. Any deed related to the acquisition or disposal of real property.
6. Documents that need to be notarized.
7. Immigration forms or reports.

**B. Methods to show Intent to Sign**

1. Anyone using an approved method to apply an electronic signature to an internal document while signed in with proper University credentials is deemed to be doing so with deliberate intent.
2. For contracts or other agreements with external parties the determination of intent can be evidenced by one or more of the following methods:
  - a. There is a prior agreement between the University and the external party allowing the use of electronic signatures. A copy of this agreement must be kept with the signed document for the applicable retention period. (Example: MOU regarding internship placements with a host company or institution that allows for electronic amendments to add additional academic programs to the placement agreement).
  - b. There is a clear and unambiguous notice or accompanying document to the agreement which states that the parties will sign electronically. A copy of this agreement must be kept with the signed document for the applicable retention period.
  - c. Acquiring access to one of the University's approved vendor's electronic signature methods and then applying an electronic signature. (Example: signing into Adobe Sign and then electronically executing an agreement).

**C. Requirement of additional attestation**

1. The completion of an additional attestation is required for some types of documents. If this is required the attestation, or additional certification, must be retained with the electronic agreement. (Examples: engineering or tax documents).
2. If you are unsure as to whether a document requires an additional attestation, please consult the Office of General Counsel.

**D. How to apply an electronic signature**



1. Employees are responsible for creating their own unique electronic signature and keeping access secure. Access to, and credentials for, electronic signature systems are not to be shared with others under any circumstances.
2. Employees and students who have accessed a University information system with proper credentials, can acknowledge their agreement electronically for some internal forms. This type of electronic signature is only valid for documents that can only be accessed while signed into a University system. (Examples include: PAF, University Marketplace, facility work order requests.)
3. Individuals who have created an account to access a University system or vendor system for the purposes of conducting electronic transactions can acknowledge their agreement electronically. (Examples include: event tickets, University Marketplace).

#### **E. When to use a digital signature**

1. Digital signatures or wet signatures must be used for documents or agreements with parties external to the University.
2. Some internal forms may also require a digital signature.
3. Only approved University vendors can be used for the application of digital signatures.
4. Digital signatures require the establishment of a private key to apply the signature.
5. Private keys must be protected from improper use and may not be shared.
6. There is a step-by-step guide for each University vendor in the guide sections for setting up a digital signature.
7. When an external party is requesting a document to be signed through a non-approved vendor:
  - a. Submit a request to have the vendor approved for digital signatures, or
  - b. Request the external party to change the signature request to an approved vendor.

#### **F. Information security requirements**

1. Protection of electronic credentials
  - a. The electronic signature account must be assigned to a specific user.



- b. Generic/group accounts cannot be used for electronic signatures.
  - c. Employees must not share their electronic signature, or credentials allowing access to their electronic signature, with others under any circumstances.
2. Compromised passwords or accounts
    - a. If a user suspects that their electronic signature has become compromised in any way, the user should immediately change their password. The user should then contact the Information Technology Service Desk and Information Security Analyst and provide details on why they think their signature has been compromised, how it may have happened, and who may have accessed the user's electronic signature, if known or suspected.
    - b. Employees who knowingly, or negligently, fail to protect their University credentials or electronic signature, or who fail to timely report unauthorized use of same, may have their authority to sign documents revoked.

**G. Methods to create documents which require a digital signature.**

1. Vendors that are currently under contract with Winthrop University can be used to create documents which contain digital signatures. Employees will need to see the separate guides for each approved vendor for specific instructions.
2. Employees who need authorization to set up documents in a vendor system which requires electronic signatures must have their supervisor complete the request. A link to the form is located in the guide section.
3. Documents which contain digital signatures may have a small fee associated with them. Those will be charged back to the department that initiated the document requesting signatures.

**5. Resources:**

**Approved vendors for creating documents with electronic signatures:**

- AdobeSign

**Approved vendors for applying electronic signatures:**

- DocuSign
- Digisign

If there is a vendor that not on the list, a request can be made to have them approved in the



forms section.

### **How to set up a digital signature in Adobe:**

- Launch Adobe Acrobat, then click "Document" in the main menu bar.
- Select "Security Settings" from the drop-down list. The Security Settings window opens.
- Click "Digital IDs" on the left side of the window.
- Click the "Add ID" button, then select the checkbox next to "Create a Self-signed Digital ID for Use with Acrobat."
- Click "Next," then select the checkbox next to "New PKCS#12 Digital ID File."
- Click "Next" and enter your personal information into the appropriate fields. For example, enter your name and your email address. Do not edit the settings, such as the "Key Algorithm" drop-down box. Click the "Next" button. The default location of the digital signature file is in the "File Name" box. If you want to change the location, click "Browse" and then go to the location where you want to save the signature file.
- Enter a password for the digital signature in the "Password" box. Re-enter the password in the "Confirm Password" box. Click the "Finish" button to complete the process.

### **How to sign documents with a digital signature.**

<https://acrobat.adobe.com/us/en/sign/how-to/create-digital-signature.html>

### **How to collect electronic signatures with Adobe Sign:**

- Open a PDF file in Acrobat DC.
- Click the Fill & Sign tool in the right pane.
- Add a recipient:
- Enter an email address and add a custom message if you want. Then click "Next."
- Create your form and signature fields:
- Either click to accept automatically-detected form and signature or drag and drop your own from the right pane.
- Send your form:
- Click "Send." Each recipient will receive an email with a link to e-sign instantly along with a copy of the signed document. Your copy will be stored securely in Adobe Document Cloud.

[E-Signature Vendor Approval Form](#)

[E-Signature Document Creation Request Form](#)

## **6. History of Revisions:**

03/08/2021      Minor Revisions

04/05/2020

Policy first established