THE OHIO STATE UNIVERSITY

Guide to Implementing Electronic Signatures

Office of Business and Finance
Office of the Chief Information Officer

Used in conjunction with the Electronic Signature policy
Issued: 09/01/2015

This document outlines the requirements and other important considerations that must be taken into account for units implementing electronic signatures at Ohio State in compliance with the Electronic Signature policy. Sections include:

- Phasing Out Handwritten Signatures – encourages use of electronic forms and work flows;
- Using the University-Approved Electronic Signature System – describes how to get started with the electronic signature system;
- Opting Out of Conducting Business Electronically – requirements for handling such requests from employees and non-employees;
- Transactions in Which Electronic Signatures Should Not Be Used – lists types of transactions that should continue to use handwritten signatures; and,
- Establishing New Systems with Electronic Signatures – lists requirements for establishing new electronic signature systems and defines the university-approved authentication method for electronic signatures.

Phasing Out Handwritten Signatures

Not all processes have full online systems built around them. Many processes still require a handwritten signature on a printed document (forms, contracts, offer letters, etc.). These completed paper documents are then scanned and uploaded into university transactional systems and/or are stored locally. The university-approved electronic signature system replaces the need for handwritten signatures. This enables the university to streamline its paper-based processes as either a short-term solution until a more permanent online system can be implemented, or as a long-term solution.

The key benefit of collecting signatures electronically (as opposed to, e.g., scanning and uploading documents signed by hand) is time savings. Processes that must wait for someone to return from a trip to sign something or that require signatures from multiple people will be completed in minutes or hours, instead of days or weeks, using electronic signatures. With this approach, processes that require input from individuals (e.g., hire data worksheet) collect the information in typed form, not hand-written form, reducing data entry questions due to illegibility. Electronically signed documents are already in electronic form (no scanning) and are stored electronically. This makes it easier to share documents with those who need access to them and it makes it easier to find specific documents since the information contained therein may be searchable. If a paper copy is ever needed, it is easy to simply print the document.

Units should discontinue using printed versions of documents to gather handwritten signatures, except when handwritten signatures are required by law (see Transactions in Which Electronic Signatures Should *Not* Be Used below). Instead, units should use electronic versions of those documents (Word, PDF, other common formats, etc.) to gather signatures electronically via the university-approved electronic signature system. Once the electronic signatures are complete, the resulting electronically signed documents can be uploaded into the appropriate university transactional systems (e.g., PeopleSoft HR/SIS/Finance, eRequest, eLeave, HR Action, AdvisingConnect, OSUMyChart, Epic, etc.) and/or stored electronically as needed.

Using the University-Approved Electronic Signature System

The university approved electronic signature system, DocuSign, enables university employees to send documents to individuals to sign electronically. **All university faculty, staff, and students are automatically set up with the ability to sign electronically and do not need to take any additional steps to be able to receive documents via the system.** Some university employees may be set up with additional access to the system that enables them to send documents out for electronic signature. Documents sent via the system can be signed electronically by both university and non-university individuals. Table 1, below, summarizes the different roles for the system and the process individuals must follow to gain access.

Used in conjunction with Electronic Signature policy
Issued: 09/01/2015

Table 1: Summary of System Roles and Processes

Role	Abilities	Request and Approval Process	Training Required?
Signer	Sign documents only	No request is needed. University individuals are automatically set up as signers through the university identity management system and use their name.n and password to log in and sign documents. Non-university individuals do not need a login/password to sign a document sent to them by an Ohio State employee; however, they may be required to enter a code sent via SMS/Text message or other method before they are able to sign.	No
Sender	What a signer can do plus send documents using predefined forms and templates only	University employee submits a request via http://my.osu.edu. Unit Senior Administrative Officer (or Senior Fiscal Officer) approves. Employee completes Institutional Data training and Electronic Signature Sender training. OCIO confirms training is complete then grants access and informs employee and approver.	Yes
Author	What a sender can do plus send custom/ad hoc documents; create and share predefined forms and templates with senders	University employee submits a request via access@osu.edu. The Unit Senior Administrative Officer (or Senior Fiscal Officer) and the Business and Finance Senior Director for Shared Services approves. Employee completes Institutional Data training and Electronic Signature Author training. OCIO confirms training is complete then grants access and informs employee and approver.	Yes
Administrator	Manage the DocuSign system and/or integrate DocuSign with other systems via API (OCIO only)	OCIO employees responsible for managing the DocuSign system and/or for integrating DocuSign with other systems via its API request administrator access directly from the Deputy CIO who approves. OCIO employees must complete both Sender and Author training plus administrative and, if applicable, API training before access will be granted.	Yes

Requesting Assistance

Signers needing technical assistance signing a document electronically may contact 8-HELP (8help@osu.edu), or contact the unit who sent the document to them originally. Senders and Authors needing assistance should contact 8-HELP who will immediately route their requests to the OCIO and B&F support teams.

Security and Additional Controls

When used as directed, the university-approved system provides reasonable assurance (1) of the authenticity of electronic signatures, (2) that the signatures will not be rescinded (the signer cannot make a legitimate or supportable claim they did not sign it), and (3) of the integrity of the electronically signed records. The proper use of this system also mitigates risks in cases when the electronic record to be signed contains internal, private, or restricted data as defined by the Institutional Data policy.

Some additional controls (e.g. a code sent via SMS/Text message in addition to the signature) are required for certain types of documents and/or certain signature processes. These controls are addressed in detail as part of the Electronic Signature Sender and Author training. Signers needing technical assistance with these should contact 8-HELP or the unit that sent the document originally.

Table 2: Summary of Two-Factor Authentication Requirements

Recipient	Type of Data	Log-in required	Two factor authentication required	Other Requirements
OSU email account	All data except restricted	Shib login	No	
OSU email account	Restricted	Shib login	No	The author is required to use the masking criteria and workflow the document such that the input of restricted data is last in the workflow when possible.
Non-OSU frequent user (e.g. vendors)	All data except restricted	DocuSign login	No	Account needs requested through OCIO
Non-OSU frequent user	Restricted	DocuSign login	Yes	Account needs requested through OCIO
Non-OSU infrequent user (e.g. new hire)	All data	N/A	Yes	

Records Retention

Once a document is complete, the unit must retain the resulting records in accordance with the university Records Retention Schedule, other university policies (e.g. Personnel Records, Travel, Procurement, etc.) and the Information Security Standards.

Opting Out of Conducting Business Electronically

As university processes are converted from handwritten signatures to the university-approved electronic signature system, employees, including student employees, acting within the scope of their employment, are expected to use it and may not opt out of conducting a transaction electronically. However, if an employee needs an ADA accommodation, handwritten signatures or other approaches recommended by the university ADA coordinator should be used.

Individuals and entities, excluding employees acting within the scope of their employment, may opt out of conducting a transaction electronically by providing written notice of the decision to opt out of conducting business with the university electronically per transaction. The written notice must be directed to the university employee responsible for the business relationship with the party. In such cases, handwritten signatures or other approaches recommended by the university ADA coordinator should be used. The notice to opt out should be retained with the record that was signed. Upon receipt of such notice, the university may reassess its interest in contracting with the party choosing to opt out, and retains the right to cancel the pending transaction, unless otherwise obligated by law or agreement.

The university may, at its discretion or as required by law, opt out of conducting a transaction electronically. In order to do this, the university employee responsible for the business relationship with the party must provide the party with written notice of the decision to opt out of conducting business electronically. In such cases, handwritten signatures should be used. The notice to opt out should be retained with the record that was signed.

Best practices on how to process requests to opt out are included in the Electronic Signature Sender training. Best practices on designing ADA accessible electronic signature forms and templates are included in the Electronic Signature Author training.

Transactions in Which Electronic Signatures Should Not Be Used

Electronic signatures should not be used for the following types of transactions (use a handwritten signature):

- Commercial paper, which includes paper checks and promissory notes (ORC §1303; UCC Article 3)
- Documents of title, for example a property deed, automotive title or bill of lading (ORC §1307; UCC Article 7)
- Documents relating to securities, for example a stock certificate (ORC §1308; UCC Article 8)
- Ohio Public Employees Retirement System forms
- Wills, codicils and testamentary trusts

The above exceptions do *not* include transactions involving the sale of goods or services or leases (see ORC §§ 1302, 1310; UCC §§ 2, 2A), for which electronic signatures *may* be used.

The university-approved electronic signature system may not be used to collect credit card numbers.

Establishing New Systems with Electronic Signatures

If a unit wishes to implement a new system with a different method of gathering electronic signatures, or seek to use an existing or the university-approved electronic signature system with a non-standard configuration, it must apply for approval by sending a request to 8help@osu.edu. The Business and Finance Senior Director for Shared Services and the Deputy CIO of the Office of the CIO will evaluate the request and either approve or deny it using the criteria below. To be approved, the new system must:

1. Employ a university-approved authentication method at the time of signature (see University-Approved Authentication Method for Electronic Signatures section below);
2. Meet Information Security Standards for electronic records that contain institutional data classified as internal, private or restricted (see Information Security Framework, ocio.osu.edu/itsecurity/framework);
3. Use separation of duty and other controls to mitigate risks;

4. Employ the access, monitoring, maintenance, security, and other controls to provide reasonable assurance of the authenticity of electronic signatures, that the signatures will not be rescinded, and the integrity of the electronically signed records.

University-Approved Authentication Method for Electronic Signatures

An electronic signature that does not employ a university-approved authentication method at the time of signature may not be binding on the university and because of this, units must use a university-approved authentication method. A university-approved authentication method meets all of the requirements outlined in Table 2. The university-approved electronic signature system meets all of these requirements.

Table 2: Requirements for University-Approved Authentication Method for Electronic Signatures

Requirement	Description	Method/System
Authenticity	The person signing is who they say they are.	The system must require authentication before enabling the signer to sign electronically. For university constituents, this authentication will happen with a user's university name.n credentials via: • Shibboleth • Other AD/LDAP system if the signer's user account is automatically synchronized with Ohio State's Identity Management System Signing a PDF file using the "Sign" option in Adobe Reader does not meet this requirement, nor does just typing one's name or drawing one's signature.
Nonrepudiation	The signer must take an affirmative action of some kind to sign it. The signer cannot make a legitimate or supportable claim they did not sign it.	Two-factor authentication (a login/password and an additional code given to the signer by some other means) is required in cases when the signature is on a record that contains private or restricted data or carries material risk. Two-factor authentication also mitigates the risks of: a) a record to be signed being forwarded from the recipient to another individual who could sign as if they were the original recipient, or b) the email account to which a signature request is sent being compromised.
Integrity	It is possible to tell if a completed electronic signature has been falsified or tampered with.	Workflow systems (e.g., eRequest) are secured to ISS standards so that completed signatures cannot be reversed or tampered with. Systems that produce certificates of signing must make those certificates tamper evident (e.g., DocuSign's digitally sealed certificate).
Statutory Requirement ORC §1306.07	Electronic records being capable of retention by recipient at time of receipt.	When the signing is complete, the recipient must be capable of retaining the electronic record in electronic or print form. With DocuSign, this is accomplished by receipt of a completed PDF once the signing is complete.
Statutory Requirement ORC §1306.04 and ORC §1306.16	In some cases, it is possible to opt out of signing electronically for a particular transaction.	Individuals and entities, excluding employees acting within the scope of their employment, may choose to opt out of conducting a transaction electronically by providing written notice of a request to opt out of conducting business with the university electronically. The written notice must be directed to the university employee responsible for the business relationship with the party.