THE OHIO STATE UNIVERSITY

# Electronic Signature, 1.12

## University Policy

Applies to: All individuals and entities internal and external to the university using electronic signatures to conduct university business.

## Responsible Office

Office of Business and Finance

## POLICY

Issued: 09/01/2015

To increase the efficiency of transactions that require authorization by signature, the university encourages and may require the use of an electronic signature. This policy governs all uses of electronic signatures to conduct university business and operates in tandem with delegation of signature authority.

### Purpose of the Policy

The purpose of this policy is to allow for electronic signatures at Ohio State by methods that are practical and secure, balance risk and cost, streamline administrative processes, and comply with applicable law.

### Definitions

| Term | Definition |
|---|---|
| Electronic signature | An electronic process, symbol, or sound attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Examples may include, but are not limited to:<br>1. The act and the resulting record of initiating or approving an electronic record in a university system (e.g., enterprise resource systems); or<br>2. The act and the resulting record of using special electronic signature software or systems (e.g., electronic signature platforms, point-of-sale electronic signature pads, biometric systems) to sign an electronic record. |
| Authentication | The assurance that the electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction. |
| Authorization | When an individual has verified permission and the requisite authority to sign a record (electronically or otherwise), access specific electronic university services, and/or perform certain operations, including executing agreements to bind the university. |
| Electronic record | A record created, generated, sent, communicated, received, or stored and signed by electronic means. |

### Policy Details

I. Electronic signature use
   A. The university may designate specific university transactions to be executed by **electronic signature**.
      1. Employees, including student employees, may be required to use an electronic signature for transactions with the university or to conduct university business.
      2. External parties (individuals, including students, and entities not employed by the university) must use an electronic signature to conduct business with the university, unless the university or the external party opts out of conducting business electronically as provided in the Procedure section.
   B. An electronic signature may be accepted in all situations when the requirement of a signature or approval is stated or implied, except when law or regulation specifically requires a hand-written signature.
   C. To the fullest extent permitted by law, the university recognizes an electronic signature as legally binding.
   D. When a university policy, rule, procedure, standard, law, or regulation requires or requests that a record have the signature of a responsible person that requirement or request is met by an electronic signature, except when law or regulation specifically requires a hand-written signature.
   E. An electronic signature may not be valid if the individual did not have the **authorization** to sign an electronic record.
   F. An electronic signature must employ a university-approved **authentication** method at the time of signature.

Applies to: All individuals and entities internal and external to the university using electronic signatures to conduct university business.

II. All new electronic signature systems must be approved by the Offices of Business and Finance and the Chief Information Officer.

III. Falsification

A. Falsification of **electronic records** or electronic signatures is prohibited.

B. It is a violation of this policy for an individual to sign as if they were another individual.

IV. Violations

A. Employees who falsify electronic signatures or otherwise violate this policy are subject to disciplinary action, including and not limited to termination of employment and/or potential criminal prosecution under applicable federal, state, and local laws.

B. Students who falsify electronic signatures or otherwise violate this policy are subject to disciplinary action under the Code of Student Conduct and/or potential criminal prosecution under applicable federal, state, and local laws.

C. Other individuals and entities to whom this policy applies who falsify electronic signatures or otherwise violate this policy are subject to appropriate sanctions, including but not limited to termination of the relationship and/or potential criminal prosecution under applicable federal, state, and local laws.

## PROCEDURE

Issued: 09/01/2015

I. All signatures, including electronic signatures, must follow the requirements specified in delegation of signature authority documents.

II. Electronic signatures may be implemented using the approaches identified in Guide to Implementing Electronic Signatures, which include:

A. Existing university transactional systems (e.g., enterprise resource planning system).

B. The university-approved electronic signature system.

III. All units that want to implement a new electronic signature system (i.e., not an existing or the university-approved system) or seek to use the university-approved electronic signature system with a non-standard configuration must contact the Offices of Business and Finance and the Chief Information Officer at the outset to ensure technical controls and requirements can be met. The unit must:

A. Assess, implement, and document steps to mitigate risks in cases when the electronic record to be signed contains internal, private, or restricted data as defined by the Institutional Data policy or when there is material risk associated with the signature.

B. Use a system that can provide with reasonable assurance:

1. Of the authenticity of electronic signatures,
2. That the signatures will not be rescinded, and
3. Of the integrity of the electronically signed records.

C. The unit is also responsible for, among other things, the access, control, monitoring, maintenance, and any other actions necessary for physical, network, and computer security.

IV. Units must maintain resulting electronic records in accordance with the university Records Retention Schedule and university Information Security Standard.

V. When fraudulent use is suspected, observed, or otherwise made known to an individual, the individual must immediately report the fraudulent activity to: a higher level of management; other university officials such as the

Applies to: All individuals and entities internal and external to the university using electronic signatures to conduct university business.

Department of Internal Audit; or the university anonymous reporting line at 866-294-9350 or ohio-state.ethicspoint.com.

VI. Opting out of conducting business electronically.

A. The university may, at its discretion or as required by law, opt out of conducting a transaction electronically.

B. Employees, including student employees, acting within the scope of their employment may not opt out of conducting a transaction electronically, unless specifically authorized to do so.

C. 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.

1. The written notice must be directed to the university employee responsible for the business relationship with the party.
2. 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.
3. Requests for reasonable accommodations to the written notice requirement will be made in consultation with the university's ADA coordinator.

D. Upon receipt of written notice of the decision to opt out of conducting business electronically, the university employee responsible for the business relationship with the party will process the decision to opt out and arrange for alternate signature. See Guide to Implementing Electronic Signatures.

VII. The Offices of Business and Finance and the Chief Information Officer will collaborate on the administration of this policy.

## Responsibilities

| Position or Office | Responsibilities |
|---|---|
| Business and Finance, Resource Management | 1. Ensure this policy remains consistent with state and federal law and university rules.<br>2. Interpret policy and guide implementation.<br>3. Approve, with the Office of the Chief Information Officer, all new electronic signature systems and non-standard configurations of existing or university-approved systems meeting requirements of this policy.<br>4. Collaborate with the Office of the Chief Information Officer on the administration of this policy. |
| OCIO, Enterprise Security | 1. Consult with units to assess the risks associated with any proposed use of electronic signatures and recommend mitigating controls.<br>2. Approve, with the Office of Business and Finance, all new electronic signature systems and non-standard configurations of existing or university-approved systems meeting requirements of this policy.<br>3. Collaborate with the Office of Business and Finance on the administration of this policy. |
| ADA Coordinator | Consult on reasonable accommodations as requested. |
| Units | 1. Implement electronic signatures using an approach outlined in this policy.<br>2. Designate specific transactions to be executed by electronic signature.<br>3. Follow requirements in Guide to Implementing Electronic Signatures.<br>4. Maintain electronic signature records in accordance with the university Records Retention Schedule and Information Security Standard.<br>5. Follow requirements specified in the delegation of signature authority document.<br><br>Additional responsibilities when using an existing or new electronic signature system or the university-approved system with a non-standard configuration:<br>6. Contact the Offices of Business and Finance and the Chief Information Officer at the outset to ensure technical controls and requirements can be met with the proposed electronic signature system.<br>7. Work with OCIO Enterprise Security or Business and Finance Resource Management to assess, implement, and document steps to mitigate risks when the electronic records to be signed contain |

Applies to: All individuals and entities internal and external to the university using electronic signatures to conduct university business.

| Position or Office | Responsibilities |
|---|---|
| | restricted or private data or a material risk.<br>8. Consult with the OCIO for assistance in risk assessment and mitigation as needed.<br>9. Provide reasonable assurance (a) of the authenticity of electronic signatures, (b) that the signatures will not be rescinded, and (c) of the integrity of electronically signed records. See Guide to Implementing Electronic Signatures. |
| External parties (individuals, including students, and entities not employed by the university) | 1. Conduct business with the university by using an electronic signature when requested.<br>2. Notify the university employee responsible for the external party relationship in writing if requesting to opt out of conducting transactions electronically. |
| Employees, including student employees | 1. Follow requirements specified in the delegation of signature authority document.<br>2. Use an electronic signature for transactions with the university as specified.<br>3. Report suspected or actual electronic signature fraud to a higher level of management; other university officials such as the Department of Internal Audit; or the university anonymous reporting line at 866-294-9350 or secure.ethicspoint.com.<br>4. Notify the university employee responsible for the transaction if requesting to opt out of conducting business with the university electronically; opt out can only occur when the transaction occurs outside of the scope of employment, or as required by law. |

## Resources

Code of Student Conduct, **studentaffairs.osu.edu/csc/**
Electronic Signatures Rules, **trustees.osu.edu/rules/electronic-signature-rules.html**
Guide to Implementing Electronic Signatures, link to be added
Information Security Standard, **go.osu.edu/infosec-iss**
Institutional Data policy, **go.osu.edu/idp**
Internal Controls policy 1.11, **busfin.osu.edu/FileStore/PDFs/111_InternalControls.pdf**
University Records Retention Schedule, **library.osu.edu/documents/records-management/general-schedule.pdf**

## Contacts

| Subject | Office | Telephone | E-mail/URL |
|---|---|---|---|
| Policy questions | Resource Management, Office of Business and Finance | | **rms.ohio-state.edu** |
| IT security issues | Enterprise Security, Office of the Chief Information Officer | | **ITpolicy@osu.edu**<br>**ocio.osu.edu/itsecurity** |
| Reporting suspected fraud | Department of Internal Audit, Office of Business and Finance | 614-292-9680 | **ia.ohio-state.edu/** |
| Reporting suspected fraud | University Anonymous Reporting Line | 866-294-9350 | **ohio-state.ethicspoint.com** |

## History

Issued: 09/01/2015