Electronic Signatures

I. Purpose

A. To provide guidance to University of Kentucky (UK) departments and employees on the implementation and use of an electronic signature process authorizing official transactions as permitted by Administrative Regulation 10:5. This includes how to:
   1. determine what forms are appropriate for electronic signatures;
   2. gauge the level of security needed;
   3. determine which methodology or technology to use;
   4. obtain approval to use electronic signatures; and
   5. responsibly use electronic signatures.

II. Definitions

- *Authentication:* the process of securely verifying the identity of an individual prior to allowing access to an electronic UK service.
- *Authorization:* verification that an authenticated user has permission to access specific electronic UK services and/or perform certain operations.
- *Electronic:* relating to technology that has electrical, digital, magnetic, wireless, optical, or electromagnetic capabilities or similar capabilities.
- *Electronic Signature (e-signature):* an electronic sound, symbol or process that is attached to or logically associated with a record and that is executed or adopted with the intent to sign the record.
- *Information:* data, text, images, sounds, codes, computer programs, software, databases or similar items.
- *Transaction:* an action or set of actions occurring between two (2) or more persons relating to the conduct of business, commercial, or governmental affairs.
- *Unit:* the UK unit conducting business by means of an e-signature; such as a college, department, auxiliary, or administrative division.

III. Responsibilities

A. UK ITS Cybersecurity Team
   1. Provide assistance to departments in the development or selection of the technology to be used for an electronic signature.

B. Unit Data Custodian (as defined in AR 10:3.II.D)
   1. Assist unit personnel with the development of the e-forms.
   2. Determine the level of security to be used for those forms, based on the recommendations in section IV. B below.
   3. Determine the technology to be used for e-signature methodology, also based on recommendations in section IV. C below.
   4. Review and give final approval to all e-forms used exclusively within the department that do not require a heightened level of security.
   5. Review and approve inter-departmental e-forms then forward to the Area Fiscal Officer.
   6. Initiate the required biennial review process.

C. Area Fiscal Officer
   1. Review and approve inter-departmental e-forms.
   2. Submit e-forms to the Executive Vice President for Finance and Administration for final approval.

D. Employees
   1. Users must keep their unique authorization information secure and secret.
   2. The use of unique identifiers (e.g., passwords, PINs, etc.) must not be shared in order to protect the integrity of electronic authorization and authentication.

IV. Policy

A. UK considers electronic forms or e-forms to include:
   1. Any electronic process that requires authorization for its transaction to be initiated;
   2. Any electronic document that requires authorization for its intended transaction to be initiated; or
   3. Any electronic transaction that would otherwise require a handwritten signature for its intended action to be initiated.

B. The e-signatures process must be secure:
   1. Acceptable level of security:
      Standard username and password protected authorization, as well as a second method of authorization such as, but not limited to:
      a. Single use password device
      b. Physical security token (e.g., thumb drive with embedded digital certificate)
      c. Two-party security token submission

C. Methodologies to be used:
   1. Preferred technologies to be used in either level of security are:
      a. ERP Automated Workflow
      b. Adobe Secure Sign
      c. UK Active Directory Authentication
   2. Other technologies that may be conditionally used in heightened level of security are:
      a. Public Key Infrastructure
      b. Proprietary technology
      c. Other (with approval given by Information Technology Services)
      d. Certain technologies will require proof of appropriate audit trail

V. Procedures

A. Electronic Signature Approval Process:
   1. Any proposal for the implementation of an electronic signature must include:
      a. What the signature would be authorizing
      b. A rational for the level of security requested
      c. Detail of the methodology/technology used for the signature
      d. Potential risks and costs associated with implementation

2. For proposed electronic signatures intended for use in inter-departmental forms, or for electronic signature requiring a heightened level of security:
   a. The Unit's Data Custodian must submit the proposal for electronic signatures to the relevant AFO for initial review.
   b. If the AFO is then initially satisfied with the electronic signature security level, purpose, costs, and methodology, he or she will present it to the Executive Vice President for Finance and Administration (EVPFA) office for final approval.
3. For proposed electronic signatures intended for intra-departmental forms, and do not require a heightened level of security:
   The Unit's Data Custodian can give final approval for use if he or she is satisfied with the proposed signature's security level, purpose, cost, and methodology.
4. Units must initiate a review and re-approval process on a biennial basis, following the original procedure laid out above.