PROCEDURES FOR ESTABLISHING USER ACCOUNT & ACCESS TO DATA
July 05, 2017

Step 1: Complete Acceptable Use Agreement
User completes form located at: https://one.iu.edu/launch-task/iu/acceptable-use-agreement

Step 2: Create IU Account

A. For affiliates:
   i. supervisor/sponsor completes the **Request to Add IU Affiliate** form located at: https://one.iu.edu/launch-task/iu/affiliate-accounts
   ii. Affiliate creates their own IU account
B. For non-affiliates (any other status):
   i. Individuals create their first IU account: https://one.iu.edu/launch-task/iu/create-my-first-iu-account

Step 3: Request Access to Applications and Data

A. Supervisor/Sponsor validates that an **Acceptable Use Agreement** is on file for this individual: https://one.iu.edu/launch-task/iu/verify-acceptable-use-agreement
B. Supervisor/sponsor completes the appropriate form: https://one.iu.edu/launch-task/iu/request-application-access

Step 4: Process Application and Data Access request

A. Data Managers check the status of requester (employee, designated appointee, etc.)
   Note: *we are exploring the possibility of changing this form, as part of the migration from OneStart to One.iu.edu, to include*
   ii. a Justification entry box
   iii. an association status indicator (i.e. Employee, Academic No-pay, Student, Affiliate, etc.)
   iv. an indicator of the type of affiliate if the user has an affiliate association with the university
   v. until then, these items will need to be collected manually

B. For individuals with Employee or Designated Appointee status, Data Managers take the following actions:
   i. Grant access to Public data
   ii. Ensure Supervisor is aware of Data Handling information and provides to requester (i.e. Critical Data Guide, Access to Data Management website and the Protect website, systems specific training)
   iii. Data Manager verifies that requester has taken Data Compliance Training for systems being requested (ex. HIPAA Training, FERPA and HR tutorials, etc.)
   iv. Grant access to Univ-Internal data
   v. For Restricted or Critical data:
      - Ask Supervisor/Manager for Justification for Access
      - Data Manager evaluates request and justification to determine if requested access should be granted.

C. For individuals with Affiliate status, Data Managers take the following actions:
   i. Grant access to Public data

ii. For requests to access Univ-Internal, Restricted and/or Critical data:
- Ensure Supervisor/Sponsor is aware of Data Handling information and provides to requester (i.e. Critical Data Guide, Access to the Data Management website and the Protect website, systems specific training)
- Ask Supervisor/Sponsor for Justification for Access
- Data Manager verifies that requester has taken Data Compliance Training for systems being requested (ex. HIPAA Training, FERPA and HR tutorials, etc.)
- Data Manager evaluates request and justification to determine if requested access should be granted

D. For individuals with Retiree status – TBD

Associated knowledgebase articles can be found at: https://kb.iu.edu/d/auod
https://kb.iu.edu/d/bfwe