Banner Time Entry Feeder System Agreement

UIC

In compliance with the OBFS Policies & Procedures Manual-Section 4: Payroll, units are required to report and approve all hours worked and benefits time used according to the published schedule and deadlines for biweekly employees. It is also noted that unit representatives identified with the role of an Approver should not approve their own time. If an Approver is also an hourly employee required to submit time, then a designated Approver must approve the individual's time.

The University Code of Conduct outlines expectations of staff related to honesty, responsibility, compliance with laws and policies, and stewardship of university property and resources. It also includes information on following good business practices related to signature authority and segregation of duties.

The Banner System contains a majority of the Student, Human Resources, and Financial data for the University. Banner contains data of every classification including High Risk, Sensitive, Internal, and Public. Securing the data within the Banner system is of the utmost priority for the University and Administrative Information Technology Services (AITS). Systems that connect and provide feeder information to Banner must be secure to ensure that the data within Banner can be relied upon.

All units that feed data to Banner must follow all policies and procedures referred to above and ensure the systems involved in the feeder process meet the security requirements below.

IT Security Program

The IT Security Program at UIC is a comprehensive program that includes data classification requirements as well as standards and guidelines for securing IT systems for all units affiliated with UIC, https://it.uic.edu/resources/policy/. All units that feed data to Banner will ensure overall compliance with the UIC IT Security Program for systems involved in the feeder process. While overall compliance is required, specific aspects within the UIC IT Security Program should be of note:

DCS.1 – Data Classifications
DCS.3 – Access Authorizations
DCS.7 – Transmission Security
SS.2 – Establish Workstation and Server Access Controls
SS.4 – Establish Protections from Malicious Software
P.1-P.5 – Physical Security

Data Classification

Please indicate the highest class of data that will be included in the feeder data that will be transmitted to Banner:

◯ High Risk

High Risk Data is a University class of information that, if disclosed or modified without authorization, would have severe adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Information in this class includes, but is not limited to:

1. Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, such as credit card information (covered by the Payment Card Industry Data Security Standard (PCI DSS)).
2. Information covered by federal and state legislation, such as the federal Health Insurance Portability and Accountability Act (HIPAA) or the Illinois Personal Information Protection Act (IL PIPA).
3. Payroll, personnel, and financial information with special privacy requirements.

○ Sensitive

Sensitive Data is a University class of information that, if disclosed or modified without authorization, would have serious adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Information that is covered by FERPA, Non-Disclosure Agreements (NDAs), and other intellectual property are, as a minimum, in this class.

Note: Non-Disclosure Agreements may fall into the High Risk Data or Sensitive Data categories and should be individually evaluated.

○ Internal

Internal Data is a University class of information that, if disclosed or modified without authorization, would have moderate adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

Process Requirement(s)

The Unit understands if the submission of their mass time entry file fails during the current calc process and the unit cannot resolve the issue in a timely manner, the only alternative will be for the unit to submit PARIS adjustments for each employee in order to get them paid.

For units requesting to become a feeder unit, a Feeder System Evaluation form will need to be completed in its entirety along with this agreement and routed to University Payroll & Benefit for review.

Units will be required to adhere to all mass time entry file deadlines as published in the UPB Payroll Schedule, Newsletter, and/or other UPB approved communications.

Units will be required to notify UPB at obfsupbsystemssupport@uillinois.edu of changes in feeder departmental contacts as they arise.

Units will be required to notify UPB at obfsupbsystemssupport@uillinois.edu of changes in timekeeping systems at least six months in advance to schedule appropriate testing and evaluation of the new timekeeping system.

Units understand that if they do not abide by the terms of this agreement, permission to feed data from their timekeeping system in mass to Banner may be revoked.

Units understand that if their College currently utilizes mass time entry, they must work with the administrators of that timekeeping system to be added to their Mass Time Entry file.

Units understand that if their College currently does NOT utilize mass time entry and they are requesting to be added to another college's timekeeping system and Mass Time Entry file, they must receive approval from BOTH colleges.*

Per this form/agreement, the unit certifies the systems included in the Banner feeder process maintained by the unit meet the applicable security program and requirements as noted above. The unit also attests to the accuracy and inclusion of all requested information and will abide by the terms set forth in this document. The unit also understands that completion of the Feeder System Agreement form and the Feeder System Evaluation form will need to be completed every two years.

Unit Contact *Phone #*

Department Name

Department Email *Date*

Department Head *Phone #*

Department Head Email *Date*

College Contact *Phone #*

College Name

College Contact Email *Date*

**Secondary College Contact* *Phone #*

**Secondary College Name*

**Secondary College Contact Email* *Date*