# 9.1.2 Segregation of Duties in Enterprise-wide Applications for Procurement and Tracking of Equipment

## Policy Statement

University of Illinois System employees must have a legitimate business need to access certain enterprise-wide applications. Enterprise-wide applications are those programs used across the University of Illinois System (e.g., Banner, iBuy, Chrome River, Contracts+, etc.) The combination of access for several of these enterprise-wide applications may cause a lack of segregation of duties creating an inherent risk for the system. Role combinations involving the requisitioning, procurement, and tracking of equipment are prohibited unless the unit obtains an approved Exception Request.

## Reason for the Policy

To mitigate the inherent risks of prohibited role combinations through the segregation of duties.

## Applicability of the Policy

This policy applies to all system employees with the following role combinations:

* iBuy Requestor with FABweb Unit Rep or Biennial Unit Contact
* iBuy Approver with FABweb Unit Rep or Biennial Unit Contact
* Banner Department Manager/Requestor with FABweb Unit Rep or Biennial Unit Contact
* P-Card Cardholder with FABweb Unit Rep or Biennial Unit Contact

## Procedure

Employees requesting access to enterprise-applications for the prohibited role combinations must submit an Exception Request that includes a risk mitigation plan and internal review procedures.

### Exception Request

To obtain access to the prohibited role combinations, units must submit an Exception Request, which must include a risk mitigation plan and internal review procedures (as defined below). The Exception Request must have documented approval from the department head, college leadership, and the Provost, Chancellor, or Vice President’s office (depending on reporting lines). Universities may have additional requirements to receive an approved Exception Request.

Once the Exception Request is approved it will be routed to the Unit Security Contact to assign the necessary permissions to the employee(s).

Exception Requests are valid for two years. Units will be notified via email prior to the expiration of a prohibited role combination exception and a new Exception Request must be submitted if still required. Should the job responsibilities of the employee(s) mentioned in the Exception Request change or if there is a staffing change impacting the additional controls mentioned in the risk mitigation plan or internal review procedures, units are required to update their Exception Request to reflect these changes and to ensure mitigating controls remain sufficient. Units and colleges are responsible for adhering to the internal review procedures as documented.

### Risk Mitigation Plan

A risk mitigation plan involves the identification and documentation of internal controls that significantly reduce the inherent risk of prohibited role combinations. Mitigating internal controls are checks and balances to provide additional security and reduce risk. They should clearly define how employee activity will be monitored and confirm Business and Financial Policies and Procedures are followed.

### Internal Review Procedures

Internal review procedures are the evaluation steps that will be employed within the unit to ensure that the mitigating internal controls are being followed correctly and consistently. Review procedures should include how mitigations will be monitored as well as how changes will be identified and acted upon.

First published: \_\_\_\_\_\_\_\_\_\_\_ | Last Updated: \_\_\_\_\_\_\_\_\_\_\_ | Last Reviewed: \_\_\_\_\_\_\_\_\_\_\_