Human Resources/Payroll/Labor Distribution Duty Segregation

HRMS/Payroll/LD Module(s)	Segregation of Duty Scenarios	Business Impact/Risk	Segregation Recommendations
HRMS – Campus	Access to update and view administrative personnel, payroll and benefit data.	Granting a single user the ability to update and view administrative personnel, payroll and benefit information increases the risk of unauthorized or unintentional changes.	Limit access to HRMS Administrator.
	Access to update and view administrative personnel and payroll data.	Granting inappropriate users access to maintain and view personnel setups and payroll data could result in erroneous, unauthorized or unintentional changes as well as confidentiality issues.	Limit access to HR / Payroll Specialist. Segregate HR / Payroll Specialist from HRMS Administrator.
	Access to perform benefit administration functions.	Granting inappropriate users access to maintain and view benefit administration could result in erroneous, unauthorized or unintentional changes as well as confidentiality issues.	Limit access to Benefit Administrator. Segregate Benefit Administrator from HRMS Administrator and HR / Payroll Specialist.
	Individuals intended to have inquiry-only access should only be granted inquiry-only responsibilities.	Unintentionally granting modify access to an inquiry-only individual increases the risk of unauthorized entries.	Limit and segregate where appropriate access to inquiry only responsibilities, such as HRMS Inquiry, HR / Payroll Inquiry and Benefit Inquiry. All other HRMS responsibilities should not be granted.
HRMS – Central Office Central Office Only	Access to setup and master information should be limited and restricted.	Granting inappropriate users access to maintain setup data could result in erroneous, unauthorized or unintentional changes.	Limit access to HRMS Setup. Access to this data should be maintained centrally within central office only.

	Access to view and update administrative personnel, payroll and benefits administration data.	Granting a single user the ability to perform all administrative personnel, payroll and benefits administration functions increases the risk of unauthorized or unintentional changes to data.	Limit access to HR Administrator, Payroll Administrator and Benefits Administrator. Segregate HR Administrator, Payroll Administrator and Benefits Administrator.
	Access to perform payroll data input processing for various campus locations.	Granting inappropriate users access to update payroll data processing information could result in erroneous, unauthorized or unintentional payroll changes occurring, as well as potential confidentiality issues.	Limit access to Payroll Specialist. Segregate Payroll Specialist from HR Administrator, Payroll Administrator and Benefits Administrator.
	Individuals intended to have inquiry-only access should only be granted inquiry-only responsibilities.	Unintentionally granting modify access to an inquiry-only individual increases the risk of unauthorized entries.	Limit and segregate where appropriate access to inquiry only responsibilities, such as HR Inquiry, Payroll Inquiry and Benefit Inquiry. All other HRMS responsibilities should not be granted.
	Access to run HRMS scheduled processes and reports should be restricted and limited. In addition, other HRMS activities should not be granted to those individuals with running IS processing.	Segregation of running batch processes and reports for HRMS is recommended to limit a single user's ability to perform IS processing and day-to-day processing activities.	Limit access to IS Processing. Segregate IS Processing from HRMS campus and central office functional responsibilities.
LD – Campus and Central Office Central Office Only	Access to create labor schedules, define and approve distribution adjustments, create/accept/certify effort reports and create encumbrances.	Granting inappropriate users access to create labor schedules, define and approve distribution adjustments and the effort reporting functionality could result in erroneous, unauthorized or unintentional data being reflected and used for reporting.	Limit access to LD Administrator. Segregate LD Administrator from Effort Reporting Specialist and Employee.
	Access to accept, certify or reject effort reports.	Granting inappropriate users access to accept, certify or reject effort reports could result in erroneous, unauthorized or	Segregate Effort Reporting Specialist from Employee.

		unintentional data being reflected and used for reporting.	
	Individuals intended to have inquiry-only access should only be granted inquiry-only responsibilities.	Unintentionally granting modify access to an inquiry-only individual increases the risk of unauthorized entries.	Limit and segregate where appropriate access to LD Inquiry only. All other LD responsibilities should not be granted.
	Access to setup and master information should be limited and restricted.	Granting inappropriate users access to maintain setup data could result in erroneous, unauthorized or unintentional changes.	Limit access to LD Setup. Access to this data should be maintained centrally within central office only.

Back to Guidelines for Segregating User Duties.