CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

Protection of Confidential Data in Non-Production Environment

CSU Bakersfield Policy

Document Number: ITS-90.025
Last Revision Date:
Responsible Office: Information Technology Services
Effective Date: 1/9/2023
Primary Author: Director, ITS - Enterprise Applications

General Description

Purpose:

Establish a standard of practices to safeguard confidential data in PeopleSoft non-production environment. This includes leveraging data masking or restrict access to essential personnel.

Definition:

Data masking or data obfuscation is the process of modifying sensitive data in such a way that it is of no or little value to unauthorized intruders while still being usable by software or authorized personnel.

Scope:

This policy applies to all PeopleSoft environments managed by the campus.

Policy/Procedure

Standard Procedures

Effective as indicated, all data refresh (aka clone) to PeopleSoft non-production environment will include additional steps to mask confidential data. Campus shell leverage standard-masking profile provided by the Chancellor's Office CMS team. The standard masking profile includes the following

Data Domain	Columns
Social Security Number	SSN, Tax ID Number (TIN), National ID (NID)
Banking Information	Routing Transit Number (RTN), Account Number, Credit Card Number

Exception

Suppose specific testing or project activities require an instance to be unmasked. In that case, all PeopleSoft accounts in an unmasked instance will be locked except for the PeopleSoft core development and testing team members. Appropriate business justifications shall also accompany unmasked data refresh requests. An unmasked instance will have a default end date of two weeks unless requested otherwise.