Prepared by: Leigh Lopez **Date:** March 14, 2023	**Approved by:** Kevin Krzewinski **Date:** March 15, 2023
Last revised by: **Date:**	**Last approved by:** **Date:**

1.0 PURPOSE

Document the procedures for the management and security of PeopleSoft test databases that are used by the campus for the development and test of patches, new features and to debug production issues.

2.0 SCOPE

The scope of these procedures includes all databases that are created by CMS for use by the campus. All persons who use the CMS PeopleSoft test databases are included in this scope.

3.0 RESPONSIBILITY

	Role (Title)	Responsibility
1	Information Security Officer	• Review and authorize unmasked versions of the database. • Review and authorize any security requests for additional access
2	Director Enterprise Development	• Coordinate with departments as to the timing of PeopleSoft test database clones • Coordinate with IT database team as to resources for cloning • Review and approve requests for database cloning

4.0 GUIDELINES

4.1 Requesting a Clone

All requests for cloning will be sent to the Director of Enterprise Development. After consultation with respective departments and the SOLAR Leads committee, a date for a clone will be communicated to SOLAR Leads, IT Database Team and Information Security. By default, all database clones will be created masked and all database clones will be created with identical security as production.

4.2 Requesting a Database to be Unmasked

If a database clone is requested to be unmasked the director of the department requesting the unmasking must submit a business case that contains the reason for the database to be unmasked and the timeframe for

unmasking. The maximum timeframe for unmasking is 30 days.

After ISO approval, the DBA team will enter the request for the unmasked clone into CMS. The DBA team when entering the initial request for the unmasked clone will also enter an additional clone request for that database to be clone with masking turned on coinciding with the end date on the request. If the date needs to be extended, the department head must submit an additional request to the ISO.

4.3 **Requesting Additional Security**

If additional security within the test database is required, the request must be made to the ISO, who will review the request appropriately.

5.0 DEFINITIONS

Database Masking

Data masking is a method of creating a structurally similar but inauthentic version of CSUN's data that is used for testing, troubleshooting and developing fixes and modifications, The purpose is to protect the actual data while having a functional substitute for occasions when the real data is not required. The data that is masked in the environments are SSN and banking information.