**Source Code Repository Policy**

# 

# Purpose

This policy outlines:

1. The approval process for Source Code Management (SCM) systems.
2. What can and cannot be stored in the SCM.
3. General requirements for an SCM.

# Scope

This Policy applies to the SLEDS Environment, SLEDS Information, Participating Entities, and other parties authorized or responsible for carrying out SLEDS Policies. This policy does not apply to the Participating Entities’ Environments and how they manage their own code repositories.

# Applicable Standards and Regulations

* [SLEDS High Availability Data MOU (HADS)](https://docs.google.com/document/d/1_iVjhRviWRvtRVd_gf7Py4ymBVOmo1aChsAOnToYOkQ/edit), (entered February 23, 2022) for the collection and linking of SLEDS data to audit and evaluate educational programs.

# Policy Statements

1. **SCM Approval Process** 
   1. Written requests to approve SCM system(s) must be submitted to the Security Subcommittee.
   2. The Security Subcommittee will respond in writing with either the approval or disapproval of the request.
2. **Allowed Storage** 
   1. The SCM can be used to store source code.
   2. The SCM can be used to store image files used in report production (e.g. Logos).
3. **Disallowed Storage**
   1. The SCM will not be used to store data files, passwords, API keys, or user-ids.
   2. The SCM will not be used to store images containing PII (e.g. screenshots).
4. **General Requirements**
   1. The SCM shall have separate accounts for administration and user access.
   2. The SCM shall use multi-factor authentication for all accounts.
   3. The SCM shall be configured to prevent making the repository public.
   4. All code must be reviewed to ensure there is no PII present. This review may be automated or part of the repository workflow procedure.
   5. The individual writing the code will not be allowed to approve their own check-ins.

## Approvals

This policy requires the following approvals:

| **Name** | **Date Approved** |
| --- | --- |
| Security Subcommittee | v1.2 Approved 1/17/2023 |
| Data Governance Committee | v1.2 Approved 1/24/2023 |