1.0 PURPOSE

The purpose of these Guidelines is to outline the coding practices to be incorporated into an application's security architecture and development lifecycle.

2.0 SCOPE

These Guidelines apply to all employees, contractors who work with and the information processing environment; onsite or remotely.

ROLES AND RESPONSIBILITIES (EXAMPLE)

ROLE	RESPONSIBILITIES
CUI Steering Committee and Operational Governance Team	• To raise and maintain awareness of the activities including asks of users and to inform staffing efforts for the service.
System Owner	• To ensure System Administrators are trained on these guidelines.
System Administrators, Users	• To follow these guidelines if developing any custom code.
System Administrators and Users	• To follow and be able to provide evidence of following these guidelines if developing any custom code.

3.0 CODING PRACTICES

- Secure coding practices will be incorporated into an application's security architecture and development lifecycle.
- Security requirements are defined early in the software development lifecycle and then evaluated for compliance with those requirements.
- All applicable practices from the OWASP Secure Coding Practices Checklist will be followed.
- Unencrypted credentials of any form will never be used.
- Peer reviews are performed for changes or additions to production code.
- Test environments are used whenever possible.

4.0 THIRD-PARTY COMPONENTS

Applications use the latest available version of third-party components (packages, modules, libraries, etc.) to ensure that all known vulnerabilities with available patches are addressed.

- All packages will evaluated against a CVE database such as https://security.snyk.io/ to check for known vulnerabilities.

- Application-specific tools:
- Python: pip-audit
- R: oysteR
- Powershell: nuget verify (nuget repositories only)

- All packages will be checked for the checksum or PGP verification method.
- Only trusted, first-party repositories are used whenever possible.
- All packages will be checked against the countries of origin per the software vetting guidance document.
- Dynamic inclusion of third-party software will be avoided, especially from sources the developer has no control or insight over.

5.0 SOURCE CODE MANAGEMENT

- The Preserve GitHub organization (CUB-OIT-SRCS) will be used to store all shared code repositories
  - This GitHub Org is tied to the Preserve Entra ID tenant for authentication and has several security settings applied to all repositories by default. For a full list of settings see the Development Platform.
- Branch protection will be enabled to require pull requests on the default branch:
  - If staffing allows, users will not be allowed to approve their own pull-requests to the main branch.

6.0 ACRONYMS

TERM	DEFINITION
CUB-OIT-SRCS	Preserve GitHub organization
PGP	
CVE	

7.0 REVISION HISTORY

REVISION	DATE	DESCRIPTION	ISSUER
	09/22/2021	Initial draft	
	10/01/2025	Reformat	MLC
	10/02/2025	Update Roles and Responsibilities section	BGS

8.0 REFERENCES

Teams IT Governance Team; CUI Governance channel; Folder: CMMC>CMMC Working Documents>Preserve SSP

>03.13 – System and Communications Protection>03.13>03.13.0203.13.02 Software Vetting Policy

>03.04 – Configuration Management>03.04.01 Change Management Procedure
03.04.01 Change Management Procedure

