SLATE Application Developer Obligations

Version	Comment	Effective date
1.0	Initial version	September 25, 2020

In order to safely operate the SLATE Platform, the SLATE Platform Administrators require that SLATE Application Developers (persons who take an existing application and package it in a way that can be installed on a SLATE platform) agree to the following:

- Application Developers must follow the SLATE Application Development and Review Procedures document, which outlines specific application design policies for any application that is to be a part of the SLATE application catalog.
- Application Developers must give due consideration to security when designing or updating applications.
    - Default configuration options should be chosen to be safe, and configuration options with significant security implications must be labeled as such, with clear advice to Application Administrators on safe and correct use.
    - Features of applications with significant security implications must be clearly described in the application's documentation.
    - Application Developers are responsible for performing due diligence in checking for and/or preventing security vulnerabilities in their applications.
- Application Developers must respond promptly to patch security vulnerabilities which are identified as posing critical risks to the SLATE federation. For example, CVEs affecting third party libraries incorporated into the image at “Critical” or “High” levels. In this case, SLATE Platform admins may notify you of such vulnerabilities, and you should provide a list of security vulnerabilities that have been patched.
- Application Developers must keep up-to-date contact information for their Applications as required in the SLATE Application Development and Review Procedures document.

The SLATE Platform Administrators may deny applications or remove them from the catalog out of urgent concern for the security or interoperability of the overall platform.

To support Application Developers' observance of these obligations, SLATE Platform Administrators will:

- Periodically review and renew contact information for Applications.
    - Any Application without valid contact information will be considered unmaintained and marked for removal from the catalog.

This document is a policy of the SLATE (Services Layer at the Edge) project, supported by the National Science Foundation Office of Advanced Cyberinfrastructure: "CIF21 DIBBs: EI: SLATE and the Mobility of Capability", award number OAC-1724821.

- Periodically review applications in the catalog, including tool-based vulnerability assessment.
- Publish lists of security patches.
- Publish a description of the functionality testing that has been done.
- Make links to application source documentation supplied by Application Developers available to SLATE Platform users.
- Scan submitted containers for security vulnerabilities and provide Critical or High results to Application Developers.

This approach is intended to consistently provide transparency of security findings and provide relying parties with relevant information to make decisions about utilizing applications.

This document is a policy of the SLATE (Services Layer at the Edge) project, supported by the National Science Foundation Office of Advanced Cyberinfrastructure: "CIF21 DIBBs: EI: SLATE and the Mobility of Capability", award number OAC-1724821.