SLATE Edge Administrator Obligations

Version	Comment	Effective date
1.0	Initial version	September 25, 2020
2.0	Reflect updated review procedures	March 23, 2021

In order to safely operate the SLATE Platform, the SLATE Platform Administrators require that SLATE Edge Administrators agree to the following:

1. Keep their contact information, including security contact information, entered in the SLATE Platform, and the contact information for any groups they create, up to date.
2. Perform the following in alignment with the edge site's policies:
    a. Patch critical[1] operating system vulnerabilities.
    b. Protect information systems they administer from intrusions using best practices and tools.
    c. Produce and retain logs appropriate for traceability of service administration and usage sufficient to be able to answer the basic questions – who? what? where? when? and how? concerning a security incident, and document the configuration of the logging mechanisms that produce this information.
3. Apply updates to SLATE components, Kubernetes, their chosen container runtime, etc. if these are indicated by the SLATE Platform Administrators to be necessary for reliable and secure operation.
4. Review the CIS Kubernetes Benchmark, especially to adhere as much as possible to its guidance on RBAC and the seccomp profile.
5. Review the CIS Docker Benchmark, even if a different CRI is being used, and adhere as much as possible to its guidance.
6. Be thoughtful about Kubernetes global network policy. With SLATE, the network policy precedence rule is more specific wins rather than win by order of declaration.
7. Be thoughtful about privileges on partitions provided to containers - keep them as minimal as possible.
8. Consult the per-application README and Review report associated with each application in SLATE's stable catalog.
9. Collaborate in the event of an incident with the SLATE Platform Administrators and other organizations participating in the SLATE Platform as needed.
    a. Information shared between collaborators for security incidents will be handled according to the Traffic Light Protocol (TLP, https://www.first.org/tlp/).

[1] As identified by the originator of the vulnerability report

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.

The SLATE Platform Administrators may remove edge clusters out of urgent concern for the security or interoperability of the overall platform.

To support Edge Administrators' observance of these obligations, the SLATE Platform Administrators will:

1. Notify SLATE Edge Administrators of vulnerabilities contained within the SLATE software.
2. Maintain documentation of software versions supported in the SLATE federation (e.g. of Kubernetes).
3. Notify Edge Administrators at least one month in advance of any change to the set of supported software versions which would necessitate Edge Administrators to install upgraded software to remain compatible with the federation.
4. Annually test the list of Edge Administrator and security contacts.
5. Notify Application Administrators of their obligation to not replace any image sources referenced in the Helm chart for an application they deploy from the SLATE stable catalog.

The SLATE Platform Administrators will additionally proffer, on a best-effort basis, notifications of misconfigurations or vulnerabilities in container orchestration (Kubernetes) and container runtime software (Docker, Podman, Singularity) used by the SLATE platform.

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.