Procedure for Federation Participants

Roles and Responsibilities of Federation Participants

- Follow the [OS], [IR], [TR], and [PR] requirements described by Sirtfi [1]
- Publish valid security contact information in federation metadata as defined by the REFEDS Security Contact Schema [2]
- Report all security incidents posing a risk to any other federation participant within or outside their own federation, to the federation security contact point at their own federation

Security Incident Response Procedure for Federation Participants

1. Follow security incident response procedures established for the organisation.
2. Contain the security incident to avoid further propagation whilst aiming at carefully preserving evidence and logs. Record all actions taken, along with an accurate timestamp.
3. Report the security incident to their federation security contact point within one local working day of the initial discovery or notification of the security incident.
4. In collaboration with the Federation Security Incident Response Coordinator, ensure all affected participants in the federation (and, if applicable, in other federations), are notified via their security contact with a “heads-up” and can take action.
5. Announce suspension of service (if applicable) in accordance with federation and interfederation practices.
6. Perform appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
7. Share additional information as often as necessary to keep all affected participants up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
8. Respond to requests for assistance from other participants involved in the security incident within one working day.
9. Take corrective action, restore access to service (if applicable) and legitimate user access.
10. In collaboration with the Federation Security Incident Response Coordinator, produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER [3] or higher.
11. Update documentation and procedures as necessary.

[1] https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

[2] https://refeds.org/metadata/contactType/security

[3] https://www.us-cert.gov/tlp