Incident Response Procedure

Security Incident Response Procedure for Infrastructure Participants

1. 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.
2. Report the security incident to the Infrastructure Security Contact point within one local working day of the initial discovery or notification of the security incident.
3. In collaboration with the Security Incident Response Coordinator (identified by the Infrastructure Security Contact), ensure all affected participants in the infrastructure and federation (and, if applicable, in other federations), are notified via their security contact with a "heads-up" and can take action.
4. Announce suspension of service (if applicable) in accordance with infrastructure, federation and interfederation practices.
5. 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.
6. 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.
7. Respond to requests for assistance from other participants involved in the security incident within one working day.
8. Take corrective action, restore access to service (if applicable) and legitimate user access.
9. In collaboration with the 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.
10. Update documentation and procedures as necessary.

Security Incident Response Procedure for the Infrastructure Security Contact

1. Assist Infrastructure participants in performing appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. 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.
2. 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.
3. Ensure all affected participants in the infrastructure and federation (and, if applicable, in other federations) are notified via their security contact with a "heads-up" within one local working day. If other federations are affected, the eduGAIN security contact point must be notified, even if affected participants in all other federations have been contacted directly.
4. Coordinate the security incident resolution process and communication with affected participants until the security incident is resolved.
5. Ensure suspension of service (if applicable) is announced in accordance with infrastructure, federation and interfederation practices.
6. 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.
7. Assist and advise participants in taking corrective action, or restoring access to service (if applicable) and legitimate user access.
8. 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.

9. Update documentation and procedures as necessary.