FAQs

This list of Frequently Asked Questions is provided to complement the information contained in the Sirtfi Trust Framework Document.

General Questions

General questions are listed on the public facing site: https://refeds.org/sirtfi/sirtfi-faqs

---

Questions on Sirtfi Assertions

Operational Security [OS]

- [OS1] Security patches in operating system and application software are applied in a timely manner.

  Q: *Does this imply that only supported software, for which patches are actively supplied, should be used?*
  A: *Many federated services within research and education rely on custom applications and development due to their age and complexity. Stipulating that only supported software be used may pose unnecessary obstacles for organisations joining the Sirtfi trust framework. OS2 implies that any software deployed by an organisation, custom or otherwise, must be actively maintained in the event that a vulnerability is identified.*

- [OS2] A process is used to manage vulnerabilities in software operated by the organisation.

  Q: *What does [OS2] add to [OS1]? How can you manage security patches in a timely manner if you don't have a process to it?*
  A: *OS1 and OS2 are specified separately to cover the case where vulnerabilities are not necessarily addressed by patches. It also addresses scenarios where software is maintained by the organisation and not a third party.*

- [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats

  Q: *Does this requirement apply to all systems run by an organisation, or just IdP/SP related services?*
  A: *As discussed in the framework: "How comprehensively or thoroughly each asserted capability should be implemented across an organisation's information system assets is not specified. The investment in mitigating a risk should be commensurate with the degree of its potential impact and the* likelihood of its occurrence, and this determination can only be made within each organization". This is applicable to all Sirtfi assertions.

- [OS4] A user's access rights can be suspended, modified or terminated in a timely manner.

  Q: *What is a "timely manner"?*
  A: *The definition of appropriate timescales will vary per organisation based on maturity of the services and resource availability. response time should be commensurate with the scale of the incident.*

  Q: *What can I do if somebody does not respond to me in a "timely manner"?*
  A: *The entity is required to remove their Sirtfi certification if they can no longer comply with the framework. Should an entity fail to respond, work with your contacts within your federation and REFEDS to encourage collaboration.*

- [OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.

  Q: *What is ITIL?*
  A: *ITIL is a standardised glossary of definitions used within the IT community. It is referenced here to limit redefinition of accepted terms. https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_GB-v1-0.pdf*

- [OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

  Q: *Does this security incident response capability need to be documented?*
  A: *Ideally this capability should be documented in the form of policies and procedures. For large organisations there is the expectation that a formalised capability exists. For smaller organisations it is possible that this capability is less formal and may simply be the availability of an individual to handle such incidents. The level of documentation available should be commensurate with the scale of the organisation and services.*

  Q: *Should organisations have equivalent agreements with their subcontractors to ensure an incident response capability exists?*
  A: *Best practice indicates that contracts with subcontractors should cover incident response. These contracts are out of scope in a federated context for the purposes of this framework. The Sirtfi trust framework could be used as a starting point for such contractual agreements.*

Incident Response [IR]

- [IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs.
- [IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.

> ***Q:*** *Are the security incident interactions covered intended to be limited to SAML interactions?*
> ***A:*** *Using the Sirtfi security contact outside the scope of SAML is undefined.*
>
> ***Q:*** *What does [IR2] add to [IR3]? If you are able and willing to collaborate for incident response (as per [IR3]) doesn't that cover that you respond to related requests (as per [IR2]) in timely manner?*
> ***A:*** *This is to highlight the importance of active collaboration, beyond a simple acknowledgment, whether or not your organisation is directly impacted by the incident.*

- [IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust framework.

> ***Q:*** *Can Sirtfi compliant entities request contact information directly interact with end-users?*
> ***A:*** *Sirtfi only mandates that communication between Sirtfi partners must be acknowledged. It is beyond the scope of this framework to demand the release of personal data on request.*

- [IR4] Follow security incident response procedures established for the organisation.

> ***Q:*** *What does [IR4] add to [OS6]? If an organisation has incident response capability (as per [OS6]) but related policies are not followed (as per IR4]) can you really say the organisation has incident response capability?*
> ***A:*** *An incident response capability does not necessarily imply having documented procedures. The two are specified separately in order for the framework to be relevant to a broad spectrum of organisations and highlight the importance of establishing an incident response procedure that addresses interaction with external organisations.*

- [IR5] Respect user privacy as determined by the organisations policies or legal counsel.
- [IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy.

> ***Q:*** *Will I need to use the TLP for all communication once I have agreed to Sirtfi?*
> ***A:*** *The TLP should be used for federated incident response but there is no stipulation for other communication. All communication regarding federated incidents, i.e. incidents affecting the entity in the metadata, must have a traffic light colour assigned. Information on the protocol is widely available, e.g. https://en.wikipedia.org/wiki/Traffic_Light_Protocol*

Traceability [TR]

- [TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.

> ***Q:*** *How can I make sure that my logs are sufficient?*
> ***A:*** *Check your logging configuration to make sure that you are storing timestamps and identifiers. It is important that these logs are available (or can easily be made available) to relevant personnel during incident response; ensure that your organisation has clear procedures on gaining access to logs for security purposes. The following example is an appender to a logback.xml file as used at a typical Shibboleth IdP that employs central logging to yoursysloghost.foo.edu. This example ensures that the IP of the remote client is recorded and may be used as inspiration for IdPs looking to improve the usability of their logs.*

logback.xml appender

```
<appender name="IDP_SYSLOG" class="ch.qos.logback.classic.net.SyslogAppender">
    <syslogHost>yoursysloghost.foo.edu</syslogHost>
    <facility>AUTH</facility>
    <port>514</port>
    <suffixPattern>[%thread] [%logger:%line] - [%mdc{idp.remote_addr}] %msg</suffixPattern>
</appender>
```

> *The following extract shows the modified root element of logback.xml to include IDP_SYSLOG.*

logback.xml <root> element

```
<root>
    <level value="INFO" />
    <appender-ref ref="IDP_PROCESS" />
    <appender-ref ref="IDP_WARN" />
    <appender-ref ref="IDP_SYSLOG" />
</root>
```

- [TR2] Information attested to in [TR1] is retained in conformance with the organisation’s security incident response policy or practices.

Participant Responsibilities [PR]

- [PR1] The participant has an Acceptable Use Policy (AUP).

  Q: *Does this AUP need to be specific for identity federation?*
  A: *No, as long as all activity conducted at entities within the federation is covered by an AUP.*

- [PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.