Service Operations Security Policy Template

Part of the generic WISE-AARC Policy Development Kit

Version 2, 20 Apr 2022

Authors: Members of the WISE Community SCI Working Group, particularly:

Linda Cornwall (UKRI), David Crooks (UKRI), Thomas Dack (UKRI), Sven Gabriel (Nikhef), Baptiste Grenier (EGI Foundation), David Groep (Nikhef), David Kelsey (UKRI), Maarten Kremers (SURF), Alf Moens (GEANT), Ian Neilson (UKRI), Ralph Niederberger (FZJ), Hannah Short (CERN), Uros Stevanovic (KIT), Romain Wartel (CERN)

e-mail: sci-wg@lists.wise-community.org

Other Sources / Attribution / Acknowledgements: "EGI Service Operations Security Policy", used under CC BY-NC-SA 3.0.The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

WISE SCI PDK policy template

When using the policy template text below, Angle brackets "< >" and bold text indicates text which either needs to be replaced with the correct information or it is optional and should be deleted or replaced as indicated. Text in coloured boxes provides advice and guidance and should not be present in the final policy document.

Questions to ask yourself when defining the policy:

- Do you require a generic security contact from Services (e.g. security@site.com) or would individually identifiable contacts in addition be beneficial?
- How quickly do you require a response during a security incident? Is this on a best effort basis, or can a more specific timeframe be expected?
- For how long is a Service obliged to fulfil its obligations after announcing its retirement?
- Which security best practices must be followed/adopted by infrastructure Services? We recommend Sirtfi but there may be others.
- For how long should logs be kept?

Service Operations Security Policy

This policy, version **<X>**, is effective from **<insert date>**.

By running a Service, you agree to the conditions laid down in this document **<and other referenced documents>**. You acknowledge that your Service's connection to the Infrastructure may be regulated for administrative, operational and security purposes if you fail to comply with these conditions. Upon retirement of a Service, the obligations specified in this policy shall not lapse for a period **<of X months>**.

You shall:

The following security specific clauses are recommended for all infrastructures

1. Aim for the safe and secure operation of the Service, which shall not be detrimental to the Infrastructure nor to its Participants.
2.

   We recommend including at least a generic contact point that ensures response regardless of individual personnel availability, and that does not expose personal data. However, you may wish to include additional individuals. Any contact is better than no contact.

   Provide and maintain accurate contact information, including at least one Security Contact. **<This contact SHOULD be responsive regardless of individual personnel availability.>**
3. Respond to requests for assistance with regards to a security incident **<or threat> <on an informal and best effort basis | within X business hours>,** when received from another Participant or the Infrastructure Security team. This includes participation in scheduled exercises to test Infrastructure resilience as a whole.
4.

   Note that a Service may be composed of many components or layers of infrastructure, logs from all of which may need to be combined. You may wish to include more precise guidance to ensure a global overview of service-level traceability.

Retain sufficient system/service generated information (logs), aggregated centrally wherever possible, and protected from unauthorised access or modification, for a minimum period of <X> days, to be used for traceability and forensics in the event of a security incident.

5. Follow IT security best practices, including pro-actively applying updates or configuration changes related to security. The following practices MUST be adopted:

> You may want to consider inserting a static copy, or a dated version, of the external practices in case they are updated.

   a. <Support of the Sirtfi Framework [insert reference] on behalf of your Service>
   b. <Include any additional mandatory practices, such as ISO compliance>
6. Inform users, where appropriate, when their access to your Service has been regulated, and do so only for administrative, operational or security purposes.
7. Promptly inform the Infrastructure Security Officer of any non-compliance with this policy.

> The following clauses are not security specific but are often included in the Service Operations Security Policy if no other suitable policy exists

8. Respect the legal rights of Infrastructure Users and others with regard to their personal data, and only use such data for administrative, operational, accounting, monitoring or security purposes.
9. Not hold Users or other Infrastructure participants responsible for any loss or damage incurred as a result of the provision or use of their Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
10. Ensure that any information you provide regarding the suitability and properties of the Service is as accurate as possible.