UKRI Science and Technology Facilities Council

Applying federated security policy in SRCNet and interTwin

Image © STFC Alan Ford

What are interTwin and SRCNet

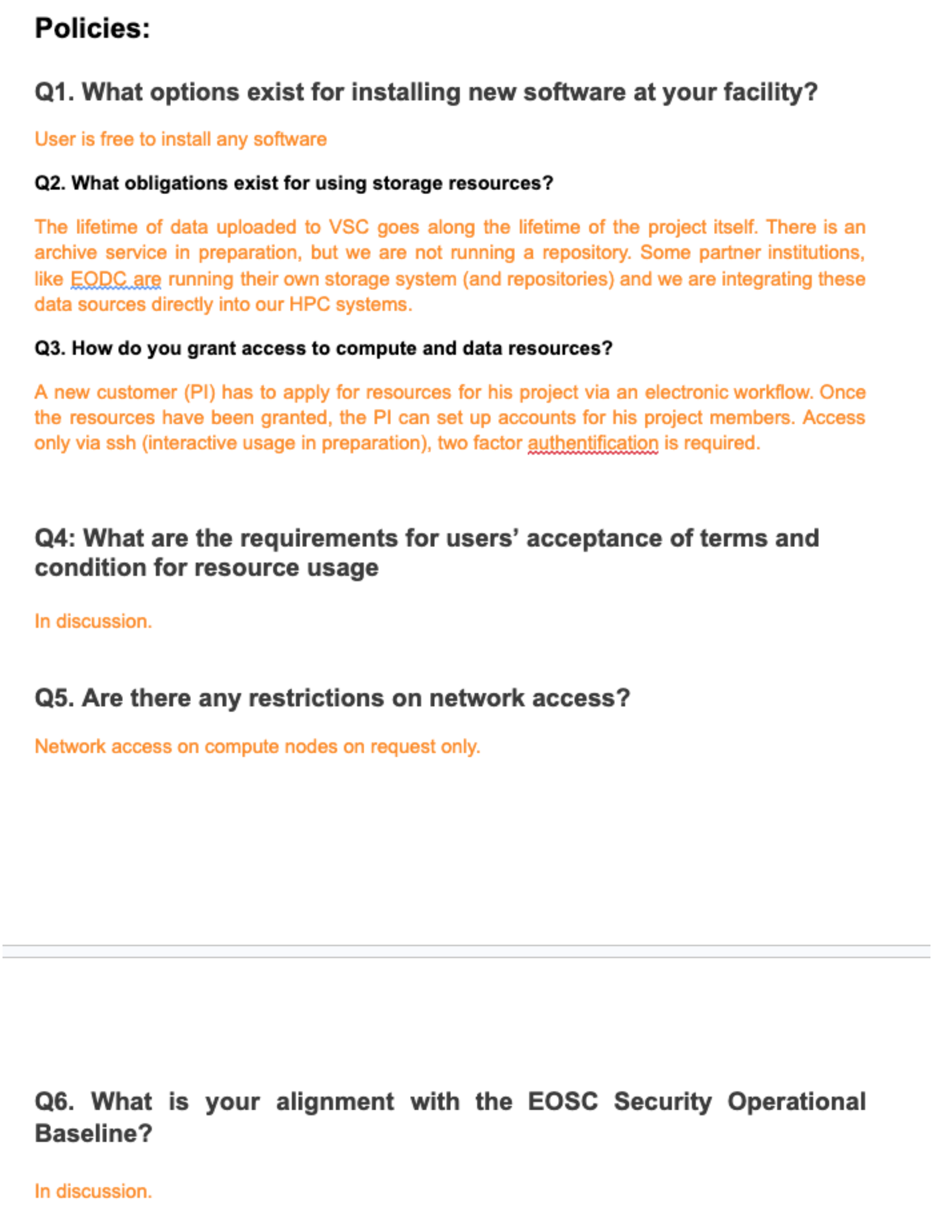
- interTwin
  - EGI digital twin development project
  - Lasting 3 years
  - Ended on the 29th of August 2025
- SRCNet
  - Networking for the SKA astronomy project (space WLCG)
  - This work was preparing for v0.1
    - Services entering production
    - Real data
    - All nodes in 0.1 some time in August

interTwin context

- Small development project
  - Real users on the testbeds
  - Policy covers both the development project and the testbeds
  - Policy templates for use cases as an output of the project
- Environment
  - Cloud
  - HPC
- Auth done with EGI Check-In
  - interTwin is a virtual organisation

interTwin Survey

- Survey covering
  - software and storage options
  - Authorisation
  - Current AUPs
  - Network restrictions
  - Compliance with EOSC baseline
- Clear split between cloud and hpc providers
  - Cloud providers were all active in WLCG and were already using AARC templates or were familiar with them
  - HPC using peer-review access processes with limited access durations
  - All AUPs still compatible
- Question 6 mostly ignored



Policies:

Q1. What options exist for installing new software at your facility?

User is free to install any software

Q2. What obligations exist for using storage resources?

The lifetime of data uploaded to VSC goes along the lifetime of the project itself. There is an archive service in preparation, but we are not running a repository. Some partner institutions, like EODC are running their own storage system (and repositories) and we are integrating these data sources directly into our HPC systems.

Q3. How do you grant access to compute and data resources?

A new customer (PI) has to apply for resources for his project via an electronic workflow. Once the resources have been granted, the PI can set up accounts for his project members. Access only via ssh (interactive usage in preparation), two factor authentification is required.

Q4: What are the requirements for users' acceptance of terms and condition for resource usage

In discussion.

Q5. Are there any restrictions on network access?

Network access on compute nodes on request only.

Q6. What is your alignment with the EOSC Security Operational Baseline?

In discussion.

Science and Technology Facilities Council

interTwin policy set and basis

Policy	Based upon
Top Level	IRIS Infrastructure Security Policy
Acceptable Use	AARC Template https://cloud.jsc.fz-juelich.de/static/dashboard/aup.html https://doc.vega.izum.si/aup/ https://doc.aris.grnet.gr/AUP/ARISTermsofUse.pdf https://eodc.eu/latest_tac https://baltig.infn.it/infn-cloud/policies_and_procedures/-/raw/master/CloudAUP_eng_latest.pdf?inline=true
Service Operations	https://wiki.geant.org/download/attachments/345276462/WISE-SCI-PDK-ServiceOpsSecPol-V2.pdf?version=1&modificationDate=1678990415769&api=v2 https://wiki.eoscfuture.eu/display/EOSCSMS/EOSC+Security+Operational+Baseline https://wiki.eoscfuture.eu/pages/viewpage.action?spaceKey=EOSCSMS&title=EOSC+Security+Operational+Baseline https://search.marketplace.eosc-portal.eu/guidelines/eosc.df8f717f77566b7adde87ede8f55b31d https://zenodo.org/record/7396725
Privacy Notice	https://stfc.github.io/IAM-Docs/policies/iris-privacy/ https://confluence.egi.eu/display/EGIPP/Information+for+End+Users
Processing of Personal Data	https://confluence.egi.eu/display/EGIPP/Policy+on+the+Processing+of+Personal+Data
Incident Response	IRIS Incident Response Procedure

Science and
Technology
Facilities Council

Key Changes

Policy	Based upon
Top Level	Centralisation of definitions and clauses, removal of security coordination. Requirements for incident response and securitycoordination seen as EGI CSIRT scope
Acceptable Use	1) Citation for use of resource 2) Personal responsibility for virtual machines 3) Users solely responsible for ensuring the security of their data
Service Operations	Consistent with IRIS policy Pulled in clauses from HPC centers • not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery • maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Service Operations Policy.
Privacy Notice	Listing exactly what data fields are collected on registration and access. More of a guidance or informational document thana policy
Processing of Personal Data	Same as EGI
Incident Response	Formatting, IRIS and AARC PDK Incident response policies are already dramatically different. IRIS focuses on actions and deadines. New format for clarity

Retrospectively

- HPC does their own AuthN and AuthZ
  - Usually passports and SSH keys
  - Not possible to fully address federation within the project
    - Time and effort limitation
- No disagreement in principle for the proposed policies
  - Due to limited duration, a lot of clauses removed
  - Service Operations
- Questionable as to how useful doing this work is for a development project

SRCNet Context

- Large development project (using agile)
  - 9 Nodes (countries)
- SRCNet is the data transfer, storage and processing for the SKA project
- Agree and compose a small set of initial policies
  - No data until 0.1
  - Some services already running
  - Reuse of existing services (IAM/FTS and more)
- AuthN
  - Existing users onboarded through creating accounts with ska email and username
  - Few enough users that participation in meetings is enough
  - Plan to use 3rd party software to check passports and then create accounts
- AuthZ
  - User accounts created and maintained by SKAO
    - (username/password)
- My Familiarity with exact workings ended almost a year ago

Science and
Technology
Facilities Council

Templates used

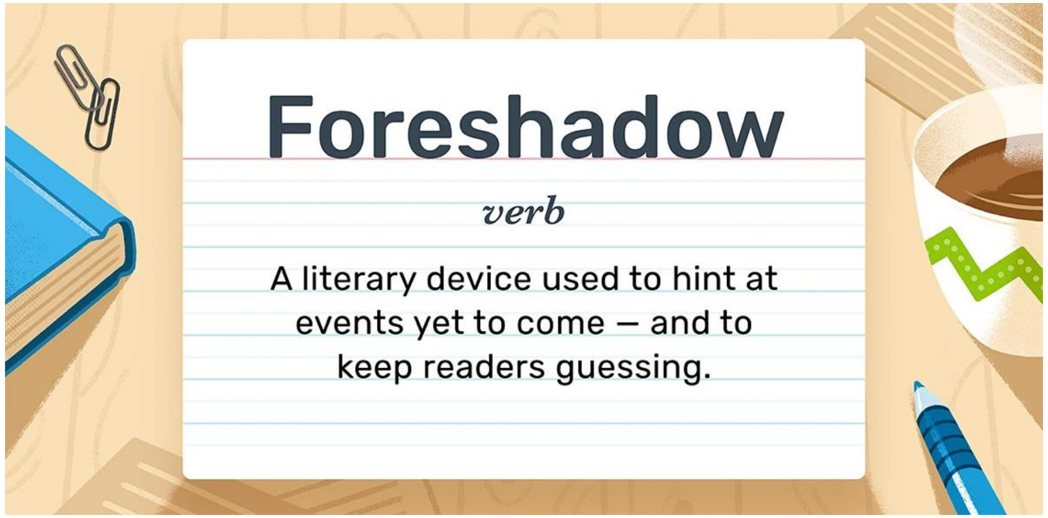
- IRIS
  - Infrastructure Policy
  - AUP
  - Service Providers
  - Incident Response
- Nothing covering processing of personal data, no data protection
  - There will only be science data in 0.1
  - IAM has a privacy policy

What we did and how it worked

- Copy IRIS policies
- Adjust for global rather than UK federation
- Agree approvals process and risk ownership within SKA
    - Least senior person capable of owning the risk
    - Approval by representative from each individual node
- Complexity by the difference in nodes
    - Some are 3 people and have no lawyers/people with policy experience/don’t have a signing process
    - Some are STFC and SURF (at the time) plus other orgs in their country
    - Technical documents so approval in the appropriate team

What went wrong as of the 1st of September 2024

- Nothing
- Presentations given to project as a whole to get feedback which
  - Constructive
  - Lots of comments on the AUP and Service Providers
  - No comments on longer/denser documents
- All policies written in the correct template and format
- Agreement with the SRCNet Project manager on the process for approval and ownership of risk
- Approvers for the nodes identified
- policies socialised with nodes



Foreshadow

verb

A literary device used to hint at events yet to come – and to keep readers guessing.

Science and Technology Facilities Council

What went wrong planning week 2nd- 6th

- Scope Creep and Agile Frameworks

During Planning week (May)	First seen 3rd of September (written on the Sunday just before)
All with the context of being sufficient for v0.1: - The contents of the MUST have policies has at least been been drafted and shared - The policy maker group have endorsed the list of MUST have policies for v0.1 - The contents of the SHOULD have policies has (at least) been been drafted and shared	All with the context of being sufficient for v0.1, regarding the Security group of policies: MUST have policies: * Have appointed Owners, Endorsers, Reviewers and Authors (you may have to speak to PT, see procedures page) * Contents has been drafted and shared with the ART * Have been *endorsed* SHOULD have policies: * Have suggested Owners, Endorsers, Reviewers and Authors * Contents has been drafted and shared with the ART NFRs: - Policies are migrated into a common template that has language consistent with the policy setting procedures written by PT - All past comments have been actioned (that action could be to make the change or consciously not make the change)

- Agreement from here to deliver new work in the next 3 months (before 0.1)

Science and
Technology
Facilities Council

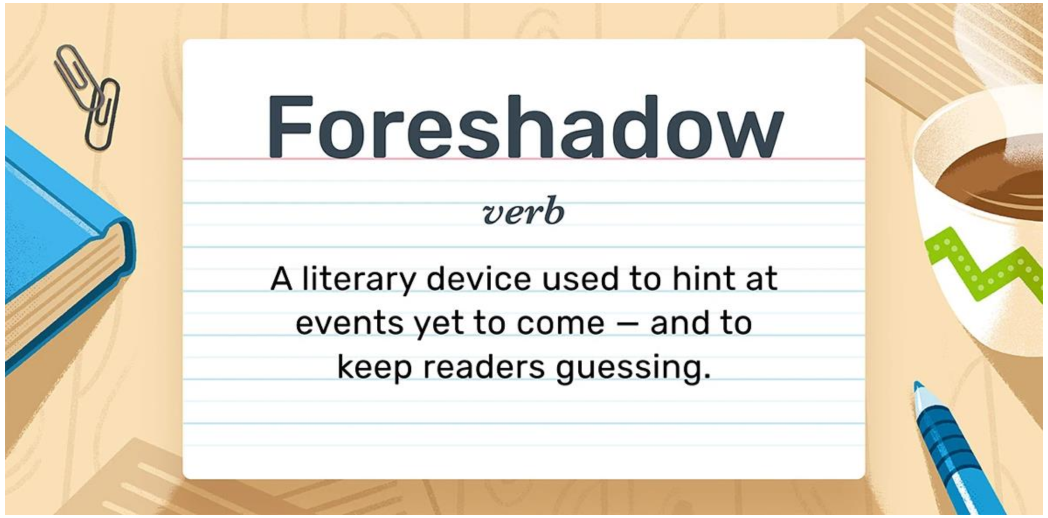
How did we go forwards

- Agreement from here to deliver new work in the next 3 months (3 months before 0.1)
- Decision to time-limit the policies so that future work is required before implementation in 0.2
- Agreement to resolve comments on the policies as soon as they appear
- Agreement to use all of the templates (including user facing policies) despite added bloat
    - Title Page (signings, general metadata)
    - Endorsers list and process for changes
    - Table of contents page
    - Outline and Scope
    - Acknowledgements
    - Definition of terms
    - References
    - Document history and maintenance

What went wrong 6th September - 4th October

- Nothing
- New templates applied to policies
- Final presentation given to approvers while in Zurich Airport flying to EGI conference on 30th of September
- Looking forward my holiday for all of next week 7th -11th of October

FRAMING THE LANDSCAPE
MANY PEOPLE LOOK BUT ONLY A FEW SEE
In partnership with National Trust
Sponsored by



Foreshadow

verb

A literary device used to hint at events yet to come – and to keep readers guessing.

What went wrong Saturday 5th of October onwards

- Surprise rewrite and reformat of all security policy
- Not policies anymore
  - “Operating Level Agreements”
  - Don’t need agreement, alignment or enforcement
- Exact details lost to time
  - Looked a lot like corporate security policies with Ctl+C Ctl+V from ISO 27001
  - Parts of policies where they don’t belong
- Only 3 documents, no infrastructure policy
  - Approvals and Maintenance in all policies
  - Responsibilities for management, service providers and users in policies for those groups
  - Exceptions and sanctions section moved to service providers policy
  - Security Officer references removed

How it was fixed

- Security policy removed as a requirement for 0.1
- Find someone new to act as a middle ground
- Awaited installment of SKAO security officer
- Policy writing through inclusion
    - Show what is being done in other federations
    - Invite to relevant conferences
    - Introduce to more senior colleagues

How does the policy framework look now?

- Still OLAs
- Content of the policies back into a workable state
- Some artifacts of change still included
  - Password length
- https://confluence.skatelescope.org/pages/viewpage.action?pageId=274527742
- No work has been done since January

Learnings

- Policy development in agile frameworks needs to be done carefully or not at all
  - Each step is fast but that doesn’t mean you can rush the process
  - Most time taken soclialising and getting approval
- Get direct involvement from federation/project leadership
  - They need to feel like they own the policies
- Need shared understanding on how the work will actually be done
  - Comments on policies are for conversation
  - There is a point from which changing the policies is destructive

Ripley

Inara

Morpheus