New Security Trust and Policies - for WLCG and other Research Infrastructures

David Kelsey (UKRI-STFC)
ISGC 2024, Taipei
26 Mar 2024

(many thanks to David Groep, Maarten Kremers, Ian Neilson, Hannah Short and others in GN5 EnCo, WISE, FIM4R and AARC Community)

Cybersecurity for Research – how?

- *Aim: to maintain the Availability, Integrity and Confidentiality of services and data*
- Standards-based best practice
  - Identify threats and manage risks
  - Security controls are used to mitigate risks
  - Controls can be technical, operational and managerial
- Trust is required to enable interoperation between Research Infrastructures
  - And to allow operational security teams to collaborate and share information
- Managerial security controls include:
  Security Policies and Trust Frameworks

Science and Technology Facilities Council

Outline of talk

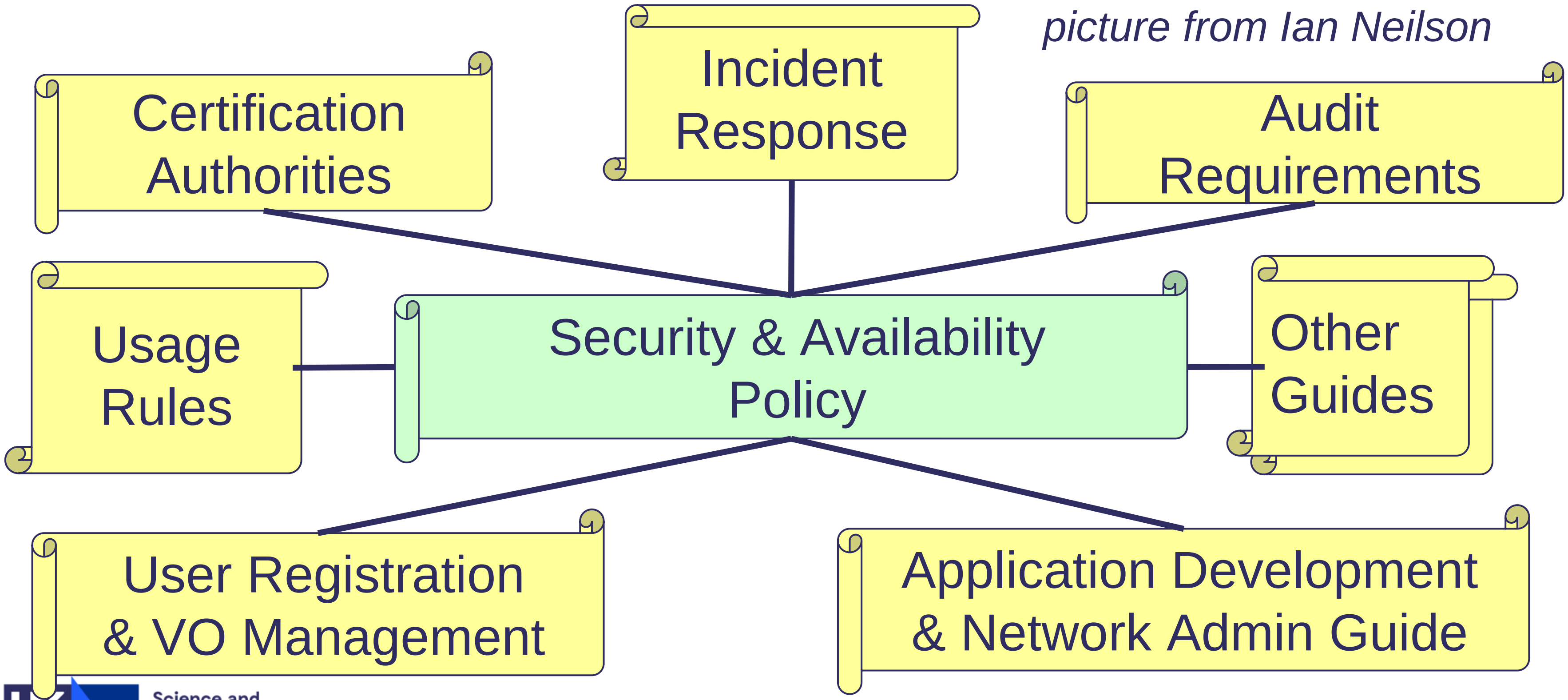
- Brief History of Trust and Policy
    - Joint (WLCG/EGEE/OSG) Security Policy Group
    - FIM4R requirements
    - WISE Security Collaborating Infrastructures Trust Framework
    - AARC Policy Development Kit (PDK)
- Updating the AARC PDK
    - Evolution of the policy templates
    - AARC TREE, AEGIS, AARC Community (with WISE SCI)
- WLCG Trust, Security and Identity activities
- Updating Security Policies for WLCG – what? And how?

History - WLCG Security Policy

- An agreed Security Policy (20 years ago)
  - Written by Joint (WLCG/EGEE/OSG) Security Policy Group
  - Approved by the Grid Deployment Board/Management Board
- A single common policy for the whole project
  - *Augments* local site policies
- The policy
  - Defines *Attitude* of the project towards security and availability
  - Gives *Authority* for defined actions
  - Puts *Responsibilities* on individuals

Science and
Technology
Facilities Council

WLCG Policy - snapshot - years ago



picture from Ian Neilson

Certification Authorities

Incident Response

Audit Requirements

Usage Rules

Security & Availability Policy

Other Guides

User Registration & VO Management

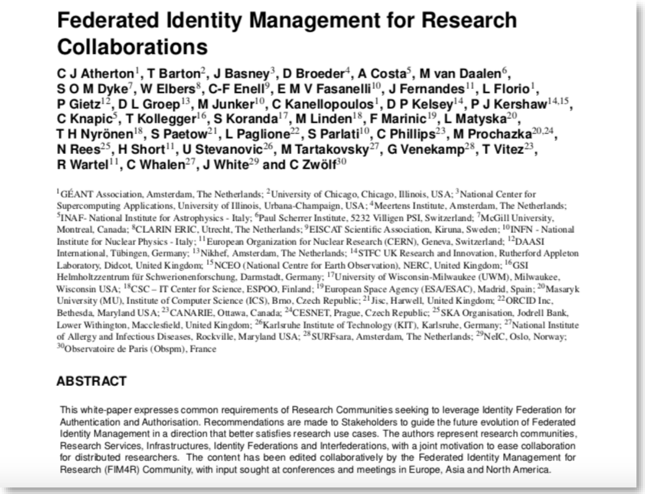
Application Development & Network Admin Guide

Federated Identity Management for Research (FIM4R)

- *FIM4R is a collection of research communities and infrastructures with a shared interest in enabling Federated Identity Management for their research cyber infrastructures*
- FIM4R version 1 paper – 2012
- FIM4R version 2 paper – 2018
- http://doi.org/10.5281/zenodo.1296031
  - Published on 9 July 2018

FIM4R agreed common requirements for Identity, Security and Trust

Maarten Kremers will talk about FIM4R on Friday at ISGC2024



Federated Identity Management for Research Collaborations

C J Atherton[1], T Barton[2], J Basney[3], D Broeder[4], A Costa[5], M van Daalen[6], S O M Dyke[7], W Elbers[8], C-F Enell[9], E M V Fasanelli[10], J Fernandes[11], L Florio[1], P Gietz[12], D L Groep[13], M Junker[10], C Kanellopoulos[1], D P Kelsey[14], P J Kershaw[14,15], C Knapic[5], T Kollegger[16], S Koranda[17], M Linden[18], F Marinic[19], L Matyska[20], T H Nyrönen[18], S Paetow[21], L Paglione[22], S Parlati[10], C Phillips[23], M Prochazka[20,24], N Rees[25], H Short[11], U Stevanovic[26], M Tartakovsky[27], G Venekamp[28], T Vitez[23], R Wartel[11], C Whalen[27], J White[29] and C Zwölf[30]

[1]GÉANT Association, Amsterdam, The Netherlands; [2]University of Chicago, Chicago, Illinois, USA; [3]National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign, USA; [4]Meertens Institute, Amsterdam, The Netherlands; [5]INAF- National Institute for Astrophysics - Italy; [6]Paul Scherrer Institute, 5232 Villigen PSI, Switzerland; [7]McGill University, Montreal, Canada; [8]CLARIN ERIC, Utrecht, The Netherlands; [9]EISCAT Scientific Association, Kiruna, Sweden; [10]INFN - National Institute for Nuclear Physics - Italy; [11]European Organization for Nuclear Research (CERN), Geneva, Switzerland; [12]DAASI International, Tübingen, Germany; [13]Nikhef, Amsterdam, The Netherlands; [14]STFC UK Research and Innovation, Rutherford Appleton Laboratory, Didcot, United Kingdom; [15]NCEO (National Centre for Earth Observation), NERC, United Kingdom; [16]GSI Helmholtzzentrum für Schwerionenforschung, Darmstadt, Germany; [17]University of Wisconsin-Milwaukee (UWM), Milwaukee, Wisconsin USA; [18]CSC – IT Center for Science, ESPOO, Finland; [19]European Space Agency (ESA/ESAC), Madrid, Spain; [20]Masaryk University (MU), Institute of Computer Science (ICS), Brno, Czech Republic; [21]Jisc, Harwell, United Kingdom; [22]ORCID Inc, Bethesda, Maryland USA; [23]CANARIE, Ottawa, Canada; [24]CESNET, Prague, Czech Republic; [25]SKA Organisation, Jodrell Bank, Lower Withington, Macclesfield, United Kingdom; [26]Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany; [27]National Institute of Allergy and Infectious Diseases, Rockville, Maryland USA; [28]SURFsara, Amsterdam, The Netherlands; [29]NeIC, Oslo, Norway; [30]Observatoire de Paris (Obspm), France

ABSTRACT

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

FIM4R - Who is represented?

Research Fields (14)

- Arts and Humanities
- Climate Science
- Earth Observation
- European Neutron and Photon Facilities
- Gamma-Ray Astronomy
- Gravitational Wave Astronomy
- High Energy Physics
- Ionospheric and Atmospheric Science
- Infectious Disease Research
- Life Sciences
- Linguistics
- Nuclear Physics
- Radio Astronomy
- Virtual Atomic and Molecular Data Centre

Others

Research Driven Services

- HNSciCloud
- ORCID

Identity Federations/Projects/Communities

- AARC(2)
- GÉANT-GN4, GN5
- InCommon/Internet2
- REFEDS

The WISE Community

Community members come from e-Infrastructures across the world

- *The WISE community enhances best practice in information security for IT infrastructures for research.*
- *WISE fosters a collaborative community of security experts and builds trust between IT infrastructures*

Security for Collaborating Infrastructures - The WISE SCI working group (SCI-WG)

WISE COMMUNITY

SCI Version 2 – published 31 May 2017 (TNC17) (version 1 was published at ISGC2013)

WISE COMMUNITY

A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

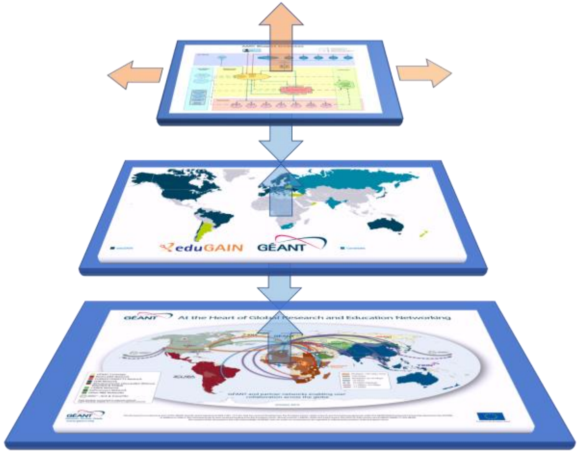
The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

Authentication and Authorisation for Research Collaboration

- EC-funded projects
  - AARC (2015-2017)
  - AARC2 (2017-2019)
- 25 Partners: NRENs, research and e-Infrastructure providers as equal partners
  - Focus on enabling FIM for eScience
- https://aarc-project.eu/

Watch the AARC video to find out more: https://tinyurl.com/What-is-AARC

“Authentication and Authorisation for Research Collaboration” Results



Blueprint Architecture

+

Guidelines & Recommendations

+

SIRTFI

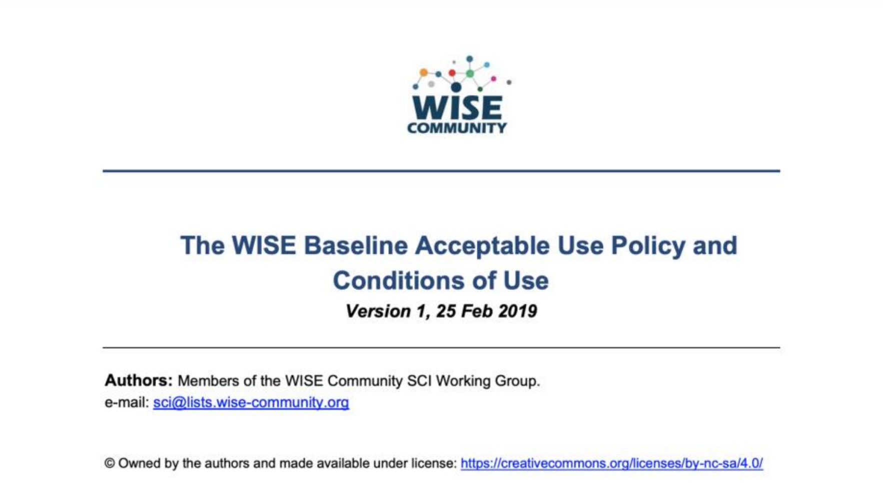
Snctfi

Policy Frameworks & Policy Development Kit (PDK)

WISE Baseline AUP (from the AARC PDK)

https://wise-community.org/wise-baseline-aup/

- a common baseline
- ease trust of users across infrastructures
- community and infrastructure-specific augmentation



WISE COMMUNITY

The WISE Baseline Acceptable Use Policy and Conditions of Use

Version 1, 25 Feb 2019

Authors: Members of the WISE Community SCI Working Group.
e-mail: sci@lists.wise-community.org

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/

Maintenance of AARC PDK by WISE SCI-WG

- Policy templates are useful to new Infrastructures and help build trust and interoperability (as compliant with SCI Trust Framework)
- Involve experience from many Infrastructures and policy groups (including AEGIS) https://aarc-project.eu/about/aegis/
- WISE SCI-wg collects feedback from Infrastructures
    - And uses this if/when a new version of a template is required
- The work of WISE SCI-WG was presented at ISGC2023 (Maarten Kremers)

The Future – AARC TREE project (2-year project)

- Authentication and Authorisation for Research Collaboration Technical Revision to Enhance Effectiveness
- Started March 2024 and run for two years
- Need to target small and medium research communities, simplify the AARC PDK, establish Trust and Interoperability where multiple proxies are connected
- FIM4R.org seen as an important place to discuss and establish requirements
- We will develop the AARC PDK in an open environment
  - AEGIS policy working group/AARC Community/WISE SCI-WG

David Groep will talk about AARC TREE on Friday at ISGC2024

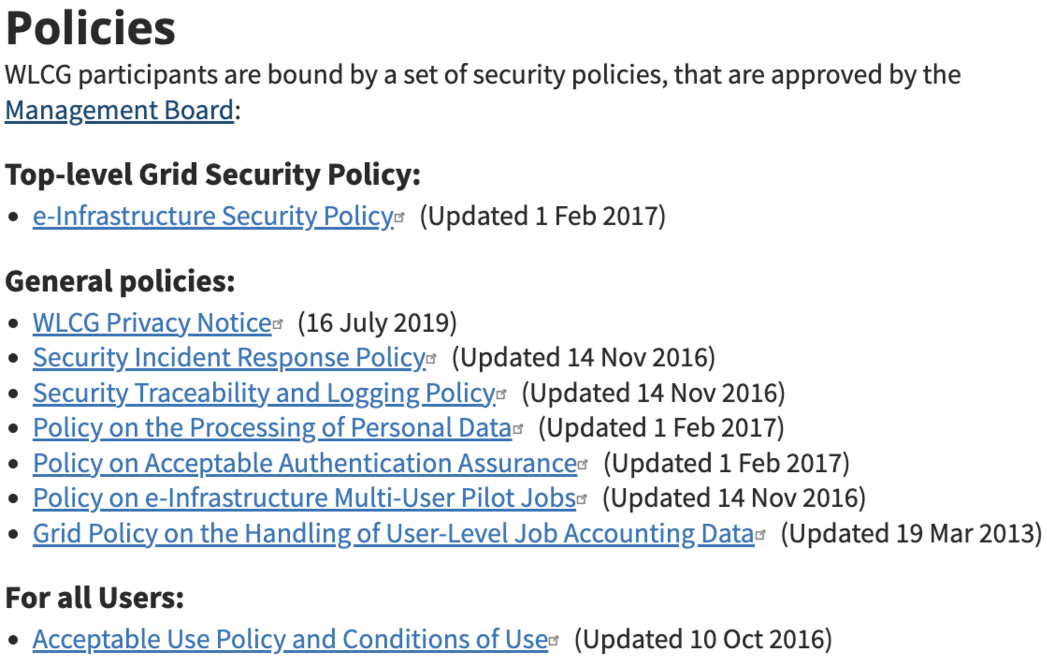
WLCG Trust, Security and Identity activities (but not just for WLCG)

- *Policy Group (see later)*
- *AuthZ working group*
  - Implement use of tokens (move from X.509 certificates)
  - Some policy and trust but mainly delegated to TTT group
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG
- *Resource Trust Evolution task force*
  - Which CA's can be used in cloud storage?
  - https://twiki.cern.ch/twiki/bin/view/LCG/ResourceTrustEvolution
- *Token Trust and Traceability (TTT) working group*
  - Answer security questions in various kinds of documentation
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGTokenTrustTraceability

Science and Technology Facilities Council

WLCG Security Policy

https://wlcg.web.cern.ch/using-wlcg/computer-security



Policies

WLCG participants are bound by a set of security policies, that are approved by the Management Board:

Top-level Grid Security Policy:

- e-Infrastructure Security Policy (Updated 1 Feb 2017)

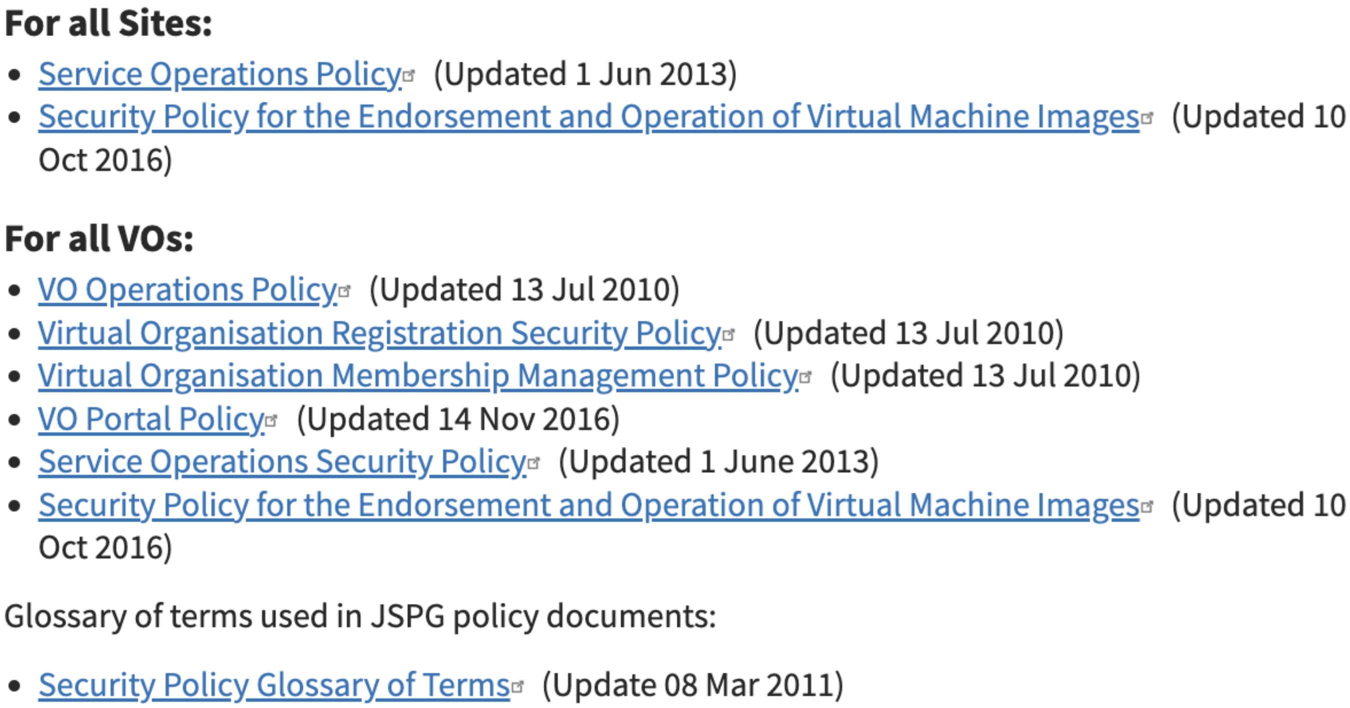
General policies:

- WLCG Privacy Notice (16 July 2019)
- Security Incident Response Policy (Updated 14 Nov 2016)
- Security Traceability and Logging Policy (Updated 14 Nov 2016)
- Policy on the Processing of Personal Data (Updated 1 Feb 2017)
- Policy on Acceptable Authentication Assurance (Updated 1 Feb 2017)
- Policy on e-Infrastructure Multi-User Pilot Jobs (Updated 14 Nov 2016)
- Grid Policy on the Handling of User-Level Job Accounting Data (Updated 19 Mar 2013)

For all Users:

- Acceptable Use Policy and Conditions of Use (Updated 10 Oct 2016)

WLCG - too many policies & need updating



For all Sites:

- Service Operations Policy (Updated 1 Jun 2013)
- Security Policy for the Endorsement and Operation of Virtual Machine Images (Updated 10 Oct 2016)

For all VOs:

- VO Operations Policy (Updated 13 Jul 2010)
- Virtual Organisation Registration Security Policy (Updated 13 Jul 2010)
- Virtual Organisation Membership Management Policy (Updated 13 Jul 2010)
- VO Portal Policy (Updated 14 Nov 2016)
- Service Operations Security Policy (Updated 1 June 2013)
- Security Policy for the Endorsement and Operation of Virtual Machine Images (Updated 10 Oct 2016)

Glossary of terms used in JSPG policy documents:

- Security Policy Glossary of Terms (Update 08 Mar 2011)

WLCG Security Policies

And same is true of the AARC Policy Development Kit

- Many are now old
- There are too many of them
- Other Research Infrastructures are confused (by AARC PDK)
  - Where and how to start?
  - Do we have to use all of them?

Future plans for WLCG security policy

- AARC TREE starts (March 2024)
  - further develop PDK and Guidance and SCI/Snctfi trust frameworks
- EGI and EOSC have already used some of the new AARC templates
  - WLCG needs to do the same
  - Simplification and revision of the WLCG policy set
- As ever - the work will be useful for other Research Communities too
  - Not just for WLCG
  - Will provide feedback to AARC-TREE
- Volunteers very welcome to join the WLCG Policy group
  - And the AARC Community activities
  - Lots of work to do in the 2024 and 2025
  - Please contact me

Science and
Technology
Facilities Council

More information – PDK (before AARC-TREE)

The original AARC PDK: https://aarc-community.org/policies/policy-development-kit/

- AARC guidance documents on policy: https://aarc-project.eu/guidelines/#policy

WISE Community: https://wise-community.org/

- WISE SCI-WG – Wiki - https://wiki.geant.org/display/WISE/SCI-WG
- WISE SCI-WG PDK updates - https://wiki.geant.org/display/WISE/Policy+Development+Kit

Join WISE mail list: https://lists.wise-community.org/sympa/info/wise
Join WISE SCI-WG: https://lists.wise-community.org/sympa/subscribe/sci-wg

Questions?

Science and
Technology
Facilities Council