

## EGI Security Policy and SCI self-assessment

David Kelsey  
STFC-RAL



- EGI Security Policy Group
- SCI self-assessment

# EGI Security Policy Group

<https://wiki.egi.eu/wiki/SPG>

<https://documents.egi.eu/document/64> (ToR)

## *SPG Purpose and Responsibilities*

- Develop and maintain Security Policy
  - For use by EGI and NGIs
  - Define expected behaviour of NGIs, Resource Centres, Users and others
  - To facilitate the operation of a secure and trustworthy DCI
- May also provide policy advice on any security matter related to operations

## *SPG Membership*

- Each (associate) participant of EGI.eu is entitled to nominate one voting member
  - But consensus wherever possible
- Also each external Resource Infrastructure Provider with signed MoU
- In addition, SPG should aim to include expertise in its deliberations from other stakeholders

- Current EGI Security Policy is available at <https://wiki.egi.eu/wiki/SPG>
- As formally adopted by EGI.eu

## Top-level Grid Security Policy:

- Grid Security Policy

## For all Users:

- Grid Acceptable Use Policy

## For all Sites:

- Service Operations Security Policy
- Security Policy for the Endorsement and Operation of Virtual Machine Images

For all VOs:

- VO Operations Policy
- Virtual Organisation Registration Security Policy
- Virtual Organisation Membership Management Policy
- VO Portal Policy
- Service Operations Security Policy
- Security Policy for the Endorsement and Operation of Virtual Machine Images



Other policies for all Grid participants:

- Traceability and Logging Policy
- Security Incident Response Policy
- Approval of Certificate Authorities
- Policy on Grid Pilot Jobs
- Grid Policy on the Handling of User-Level Job Accounting Data

Glossary of terms used in security policy documents:

- Security Policy Glossary of Terms
- And the general EGI glossary

# Security for Collaborating Infrastructures (SCI)

- To evaluate extent to which requirements are met, we recommend Infrastructures to assess the maturity of their implementations
- According to following levels
  - Level 0: Function/feature not implemented
  - Level 1: Function/feature exists, is operationally implemented but not documented
  - Level 2: ... and comprehensively documented
  - Level 3: ... and reviewed by independent external body

- See spreadsheet

Questions?