EGI/WLCG Security Policies

David Kelsey (STFC-RAL)

WLCG GDB, CERN
14 December 2016

www.egi.eu

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Outline

Update since GDB January 2016

- EGI SPG – updated/new policies in 2016
- EGI SPG – policies not yet formally adopted
- SPG plans for 2017
  - Including collaboration with others
  - E.g. WISE SCIV2-WG

Policies which have been revised by SPG and adopted by EGI during 2016
but NOT yet adopted by WLCG

AUP and Conditions of Use

AUP (version 2) to address

- Generalise to include all EGI service offerings
  - HTC, Clouds, etc. (remove the G word!)
- Require: acknowledge support in publications

https://documents.egi.eu/document/2623

- Adopted by EGI on 10 Oct 2016

VM Endorsement & Operation

- This policy started life in the HEPiX Virtualisation WG
- Needed to modify the policy and trust issues
  - To reflect current use cases
- Important for EGI Federated Cloud Services
  - New trust and responsibilities
- Defined terms
  - VM Operator – responsible for all security aspects
  - VM Consumer – end user with no privileges
- *https://documents.egi.eu/document/2729*
- Version 4 adopted by EGI on 10 Oct 2016

Other revised policies

- Also adopted on 10 Oct 2016
  - EGI Access Platform (LTOS) AUP & Security policy
- More revisions – all adopted by EGI on 14 Nov 2016
  - Changes to terminology to bring up to date
    - "Grid" becomes "e-Infrastructure"
    - "Site" becomes "Resource Centre"
  - Update links to other policies
  - Otherwise no change to the policy words
- VO Portal Policy
- Policy on e-Infrastructure Multi User Pilot Jobs
- Security Traceability and Logging Policy
- Security Incident Response Policy

Policies which have been revised by SPG yet still to be adopted by EGI

(feedback welcome from WLCG)

Other revised policies

Finalised earlier this year

- **Personal Data Protection Policy**
  - OMB meeting: March 2016
  - Ready – and proposed now as basis for EGI CheckIn Privacy
  - https://documents.egi.eu/document/2732
- **Acceptable Authentication Assurance**
  - Approved OMB: July and Sep 2016
  - https://documents.egi.eu/document/2930
  - Awaiting approval and adoption

Revised Top-Level Security Policy

Thanks to David Groep for slides on this

Current version (doc #86) is 'well matured', dating July 2010, and wording does not immediately indicate its relevance to new infrastructure concepts (although it does apply)

- Reword in **technology-agnostic** way
- Keeps **subsidiarity principle** that characterizes our current security model
- **Clarify applicability** to each constituency ("participants")
- Points to **common processes** as much as possible
- **Use existing policies** from our suite to assign responsibilities and give mandates

Structure

2. Introduction and Definitions
3. Roles and Responsibilities
    1. The Management
    2. The e-Infrastructure Security Officer and the CSIRT
    3. User Community Management
    4. Users
    5. Resource Centre Management
4. Physical Security
5. Network Security
6. Exceptions to Compliance
7. Sanctions

Example: User Community Management

The *User Community Management* must designate a Security contact point [...]

The *User Community Management* should abide by the *e-Infrastructure* policies in the areas of Acceptable Use, User Registration and Membership Management and all other applicable policies. Exceptions to this must be handled as in section Exceptions to Compliance. They must ensure that only individuals who have agreed to abide by the *e-Infrastructure* AUP and the User Community AUP are registered as members of the *User Community*.

User Community Management and *Users* that provide and/or operate *resources* or *services* must abide by the Service Operations Security Policy, the Traceability and Logging Policy and all other applicable policies.

For services requiring authentication of entities the *User Community Management* must abide by the policy on Acceptable Authentication Assurance.

User Community Management is responsible for promptly investigating reports of *Users* failing to comply with the policies and for taking appropriate action to limit the risk to the *e-Infrastructure* and ensure compliance in the future, as defined in section Sanctions.

Exceptions to compliance

Wherever possible, *e-Infrastructure* policies and procedures are designed to apply uniformly to all *participants*.

If this is not possible, for example due to legal or contractual obligations, exceptions may be made.

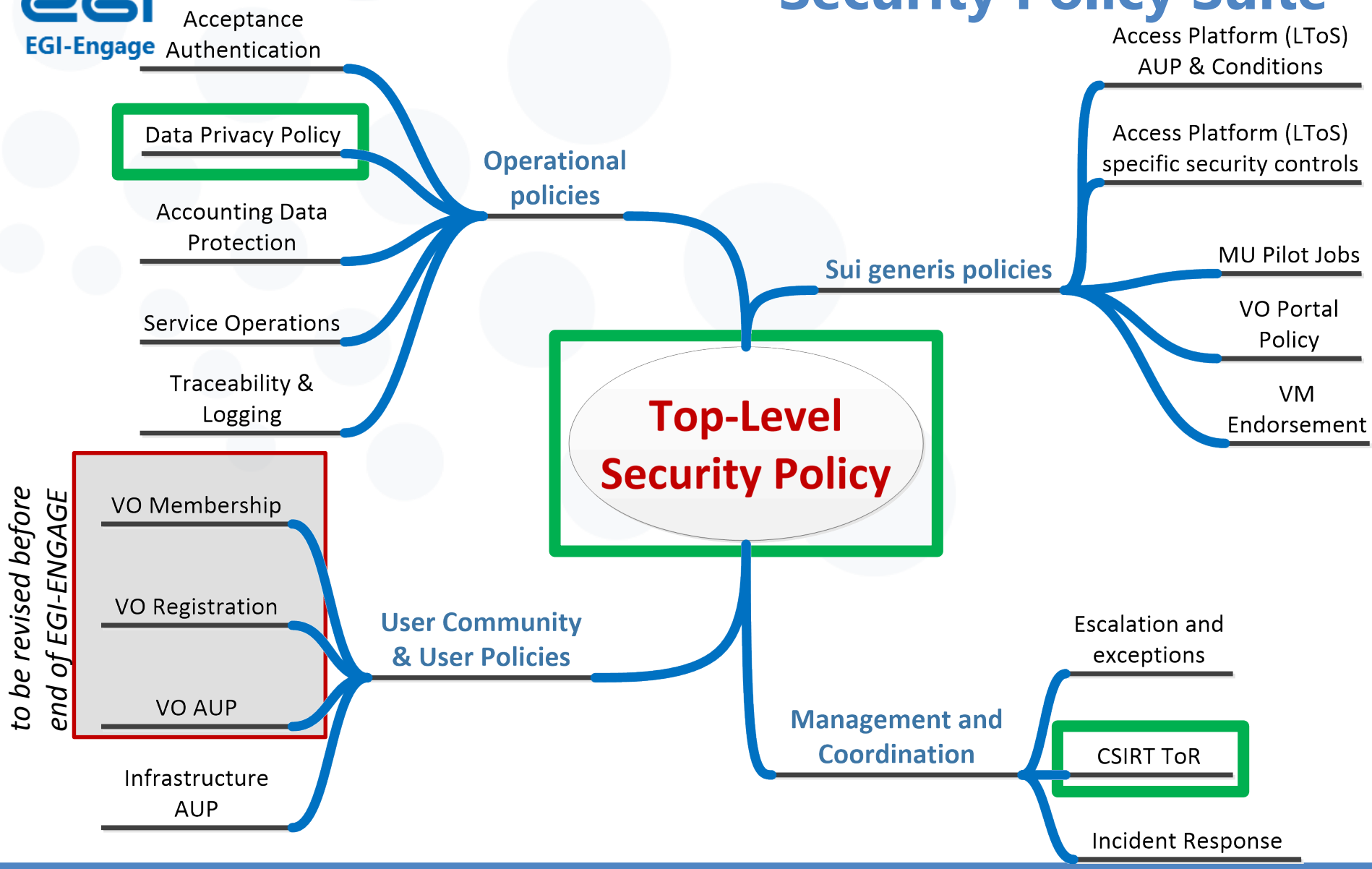
Such exceptions should be time-limited and must be documented and authorised
by the *e-Infrastructure* Security Officer and,
if required, approved at the appropriate level of management.

…

Plans for EGI SPG in 2017

Slide from David Groep

Security Policy Suite



Future work items

User-community related security policies

- Today there are three policies for "VOs": registration, membership management, operations & the AUP – which is too many, are too vague, and inadvertently suggests some technology. But they are tech-agnostic!
- Policy documents govern *relationships*
- User Communities relate
  - **with their constituent users**, for which we can provide reference templates (it says "should abide" in the top-level policy, i.e. uses a "comply or explain" model)
  - **with the infrastructure**, for which we are authoritative ("must abide")
- *SPG will propose revised community policies before the end of EGI-Engage*

Other Policy work

- EGI will continue collaboration with other Infrastructures via **WISE and SCIV2-WG**
  - **SCI = Security for Collaborating Infrastructures**
  - **Version 2 will be finalised in 2017**
    - **Will include GEANT and NRENs and other infrastructures**
- Policy and trust issues will also be addressed by AARC
  - SCI has been used for Sirtfi and Snctfi frameworks
- We will continue to identify
  - potential further gaps
  - inconsistencies

Requests to WLCG GDB

- We will be asking WLCG MB to adopt the new top-level Security Policy (during 1st quarter of 2017?)
  - Please provide feedback soon if you have any
- We will also (at the same time) seek approval to adopt all other policy documents which have been adopted by EGI during 2016
  - I will create versions in the WLCG document template
  - If there are objections – please let me know soon!
- Data Protection and Acceptable Authentication Assurance will also be finalised by EGI in the coming weeks
  - If EGI can adopt before we seek WLCG MB approval all the better
- We can then seek approval of the complete set!
- The new VO policies will need to follow later in the year.

Thank you for your attention.

Questions?

www.egi.eu