Update - Security Policies

David Groep (Nikhef)

EGI OMB
24 November 2016

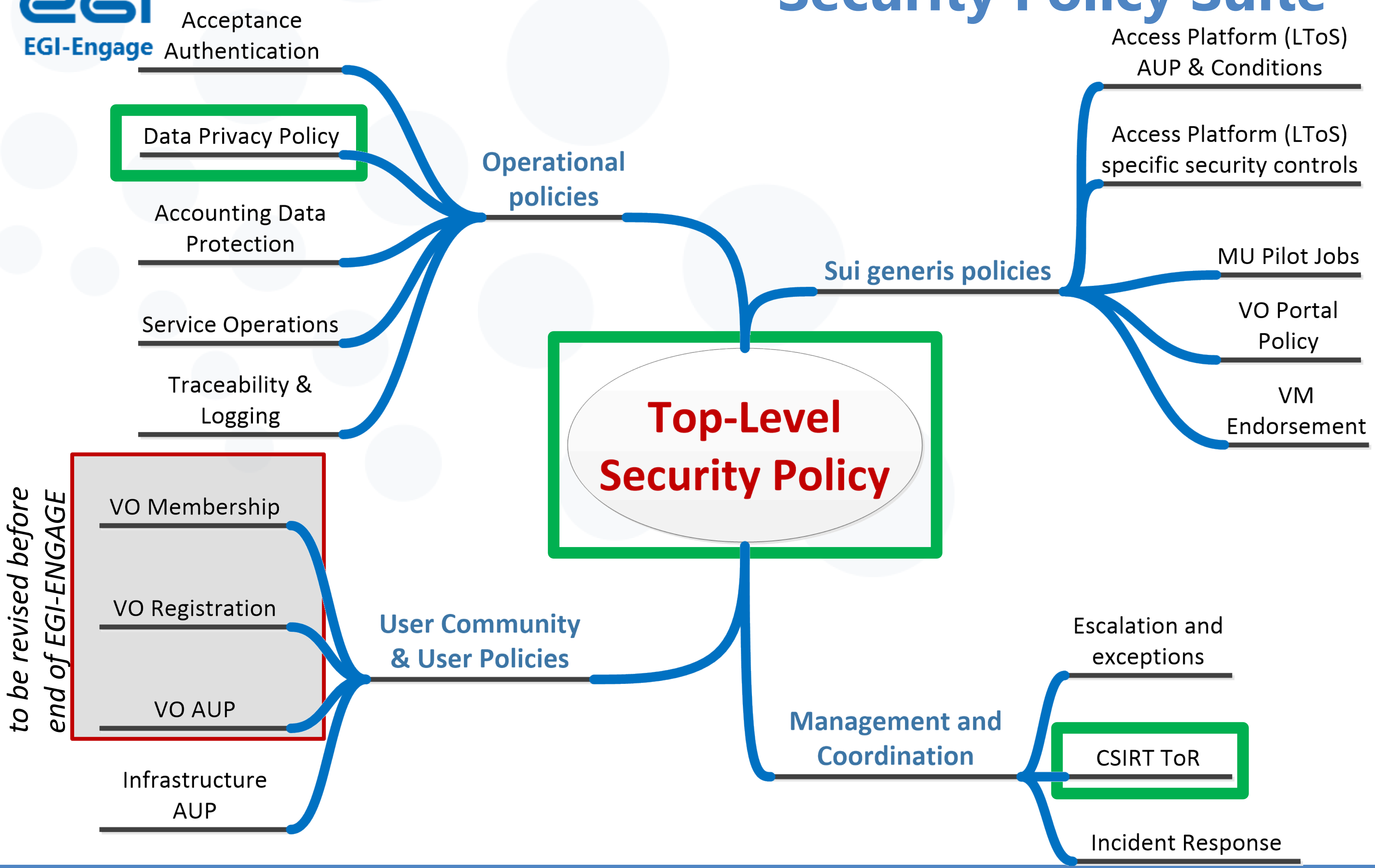
EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Refreshing the security policy suite

Finalised earlier this year

- Formal adoption – Oct 2016:
  LTOS AUP, LTOS Security policy, VMI Endorsement and operations (V4), Revised AUP (V2)
- **Personal Data Protection Policy**
  - OMB meeting: presented March 2016
  - Almost ready – and now used as basis for EGI CheckIn Privacy
    privacy template appendix should evolve taking this into account
  - https://documents.egi.eu/document/2732
- **Acceptable Authentication Assurance**
  - Approved OMB: July and Sep 2016
  - https://documents.egi.eu/document/2930
  - Awaiting formal approval and adoption

Security Policy Suite



Top-Level Security Policy
Operational policies
Acceptance Authentication
Data Privacy Policy
Accounting Data Protection
Service Operations
Traceability & Logging
Sui generis policies
Access Platform (LToS) AUP & Conditions
Access Platform (LToS) specific security controls
MU Pilot Jobs
VO Portal Policy
VM Endorsement
User Community & User Policies
VO Membership
VO Registration
VO AUP
Infrastructure AUP
to be revised before end of EGI-ENGAGE
Management and Coordination
Escalation and exceptions
CSIRT ToR
Incident Response

Top-Level Security Policy

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

- Reword in **technology-agnostic** way
- **Minimal changes**, as the previous policy worked well
- 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.

…

EGI-Engage

EGI CheckIn – Data Privacy Policy

- Builds on the – previously OMB-endorsed – Data Protection policy and the Privacy Template
- Having a privacy policy is a necessary prerequisite
  - For running a service handling personal data
  - For registering the service in eduGAIN with the GEANT DP CoCo “Code of Conduct” trust mark
  - To have all users be well informed on how we process their personal data in the portal and in EGI services

A data privacy policy answers questions!

- What Personal Data do We process?
- Purposes of Processing?
- Stored where?
- Accessed by whom?
- Retained for how long?
- If so: how is your data shared with others?
- Name and Contact details of Data Processor
- Name and Contact details of
  the EGI CheckIn Service Data Protection Officer

But: EGI CheckIn in a just a front!

- EGI CheckIn itself conveyed attributes to others *that the entire purpose of it* ☺
- All services that connect to CheckIn, **must be part of the same policy framework**

- Data protection model for sharing is inspired by the GDPR "Binding Corporate Rules" (BCR) model, that leverages our comprehensive policy set
- Only entities that comply with all the policies, and where we have viable enforcement mechanisms, may have access to the data

10.4 Policy

By their activity in the Infrastructure, Participants:

- Declare that they have read, understood and will abide by the Principles of Personal Data Processing as set out below.
- Declare their acknowledgment that failure to abide by these Principles may result in exclusion from the Infrastructure, and that if such failure is thought to be the result of an unlawful act or results in unlawful information disclosure, they may be reported to the relevant legal authorities.

A first step: getting this to work … ASAP!

The draft data privacy policy for EGI CheckIn
https://wiki.egi.eu/wiki/SPG:Drafts:Data_Privacy_EGI_CheckIn

- Addresses all basic 8 questions
- Has the service-specific
  "EGI Policy on the Processing of Personal Data"

- Is really needed, real soon, like, "yesterday"
- Can be evolved by updating EGI CheckIn website *unless we make user-impacting changes*

Future work items

User-community related security policies

- Today there are three policies for "VOs": registration, membership management, and the AUP – which is too many, are to vague, and inadvertently suggests some technology. But they are tech-agnostic!
- Policy documents govern *relationships*, and communities relate
  - **with their constituent users**, for which we can provide a 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 ENGAGE*

Continue collaboration with other Infrastructures via **WISE and SCIV2-WG**

- Policy and trust issues
- To identify potential further gaps and inconsistencies

Requests to the OMB

- To *endorse* the new top-level security policy https://wiki.egi.eu/wiki/SPG:Drafts:Security_Policy

- To *endorse* the first version of the AAI CheckIn Data Privacy Policy – so that it can be used as of now for informing the users on the processing https://wiki.egi.eu/wiki/SPG:Drafts:Data_Privacy_EGI_CheckIn

- To *(re-)confirm* the CSIRT ToR https://documents.egi.eu/secure/ShowDocument?docid=385&version=11

Thank you for your attention.

Questions?

www.egi.eu