|  |  |
| --- | --- |
| **Meeting:** | Security Policy Group (SPG) |
| **Date and Time:** | 16 June 2011 – 14:00-16:00 |
| **Venue:** | Telecon |
| **Agenda:** | <https://www.egi.eu/indico/conferenceDisplay.py?confId=503> |

Participants 2

MINUTES AND ACTIONS FROM APRIL 2011 MEETING 3

ITEMS OF BUSINESS 3

Editorial team: Service Operations Security Policy 3

Editorial team: Virtual machines endorsement policy 3

AOB 3

Date for Next Meeting 4

Actions 5

# Participants

|  |  |  |
| --- | --- | --- |
| **Participants** | **Abbr.** | **Organisation** |
| **David Kelsey**  | DK | STFC SPG Chair |
| **Damir Marinovic** | DM | EGI.eu Policy Development Officer (Secretary) |
| **Tiziana Ferrari**  | TF | EGI.eu COO |
| **Peter Solagna** | PS | EGI.eu Operations Officer |
| **Linda Cornwall**  | LC | STFC/SVG |
| **Oxana Smirnova** | OS | NDGF |
| **Dorine Fouossong** | DF | IN2P3 |
| **David O’Callaghan** | DO | TCD |
| **David Groep** | DG | Nikhef SPG Deputy Chair |
| **Romain Wartel** | RW | CERN |
| **Mingchao Ma** | MM | STFC EGI Security Officer |
| **David Jackson** | DJ | STFC  |
| **Vincent Ribaillier** | VR | IDRIS/PRACE |
| **Sergio Andreozzi**  | SA | EGI.eu Policy Development Manager |

AGENDA BASHING

DK presented the agenda points and explained that it would be good to focus on the two policy drafts that need to be discussed. DK suggested adding discussion of the draft Common glossary to AOB.

# MINUTES AND ACTIONS FROM APRIL 2011 MEETING

Minutes from the previous SPG meeting held on 12 April were approved.

DK checked with other SPG members the action list from the previous SPG meeting. Several actions were closed. See the table at the end of the minutes for details.

Concerning action 01/03 SA sent email to Steven Newhouse to ask him what kind of membership can have external Resource infrastructure Providers (RPs) that signed MoU - voting or non-voting membership? DK - Whenever possible SPG will act on achieving consensus so it should be acceptable to these MoU signers that they are non-voting members. SA - So far we have signed MoU with Universidade Federal do Rio de Janeiro (UFRJ), one MoU is in final stage with SAGrid (South Africa), and the ones we are still in negotiation phase are with EDGI and other Latin America RP. Steven Newhouse confirmed by email that external Resource infrastructure Providers with whom EGI.eu signed MoU will gain SPG membership **with** voting capabilities. Therefore, action 01/03 is closed and the SPG ToR and the MoU templates should be amended accordingly. DM should propose handling of the SPG ToR amendment and actual changes to the document for the next SPG meeting ***(action 03/01)***

DK asked whether EGI.eu plans to prepare MoU with PRACE. This is important because we have strong representation of PRACE in SPG. SA - So far there was no discussion, we are finalizing MoU with Mapper project that covers certain aspects of collaboration with PRACE. SA will ask Steven Newhouse about possible mode of collaboration with PRACE ***(action 03/02).***

In regard to action 02/03 - Resource Center OLA is approved by OMB and TF sent (today) an email with the OLA <https://documents.egi.eu/document/31>. In agreement with TF, we will follow the PDP so it means OLA will be considered as a policy and it will require formal review by SPG.

# ITEMS OF BUSINESS

## Editorial team: Service Operations Security Policy

DG - There was quite a lot of discussion on internal draft wiki page and I tracked discussion on mailing list. Last comment by PS and all those changes were incorporated.

TF said that she included this text from point 1 in OLA and for her that is redundant. DG - We should keep it taking in account that there is procedure in place. DF – question about Resource Centre OLA TF - requirement to be certified Resource Centre, the idea is to have different OLAs and other who focus on resource providers and the OLA focusing on EGI.eu OS - It is important whoever provide the service to comply with this policy. It should apply to everybody, not only for resource providers. It should be explicitly said that the document apply to all parties. DK - Maybe some VO can say my VO box is not part of the infrastructure. Maybe it is worth to have sentence – all services real or virtualized. DG – It can mean that policy applies also to networks and physical buildings. We don’t want to go that far. Leave the text the way it is. DG - last sentence; add that they can be revised from time to time **(agreed)**

Discussion about Point 4 revised according to DJ suggestion “You should follow IT security best practices that include pro-actively applying software patches, updates or configuration changes related to security. When notified by the Infrastructure or any Resource Centers involved of software patches, updates or configuration changes required for security, you shall apply these to your services within the specified time period” **(agreed)**

POINT 7, 8 and 11. DK - Should these statements be somewhere else?

POINT 7 TF - This could be put under responsibilities of the OLA. We have just approved the final draft so I am reluctant to revise it again.

DK SPG can suggest that these statements (point 7 and 8) be added in the next release of the OLA**.**

POINT 8 This is general statement provided to everyone not only to RC. TF - Statement under Resource Centre responsibility is in the OLA.

POINT 11 DK - Just delete it, it should be in top level security policy. OS - We need clear statement and connection with Top level security policy. DG - Leave it as it is, to leave it vague and with a broader meaning and it is good to have it **(agreed).** TF - OMB have different escalation processes described in different documents so we should clarify what it refers to. We should have Suspension policy, it is in our plans. We need to reference to different procedures. DK - Maybe to keep it general and not to put link. TF - We have operational procedures gathered into single wiki page. That can be solution; it is just a matter of identifying referenced documents. DG - There are number of references that should be put added to the policy draft ***(action 03/03).***

TF - What are the obligation of the suspended sites? It is general problem for existing procedures and policies. DG - How many other policies suffer from the same issue? TF - We said in the OLA that is not binding during suspension. DG - At this point I would not bother. TF - Then site which is not part of the infrastructure can decide not to comply with policies MM - Do we have a procedure for RPs to leave the infrastructure for whatever reason? If site is suspended he is still part of infrastructure and policies should apply. TF - We have procedure for RP to be decommissioned. When you leave there is no reason for doubt. DK – When RCs are leaving, they need to leave traceability and logging information. TF - For suspension which is temporary it is not clear for me. Maybe to make clear that suspended sites will stay part of infrastructure. DK - We don’t mentioned suspension here. DG - point 4, 5 and 6 of the draft remain in effect even after you have left infrastructure, maybe to add sentence at the end. DK - I think it is better to address this in some other document, there are advantages to keep it vague. TF - Stick to the plan in having a suspension policy, it should be clarified than. Maybe we can have interim solution. TF suggestion: Policies are also applicable to service providers that are temporarily suspended. DK - Adding a sentence to introduction.

DK - We have to finalise internal draft by the end of June. We should announce a last call for any final important edit ***(action 03/04).***

## Editorial team: Virtual machines endorsement policy

RW had circulated a draft before the meeting. He described the changes he had made to generalize the existing HEPiX policy on Endorsement of Virtual Machine Images. The document was then discussed in detail.

DK – We need to produce a good internal draft by about the end of June, with an “external” draft by 14th July. For now the old template (HEPiX/WLCG) is used. Later we can put final draft into EGI policy template. RW explained the parts of the draft.

Section 3 Classification and Responsibilities. DK – The term “payload” suggests something limited in time, where a virtualised service is continuing in time. DO – Section 3.1; instead of trusted you can use external.

DK - Whole section 4 should apply to 3.3? RW - I think it should apply to all use cases especially 3.3.

Sometimes to describe these three classes (Third part VO, use case in better way, put some condition to part 4 to make sure it is applied to other sections). DK - Also ability to allow virtualised services e.g. VOs that want to offer services but not running gLite. DK – We should make the classes as general as they can be.

Is the current document title still correct? Most agree that it is still valid. RW – We can name it Policy on management. DK – Policy on endorsement, distribution and operation of VM images or Policy on endorsement and operation of VM images? No agreement yet.

 RW – I will put on the wiki changes for people to comment. DK – It is important that during the coming two weeks we have a complete internal draft followed by a meeting of the editorial team and then to come back to a full SPG meeting in the middle of July followed by going for external consultation ***(action 03/05).***

RW – Do we need to clarify the requirements on VM operators? DG – If EGI uses third party services such as Amazon, then the standard contracts do not bind the VM operator to any policy requirements. These would have to come via additional contracts; e.g. for University email providers they do just that. DK – We should make it clear that we are not addressing this particular issue; a good topic for a future F2F meeting.

## AOB

Common Glossary. DK - What can we do in the short term period? SA - In short term we should have draft and after it get stabilised, the glossary should be approved by the EGI.eu Executive Board. In this moment we have terms from OMB and TCB and we need to bring SPG terms to the glossary. My idea is by Monday (20th June) to make the merge with SPG terms, so SPG members will have one week to comment on additional changes. DK - It took us many months to finalise SPG glossary, it is my concern that we cannot do this in the time you want. Maybe best in the short term to keep the SPG Glossary separate. SA - This draft glossary will not impact policies and procedures. When we have integral common glossary as final and approved, all the policies and procedures will refer to this glossary. DK - For example, for the first Service Operation Security Policy, what terms do we need in glossary; it needs to be investigated. In short term, I will have a look at potential conflicts that are currently in draft common glossary ***(action 03/06).*** SA – We should to try, when it is possible, to harmonise our terms and definitions with ITIL terms and definitions. As soon as you define Service Operations Security Policy (and other new policy documents) you should define terms that should be in Common Glossary ***(action 03/07******)***.

## Date for Next Meeting

It was agreed that the next SPG telecon meeting should be held in the middle of July ***(action 03/08)*** in order to follow the progress of editorial teams on having complete internal drafts and agree on external drafts.

# Actions

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Resp.** | **Description** | **Status** |
| **01/02** | DK | Invite all EGI.eu Council participants to nominate a voting member of SPG | ONGOING |
| **01/03** | SA | Define how external infrastructure providers and virtual research communities can be represented/engaged in SPG (Steve/Gergely) | CLOSED |
| **01/04** | SA | License statement, to make more compact and explain how external partners should mention it | ONGOING |
| **01/05** | DG | Provide English translation for Dutch data protection law, art. 35(?) | ONGOING  |
|  |  |  |  |
| **01/07** | DG&DK | Go through digital agenda items related to trust and security | ONGOING |
| **01/08** | DK | Harmonise security and operation terminology | ONGOING |
| **01/09** | DK | Get rid of “site registration security policy” at the same time as the updated site operations policy is approved | ONGOING |
| **01/12** | DK | Ask TERENA if they have policies in the area of cloud to be considered as base for new top level security policy | ONGOING |
| **02/01** | DK | Ask members to check whether their entry in the membership list is correct | ONGOING |
| **02/02** | DK, TF | Have a phone conference with Operations team before the EGI-InSPIRE review about harmonising security and operation terminology (related to action 01/08) | ONGOING |
| **02/03** | TF | TF should send approved Site operations procedure and OLA to SPG mailing list and check whether SPG agrees with them | ONGOING |
| **02/04** | DG | On the next meeting of editorial team the deadline for the draft version of General services security policy should be set up | CLOSED  |
| **02/05** | DK | Send the list of Editorial team members to RW for generalising the HEPiX VM Endorsement policy to include other types of trustworthy VMs.  | CLOSED |
|  |  |  |  |
| **02/06** | RW | Have an internal draft for the Generalised HEPiX VM Endorsement to include other types of trustworthy VMs by 14 June. | CLOSED |
| **02/07** | DK | Investigate whether the document Security for Collaborating Infrastructures (SCI) overlaps with existing CSIRT agreements | ONGOING |
| **02/08** | DK, SA | Investigate possibility of involvement of Balboni during SPG work on drafting the Data protection policy and what we could offer to him  | ONGOING |
| **02/09** | DK | Set up Doodle poll for the date of next SPG phone conference mtg | CLOSED |
| **03/01** | DM | Propose handling of the SPG ToR amendment and actual changes to the document for the next SPG meeting | NEW |
| **03/02** | SA | Ask Steven Newhouse about possible mode of collaboration with the PRACE | NEW |
| **03/03** | DG/DK | Check what references should be added to the Service Operations Security Policy draft | NEW |
| **03/04** | DG | Announce a last call for any final important edit (Service Operations) | NEW |
| **03/05** | RW | Have a meeting of editorial team within two weeks and complete internal draft in two weeks’ time | NEW |
| **03/06** | DK | Have a look at potential terms and definitions conflicts that are currently present in the common glossary draft | NEW |
| **03/07** | DK and PDT  | Define terms and definitions that should be included in the Common Glossary after the Service Operations Security Policy is finalised  | NEW |
| **03/08** | DK | Set up Doodle poll for the date of next SPG phone conference meeting in July  | NEW |

Minutes prepared by Damir Marinovic, 17.06.2011

Minutes Approved SPG Chair David Kelsey

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

COPYRIGHT NOTICE

Copyright © EGI.eu. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

The work must be attributed by attaching the following reference to the copied elements: “Copyright © EGI.eu (www.egi.eu). Using this document in a way and/or for purposes not foreseen in the license, requires the prior written permission of the copyright holders. The information contained in this document represents the views of the copyright holders as of the date such views are published.