Policy Issues

David Kelsey
GridPP Deployment Board
14 Sep 2005

d.p.kelsey@rl.ac.uk

Introduction

- **Joint Security Policy Group meetings**
  - 12 Sep: JSPG meeting (CERN)
    - http://agenda.cern.ch/fullAgenda.php?ida=a054502
  - 13 Sep: LCG Authorization Workshop (CERN)
    - http://agenda.cern.ch/fullAgenda.php?ida=a054503
- **Topics today**
  - User AUP
  - VO boxes (security aspects)
- **JSPG also discussing**
  - Legal issues – access to accounting at user level
  - Emergency/Disaster recovery plans

User AUP

- Aiming for simple, short, common AUP across LCG, EGEE, OSG, GridPP, ...

- General AUP for all VO's

  – Ties user to the VO-specific AUP

- Showed previous version at Jun 05 DB meeting

  – Concerns about liability, data protection

- Since then

  – consulted lawyers at several sites

  – Work on new draft

  – Now ready for approval process

Draft of 12 Sep 2005

By registering with the Virtual Organization (the "VO") as a GRID user you shall be deemed to accept these conditions of use:

1. You shall only use the GRID to perform work, or transmit or store data consistent with the stated goals and policies of the VO of which you are a member and in compliance with these conditions of use.

2. You shall not use the GRID for any unlawful purposes and not (attempt to) breach or circumvent any GRID administrative or security controls. You shall respect copyright and confidentiality agreements and protect your GRID credentials (e.g. private keys, passwords), sensitive data and files.

User AUP (3)

3. You shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the relevant VO(s) and to the relevant credential issuing authorities.

4. Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose. Although efforts are made to maintain confidentiality, no guarantees are given. Logged information, including information provided by you for registration purposes, shall be used for administrative, operational and security purposes only.

5. The Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions.

6. You are liable for the consequences of any violation by you of these conditions of use.

Security & VO boxes

- Issues
  - Uncertified software running inside our zone
  - Traceability/auditing at individual level
  - No root access
  - Restricted set of users allowed to login
  - Who is responsible? Who installs?
- o/s hardening, iptables, intrusion detection, system call auditing
- Those allowed to login must be bound by Security and Availability policy
- VO Box can sit at "edge" of site. WNs may not have full connectivity.
- JSPG will write a document as input to discussions at Operations workshop