Computer Security

Security incidents

When a security incident potentially affecting grid users, services or operations is suspected, please immediately contact your local security team.

Your local security will then inform the EGI CSIRT or the OSG Security Team, depending on your location.

Further information:

- The EGI Incident Response procedure
- The OSG Incident Response procedure

Policies

WLCG participants are bound by a set of security policies, that are approved by the Management Board:

Top-level Grid Security Policy:

- Grid Security Policy (Version 5.7a)

For all Users:

- Grid Acceptable Use Policy (Version 4.2a)

For all Sites:

- Grid Site Operations Policy (Version 1.4a)
- Site Registration Security Policy (Version 3.2a)

For all VOs:

- VO Operations Policy (Version 1.6a)
- Virtual Organisation Registration Security Policy (Version 2.6a)
- Virtual Organisation Membership Management Policy (Version 3.7a)
- VO Portal Policy (Version 3.2a)

Other policies for all Grid participants:

- Traceability and Logging Policy (Version 2.0)
- Security Incident Response Policy (Version 3.2a)
- Approval of Certificate Authorities (Version 3.0)
- Policy on Grid Pilot Jobs (Version 1.0)
- Grid Policy on the Handling of User-Level Job Accounting Data (Version 1.0)

Glossary of terms used in JSPG policy documents:

- Security Policy Glossary of Terms (Version 2.3)