



National Grid Service

core production computational and data grid

Grid Security Incident Handling and Response Guide

Issue	Date	Comment
0.1	07 March 05	Draft release
0.2	16 June 05	Comments from NGS board and input from Ian Neilson's LCG/EGE policy

1. Introduction

The UK National Grid Service (NGS) adopts the Grid Security Incident Handling and Response Guide developed by the Open Science Grid Consortium¹ (OSG). This document is included unaltered below. Whilst the document was developed by close collaboration between the security activities of the projects, the following paragraphs are aimed at clarifying issues which arise due to the differing operational environments of the NGS and OSG projects.

2. Intended Audience

This document is intended for Grid site security contacts and site administrators. It is expected that this policy document will be supplemented by additional information concerning Incident Response procedures published on project website. All registered NGS sites must follow these procedures.

3 Reporting and Communications

Security contact information for NGS is maintained in the security area of the NGS website (https://www.ngs.ac.uk/security_ops/). It is a requirement of the NGS Joining Procedure (<http://www.ngs.ac.uk/guide/index.html>) that security contact information is provided and maintained for each grid site.

3.1 Mailing Lists

The INCIDENT-REPORT-L@xxx.yyy and INCIDENT-DISCUSS-L@xxx.yyy in Section 5.1 of the OSG document are replaced respectively by the following email addresses:

- Incident reporting will be done through the list NGS-SECURITY@JISCMAIL.AC.UK
- Discussion will be done through the list NGS-OPERATIONS@JISCMAIL.AC.UK

Similarly abuse@xxx.yyy and security@xxx.yyy are replaced respectively by the following email addresses:

- Abuse: abuse@grid-support.ac.uk
- Security: security@grid-support.ac.uk

¹ Open Science Grid Consortium - <http://www.opensciencegrid.org/>

3.2 Information Exchange with peer projects

With reference to section 3.2 of the OSG document: Handling of Sensitive Data, security contacts are hereby notified that data posted to the incident reporting or discussion lists described in this document may be cross-posted to peer grid projects who operate under this policy and with reciprocal information exchange agreements. Similarly, any information received from peer projects must be handled appropriately.

3.3 Users outside of any VO

With reference to section 6.3.1 of the OSG document: for users who are not member of any VO, the NGS Technical board has to be contacted so they can perform correction actions before the user is re-enabled.