LHC OPN Security Policy Final

Robin Tasker (r.tasker@dl.ac.uk)
CCLRC, Daresbury Laboratory

4 April 2006

Status of OPN IS Policy

Published	1. *Hosted by the JSPG within the CERN EDMS at* *https://edms.cern.ch/file/708248/LAST_RELEASED* 2. *Link from the OPN twiki page at* *https://twiki.cern.ch/twiki/bin/view/LHCOPN/WebHome*
Engagement	1. *Liaison with, and agreement from, site IS Security officers.* 2. *Implementation…just do it!* 3. *Report compliance on the twiki*

Summary of Security Policy

Purpose Assumptions Intended Audience	*Setting the Scene*
Scope	*Setting the Context*
Roles and Responsibilities Legislation and Compliance	*Spelling out the Governance*
IP Routing IP Protocols Access Control	*The technical stuff of the policy* *See later slides…*
Incident Handling and Reporting	*Procedural matters*
Open Questions	*Still up for discussion!*

Key Components of Policy

Purpose	1. *The OPN is used to facilitate high performance transport of LHC data between Tier 0 and Tier 1 Centres.* 2. *This policy is concerned with the service of carrying LHC data between Tier 0 and Tier 1 sites.* 3. *The OPN IS Policy purpose is to mitigate those risks associated with delivering the service.*
Assumptions	1. *BCP is not included here.* 2. *Each site will decide what is and is not acceptable with respect to Information Security.* 3. *Existing LCG/EGEE Security Policy and procedures will be followed.* 4. *Site access to the OPN available only after agreement to follow this OPN IS Policy.* 5. *The OPN is provided for a specific purpose and not for generalised inter-connectivity*

Key Components of Policy

Intended Audience	1. *LHC Tier Centres and those who provide the service operating across the LHC OPN on their behalf*
Scope	1. *This Policy specifies the rules which determine whether or not a site is permitted to transmit data across the OPN.* 2. *This Policy mandates a site to police and enforce the rules on the reception.* 3. *Membership of the OPN is restricted to the Tier 0 and Tier 1 sites based on the information held at* http://www.ripe.net/perl/whois?&searchtext=rs-LHCOPN 4. *CERN will maintain and publish this information in the RIPE database with a turn around of 3 working days* 5. *Any other use of the OPN is deprecated. Any traffic resulting from such use may be discarded without warning or notification.*

Key Components of Policy

Roles and Responsibilities	1. *IS Contact Management is maintained centrally for security contacts. It is a requirement that all sites must be registered in the Grid Operations Centre database held at* http://goc.grid-support.ac.uk/gridsite/gocdb/ 2. *The IS Officer at each OPN site will be satisfied with the mitigation of any IS risk associated with that site's connection to the OPN.* 3. *The OPN security contacts will be responsible for on-site liaisons with the local site to obtain a formal record of acceptance and implementation of this policy.*
Legislation and Compliance	1. *Each site will act in accordance with any national or international legislation applicable in that country to the operation of a data network.* 2. *The OPN security contacts will work with the local site IS Security officer to demonstrate compliance with this Policy.*

Key Components of Policy

IP Routing	1. *Specifies general BGP rules for the Tier sites* 2. *Specific Tier 0 BGP configuration rules* 3. *Specific Tier 1 BGP configuration rules* 4. *Rules for non-OPN traffic – no transit here!*
IP Protocols	1. *Protocols to support LHC data transfer and control and management are allowed* 2. *There is the expectation that applications will develop and as a consequence required protocols will also change. This is supported here.*
Access Control	1. *Requirement to use either an Access Control List (ACL) or similar technical process, e.g. a firewall, to deliver this Security Policy* 2. *Each site will deploy access control on received traffic based upon that site's IS Security policy.* 3. *Outbound traffic subject to access control* 4. *Inbound traffic policed to meet the site IS Policy*

Key Components of Policy

Incident Handling and Reporting	1. *For security incidents, LCG sites have an agreed policy and procedure.* 2. *It is assumed that [1] above is applicable to all OPN sites and will be applied* 3. *This Policy follows these procedures!*
Open Questions	1. *Currently no open questions*

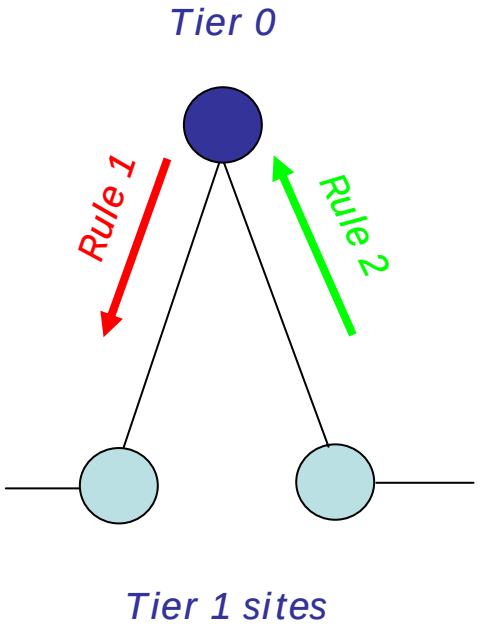
Access Control – Details #1

The Default Tier 0 Site Access Lists

1. The Tier 0 site will apply an *outbound* ACL that allows only traffic with *a source IP address in its own prefix* or *from any of the prefixes specified in Table 1* [to allow transit], and *with a destination IP address from any of the prefixes specified in Table 1.*

2. The Tier 0 site will apply an *inbound* ACL to every interface facing the Tier 1 sites. At its simplest the Tier 0 will accept traffic where the source IP address is from any of the prefixes specified in Table 1, and the destination IP address lies within the range of its own prefix or from any of the prefixes specified in Table 1 [to allow transit].

3. Where source/destination port numbers can be associated with data flows, then these should be used in addition to the IP address information specified above.



Access Control – Details #2

The Default Tier 1 Site Access Lists

1. Each Tier 1 site will have a specific outbound ACL that allows only traffic with *a source IP address in its own prefix* or the *prefix of another Tier 1 site* where transit has been specifically agreed, and *with a destination IP address from any of the prefixes specified in Table 1* [i.e. access to the Tier 0 and transit via the Tier 0 to other Tier 1 sites].
2. Each Tier 1 site will accept only traffic with a *source IP address from any of the prefixes specified in Table 1*, and *the destination IP address lies in its own prefix*, or another *prefix specified in Table 1* where transit has been specifically agreed.
3. Where source/destination port numbers can be associated with data flows, then these should be used in addition to the IP address information specified above.