LHC Optical Private Network Security Policy
Draft 4

LHC OPN Security Group
3 November 2005

1. ASSUMPTIONS

1. It is clearly understood each site that connects to the OPN will take its own view on what is and is not acceptable with respect to Information Security (IS).

2. It is noted that all LCG sites agree to abide by the LCG/EGEE Security Policy and procedures as specified at
   http://proj-lcg-security.web.cern.ch/proj-lcg-security
   http://proj-lcg-security.web.cern.ch/proj-lcg-security/documents.html

3. This OPN IS Policy does not supersede or invalidate any local IS polices at any local site. Should this policy conflict with any local site policies, the local site policy will take precedence for that site.

4. Each site will assess suitability of access to the OPN based upon the specification and implementation of its own local IS policy.

5. Sites will only be allowed access to the OPN once they have agreed to follow this OPN IS Policy.

6. The OPN is provided to support the LCH project and not as a replacement or alternative connection to other OPN sites, the Internet or other TCP/IP based networks.

2. INTENDED AUDIENCE

To be supplied – any suggested text most welcome.

3. SCOPE

1. The security policy specified here specifies the set of rules which govern whether or not a site is permitted to *transmit* data across the OPN. This is achieved by specifying the precise nature of the data transmitted. The better the specification of the data flows across the OPN, the more precise can be the specification of the rules, for example, IP source/destination addresses; source/destination port numbers used by the experiments to transfer their data. This approach leads to a generalised policy and rule set for access to the OPN to transmit data.

2. With the transmission rules specified, this policy mandates the OPN sites to police and enforce the rules on the *receive side*. Access Control Lists (ACLs) or similar techniques may be used.

3. Each site is responsible for ensuring that traffic transmitted on to the OPN is in accordance with this security policy.

4. Membership of the OPN is restricted to the Tier 0 and Tier 1 sites as defined in

   Table 1 – [https://uimon.cern.ch/twiki/bin/view/LHCOPN/LHCopnTables]

   This table also specifies the CIDR address ranges to be used by the sites for this purpose. These ranges are strictly limited and are the only address ranges that are supported within the OPN.

   If an OPN site(s) does not agree to implement this OPN IS Policy, all other OPN sites that have agreed to the policy may reject all transmissions from the site(s) that has not agreed to implement this policy.

5. Any other use of the OPN is deprecated and any traffic resulting from such usage may be discarded by any member site of the OPN without warning or notification.

4. ROLES AND RESPONSIBILITIES

1. Each site will nominate a suitable person and deputy to represent the interests of their site with respect to the provision of security on the OPN. The names and contact details of these representatives will be maintained centrally and be available at

   Table 2 – [https://to be supplied]

2. It is expected that the Information Security Officer (or equivalent) at each OPN site will be satisfied with the mitigation of any information security risk associated with that site's connection to the OPN. This mitigation is achieved through the implementation of this OPN IS policy. The OPN representatives specified in Table 2 will be responsible for all necessary on-site liaisons with the local site to obtain a formal record of acceptance and implementation of this policy.

3. Changes to this security policy will be discussed and agreed by the representatives specified in Table 2. Any resulting operational changes will take place only at specified advertised times once agreement has been reached.

4. The representatives in Table 2 will be responsible for notifying their colleagues should any of the contact details or names alter.

5. 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. The Security representative will ensure that the OPN sites are aware of any matter that bears upon the operation of the OPN.

2. The representatives specified in Table 2 will ensure that the OPN sites are aware of any such matter that bears upon the operation of the OPN.

3. The representatives specified in Table 2 will work with the local site IS Security officer to demonstrate compliance with this Policy. The output from this review will be shared with the LHC Security representatives.

6. IP ROUTING

1. The Tier 0 and Tier 1 OPN sites will only exchange IP routing information via the Border Gateway Routing (BGP) version 4 protocols.

2. The Tier 0 BGP speakers will accept only the announcements of those prefixes that each Tier 1 has specified in Table 1

3. The Tier 0 BGP speakers will announce the Tier 0 LHC prefixes and re-announce the LHC prefixes received from the Tier 1 sites.

4. The Tier 0 routers will not have a default route pointing to the OPN network.

5. A Tier 1 BGP speaker will announce only the Tier 1 LHC prefix specified in Table 1 for that site.

6. The Tier 1 routers will not have a default route pointing to the OPN network.

7. The announcement of prefixes associated with Tier 2 sites is deprecated and any site has the right ignore such announcements.

8. The OPN does not support announcements of alternate routes.

9. The OPN does not support transit for non-OPN traffic.

7. IP PROTOCOLS

1. In addition to the protocols necessary to support the LHC traffic between the Tier 0 and Tier 1 sites, the following protocols are supported within the OPN,

   ICMP
   SNMP
   PMTUD traffic

8. ACCESS-LISTS

1. Each OPN site is required to use an Access Control List (ACL) or similar technical process to restrict data flows on the OPN as defined within this documents. Reliance on routing and BGP filters to "ring fence" OPN traffic is in itself insufficient.

2. Each site will deploy access control to *received* traffic based upon that site's IS Security policy.

The Default Tier 0 Site Access Lists

1. The Tier 0 site will have 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 border routers will apply an *inbound* ACL to every interface facing the Tier1 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.

The Default Tier 1 Site Access Lists

1. Each Tier1 site will have a specific *outbound* ACL that allows only traffic with a source IP address in that Tier1 prefix and with a destination IP address from any of the prefixes specified in Table 1 [to allow access to the Tier 0 and to make use of the transit provided by the Tier 0].

2. Each Tier 1 site is expected to police the *inbound* traffic to meet its particular IS Security policy. At its simplest each Tier 1 will accept only 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.

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.

9. INCIDENT HANDLING AND REPORTING

1. For security incident response LCG sites have an agreed policy and procedure, http://proj-lcg-security.web.cern.ch/proj-lcg-security/documents.html

   It is assumed that this policy is applicable to all OPN sites and will be followed.

2. It is noted that a new draft document on incident response handling is currently being processed through the LCG and EGEE approval mechanisms, https://edms.cern.ch/file/428035/3/Incident_Response_Guide.doc

   It is assumed that this policy is applicable to all OPN sites and will be followed.

10. OPEN QUESTIONS

1. Input from the Operations Group is needed on the use of, for example, SNMP?

2. This document needs to be reviewed by the Operations group.

3. Who will co-ordinate and maintain the list of IS contact names?

4. Who updated the CIDR address lists and when?

5. **Domain Name Services**
   The following DNS issues **raised by BNL** need to be discussed and direction agreed.

   "Although not specifically mentioned in any of the LHC OPN preliminary design documents, Domain Name System (DNS) requirements should be discussed in support of the LHC. One of the options available is to create a unique instance of DNS within the confines of the LHC OPN network. As a discussion point, a unique domain name can be registered with the Internet authorities for use by the LHC facilities. A simple example that comes to mind is LHCOPN.ORG or LHCOPN.NET but can be anything the user community deems appropriate. Each site could provision two slave DNS servers for use by hosts attached to their specific segments of the LHC OPN network. If acceptable to BNL management, the DNS manager application, which was developed at BNL, could be deployed within the LHC facilities to allow timely DNS updates. Since this web-based application does support username and password authentication, multiple users at the different sites of the LHC OPN network would be able to maintain their own DNS information. Since the DNS manager application was developed at BNL, the DNS primary master DNS server for the LHC OPN should be housed on the BNL site to take advantage of the in–house support for both the application and the backend database server. The DNS requirements for the LHC OPN networks need to be discussed by all the members of this community to achieve a consensus on this suggestion."

   A response has been received from **Edoardo Martelli, CERN** expressing,

   "In my opinion a domain name for the LHCOPN is not necessary, because there won't be any layer3 device that will exclusively belong to the OPN. Every Tier centre can use its domain name and its naming convention for the IP addresses assigned to its routers. This is valid also for the /30 assigned to the T0-T1 light paths.

   Also, the end systems connected to the OPN should rely on the DNS servers provided locally by their infrastructure, there shouldn't be any need for a common DNS server."

6. **Business Continuity**

   The following has been received from **Dave Kelsey representing the JSPG** and needs to be discussed and direction agreed.

   "The JSPG have recently started work on disaster/emergency planning for LCG/EGEE. There are many possible reasons for downtime, but the most likely distributed "disaster" is a security incident. The main aim is to ensure that communication channels are properly defined (alternate e-mail addresses, phone numbers, IM names etc) and that we have properly agreed decision making processes. But we have also realised that we should investigate the feasibility of LHC data taking continuing and the OPN remaining up for Tier0 to Tier1 data transfer during a wide-spread security problem (which may not be Grid related of course). If the Tier 0 can be isolated from the CERN site network and each

of the Tier 1's be isolated from their respective general networks, it may be possible to keep the OPN up and running even when all else around is in complete chaos. Is this technically possible?"