LHC Optical Private Network Information Security Policy
Draft 8

LHC OPN Security Group
27 January 2006

1. PURPOSE

1. The LHC OPN will be used to facilitate the high performance transfer of LHC data between the LHC Tier 0 and Tier 1 Centres. The correct operation of this provision is therefore central to the scientific exploitation of the LHC. In this sense the LHC OPN carries a significant service.

2. Whilst the LHC OPN is in essence no more than a high speed inter-connect between LHC sites, the service it carries is fundamental to the HEP community's ability "to do" science. This service necessarily reaches into research institutes located around the world and in many respects short-circuits their conventional Internet connectivity.

3. The purpose of this LHC OPN Information Security (IS) Policy is to mitigate those risks associated with the delivery of the service across the LHC OPN.

4. In essence the risks are no different from any other production network. There are however two significant exceptions to this conventional perspective.

    1. The exceptional data rates expected over this network means that conventional security access devices may not provide sufficient or adequate protection.

    2. The LHC OPN is designed to closely couple administratively distinct institutes to deliver the service that it carries.

2. IS SECURITY POLICY ASSUMPTIONS

1. Consideration of Business Continuity is outside the scope of this document. Business Continuity of the LHC OPN is addressed at [*reference to be supplied*].

2. It is clearly understood that 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).

3. 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

4. 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.

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

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

7. 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.

3. INTENDED AUDIENCE

1. The LHC Tier Centre communities and those who provide the LHC OPN on their behalf.

4. SCOPE

1. The security policy specified here lays out 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 are sufficient whilst source/destination port numbers used by the experiments to transfer their data would provide greater protection.] 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. A list of these sites together with their associated CIDR address ranges which are to be used by the sites for the purpose of the OPN can be found in

   Table 1: [http://www.ripe.net/perl/whois?&searchtext=rs-LHCOPN]

   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. CERN will update the CIDR address list and publish it in the RIPE database, i.e. Table 1. Requests for changes must be sent to <extip@cern.ch> and will be published within three CERN working days

6. 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.

5. ROLES AND RESPONSIBILITIES

1. Currently IS Contact Management is maintained centrally for security contacts at grid sites with the requirement that all the sites must be registered in the Grid Operations Centre database. Shortly it is expected that sites will be allowed to manage the security contact data themselves using an interface with appropriate certificate-based authorization. This information is stored at,

   Table 2 – [http://goc.grid-support.ac.uk/gridsite/gocdb/]

2. It is expected that the local Institute's 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 from the local Institute's Information Security Officer 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.

6. 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.

7. 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 OPN prefixes and re-announce the OPN 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 the Tier 1 OPN prefix for that site, and optionally by bilateral agreement any other Tier 1 OPN prefix as specified in Table 1.

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 transit for non-OPN traffic.

8. IP PROTOCOLS

1. A range of protocols are expected to be in use to support the LHC traffic between the Tier 0 and Tier 1 sites both for the data transfer itself and for the control and management of the network.

2. It is expected that LHC applications will develop and evolve through the lifetime of the LHC and as a consequence the network protocols used in their support are also expected to change. This Security policy is supportive of such developments.

9. 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 site 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 its own prefix or, where transit has been specifically agreed, another prefix specified in Table 1; 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 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, or within 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.

10. INCIDENT HANDLING AND REPORTING

1. Incident response handling is processed through an LCG and EGEE approved mechanisms,

   https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_Response_Guide.pdf

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

11. OPEN QUESTIONS

1. There are currently no open questions.