

# LHCONE AUP

Modifications / additional (text/ideas)

Bruno Hoefft / KIT

STEINBUCH CENTRE FOR COMPUTING - SCC



# LHCONE AUPs

- Current LHCONE AUP:

<https://twiki.cern.ch/twiki/bin/view/LHCONE/LhcOneAup>

- Proposed LHCONE AUP:

<https://twiki.cern.ch/twiki/bin/view/LHCONE/NewLhcOneAup>

Editors of „Proposed LHCONE AUP“

David Kelsy,

Romain Wartel,

Bruno Hoefft

## Preamble

The LHCONE is a dedicated network architecture inter-connecting participating HEP Sites and allowing those sites to pool their computing resources for a more efficient distribution, storage, processing and analysis of HEP data.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) .

# Participating Collaborations and related information

The following Collaborations are currently participating in using the LHCONE:

- **WLCG**
- **Belle II**
- **U.S. ATLAS**
- **U.S. CMS**
- **Pierre Auger Observatory**
- **NOvA**
- **XENON**

- The WLCG collaboration is documented on the web site <http://wlcg.web.cern.ch/>
- The WLCG collaboration is managed by the WLCG Management Board
- WLCG sites are listed [on this web page](#)
- WLCG Security Policies: [Grid Security Policies](#) ,  
[Security Incident Response Policy](#) , [Grid Site Operations Policy](#)
- Additional information can be asked to [wlcg.office@cernNOSPAMPLEASE.ch](mailto:wlcg.office@cern.ch)

# Security incident reporting

A security incident is the act of violating an explicit or implied security policy. In line with WLCG Security policies requirements, LHCONE Sites **MUST** report suspected security incident as described in the [WLCG Security Incident Response procedures](#) .

- removed

# Security incidents response and Non-compliance with the AUP

Policy violations and non-compliance issues **MUST** be reported to [lhcone-operations@cernNOSPAMPLEASE.ch](mailto:lhcone-operations@cern.ch). Violations impacting the operational security of LHCONE **MUST** be reported as described in the [WLCG Security Incident Response procedures](#) . Severe or repeated violations **MAY** be escalated to **the/one?**  
**TBC** LHCONE Management Board and the offending LHCONE Site **MAY** be disconnected from LHCONE.

In addition, when confronted to policy violations or suspected security incidents, a LHCONE Site is allowed to drop the prefixes announced by the offending LHCONE Site at any time, disconnect itself from the LHCONE, as long as the changes are announced to the mailing list [lhcone-operations@cernNOSPAMPLEASE.ch](mailto:lhcone-operations@cern.ch). The 65010:ASN [LHCONE BGP community](#) can be used to ensure symmetry.

- → replace by:
  - **Non-compliance with the AUP**
  - **Compromised Security**

# Non-compliance with the AUP

- If a LHCONE Site believes that another one is not complying with this AUP, it can report the fact to its Collaboration's Management Board. Thus, this procedure will be followed: Should the Management Board believe a report of non-compliance to be justified, it will ask the non-compliant site to take all necessary action in order to resume compliance;
- If no action is taken by the site within the next 2 months, the Management Board will ask the non-compliant site to disconnect itself from the LHCONE L3VPN;
- If it doesn't happen within another one month, the Management Board will ask the upstream LHCONE Provider to disconnect the non-compliant site;
- It is at a LHCONE Site's discretion to drop the prefixes announced by the non-compliant site at any time, regardless of the effect it may be caused by the asymmetry. The 65010:ASN LHCONE BGP community can be used to ensure symmetry.



# Compromised Security

- Like any WAN network, the LHCONE is not intrinsically secure. If a LHCONE Site receives malicious traffic via its LHCONE connection, it can disconnect itself from the LHCONE without any notice. If the threatened site knows which LHCONE Site is sending the malicious traffic, it can ask the LHCONE Provider of the compromised site to temporarily disconnect it from the LHCONE in the interest of all the connected sites.

## Roles and Responsibilities – Sites

- **LCG and LHCONE Sites:**

### **Original:**

- have to acknowledge this AUP;
- are responsible for forming their own security policy with regard to traffic arriving from the LHCONE;
- can decide independently if the LHCONE traffic can bypass their own perimeter firewall or not.

### **New:**

- **MUST** abide by this AUP and all others applicable **WLCG Security Policies**;
- **MAY** define their own local security requirements with regard to traffic arriving from the LHCONE;
- **MAY** decide independently if the LHCONE traffic can bypass their own perimeter firewall or not

## Original:

- **LHCONE Providers** LHCONE Providers:
  - must make sure that they connect to the LHCONE L3VPN only sites that are HEP Sites and which have acknowledged this AUP;
  - must announce to the [lhcone-operations@cern.ch](mailto:lhcone-operations@cern.ch) mailing list whenever a new site get connected to the LHCONE;
  - must acknowledge disconnection requests made by a LHCONE Management Board;
  - should disconnect a LHCONE Site from the LHCONE if told so by a LHCONE Management Board;
  - must implement BGP filtering based on LHCOPN BGP communities.

## New:

- **LHCONE Providers** LHCONE Providers:
  - MUST make sure that they connect to the LHCONE L3VPN only sites that are **approved** LHCONE Sites, **that have also agreed to comply this AUP**;
  - MUST announce to the [lhcone-operations@cern.ch](mailto:lhcone-operations@cern.ch) mailing list whenever a new site get connected to the LHCONE;
  - MUST implement disconnection requests made by the **the/one? TBC LHCONE Management Board**;
  - MUST implement BGP filtering based on LHCOPN BGP communities.

## Original:

- **LHCONE Management Boards**
  - Any LHCONE Management Board can ask a LHCONE Provider to disconnect a not compliant LHCONE Site from the LHCONE.

## New:

- **the/one? TBC LHCONE Management Board the/one? TBC LHCONE Management Board:**
  - *This needs to be defined. Consensus among the different LHCONE Management Boards? Is each LHCONE Management Board going to decide whom to block or not? Should another board be defined to allow urgent decisions to be taken? Should an operational team be appointed for this purpose?*

## Coments / Questions

- Is there any procedure : „how to update the AUP“
- Does all sites to sign the updated AUP
  
- ...?