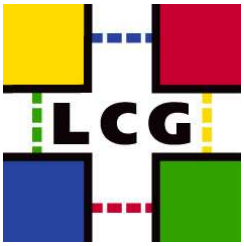

LCG Security Group

Security and Availability Policy for LCG

Date:	**30 September 2003**
Version:	**4b**
Status:	**Draft**
Author:	**Trevor Daniels**

Document Log			
Issue	**Date**	**Author**	**Comment**
1.0	19 Aug 2003	Trevor Daniels	Draft for meeting of LCG Security Group on 28 Aug 2003
2.0	1 Sep 2003	Trevor Daniels	Incorporates comments from meeting above; targeted for the GDB on 8 Sep 2003
3.0	3 Sep 2003	Trevor Daniels	Incorporates more comments from LCG Security Group mailing list. Sent to the GDB for Sept meeting.
4.0	30 Sep 2003	Trevor Daniels	Incorporates comments from the GDB, and from further consideration by the LCG Security Group. Sent to the GDB for Oct meeting.

1 Introduction

The LHC Computing Grid (LCG) project was formed to build the computing environment to support the scientific exploitation of the Large Hadron Collider (LHC) at CERN. From 2003 to 2005 it proposes to build a series of prototypes based on grid technology, gradually evolving in scale and complexity, to validate the computing model and to drive the design of the full system which will be built from 2006.

This document sets out the Policy regulating the activities of Grid participants which relate to the security and availability of Grid facilities and resources.

1.1 Objectives of Policy

This Policy

- presents an agreed set of statements which define the ***attitude*** adopted by the LCG Project towards LCG security and availability
- gives ***authority*** for certain defined actions which may be carried out by individuals and bodies such as the Grid Operations Centre (GOC), Virtual Organisations (VOs) and local administrators
- places ***responsibilities*** on individuals and bodies participating in LCG.

The overriding objective of this Policy is to promote the LHC science mission by setting out the approach to controlling LCG resources and protecting them from abuse in such a way that the science is not unduly compromised by overly strict security while the protection is sufficient to prevent undue disruption to that science by security-related incidents. The Policy aims to minimise the aggregated disruption to scientific activities caused by security restrictions and security incidents taken together.

The Policy also recognises LCG's obligation to minimise the effect of its activities on other users of both the Internet generally and the internal networks of participating institutes, and its obligation to adopt policies and practices which are directed to that end.

1.2 Scope of Policy

Parts of this Policy apply to LCG ***Resources***, to ***Users*** of those Resources, to ***Administrators*** of those Resources (including systems and networking personnel) at participating sites, to the ***Developers*** of systems supporting those Resources, to the ***Virtual Organizations*** (VOs) supporting the LHC experiments and to developers of ***Applications*** running on those Resources.

Security means more than merely preventing unauthorised access: it should be pro-actively concerned with maximising the availability and integrity of all the services and data which might be required by authorised users. This Policy accordingly addresses the protection, confidentiality, integrity and availability of LCG Resources and the Services running on them.

Every site participating in LCG will autonomously own and follow their own local Security Policies with respect to the system administration and networking of all the resources they own, including resources which are part of LCG. This LCG Policy should not be regarded as replacing or over-riding these local Policies; it acts as a supplement to them by setting out additional LCG-specific requirements and the minimum standards for sites participating in LCG.

The Policy itself does not set out Procedures, Rules, User Guides or other detailed technical requirements itself, but it does require such documents to exist separately to ensure the Policy is properly implemented and followed. These documents are referenced in Section 9 and carry the same force as if they were part of this Policy.

1.3 Ownership, Maintenance and Review of Policy

This Policy is prepared and maintained by the LCG Security Group and GOC, approved by the Grid Deployment Board (GDB) and formally owned and adopted as Policy by the LCG Software and Computing Committee (SC2) on behalf of the LCG Project. This version was formally adopted by the SC2 on <*date*>.

This Policy will be reviewed at intervals not exceeding 2 years by the LCG Security Group and resubmitted to the SC2 via the GDB for formal ratification whenever significant changes are needed.

The various Procedures, Rules, User Guides and other detailed technical documents which are required to implement this Policy are owned by the LCG Security Group or GOC, as appropriate, who regularly review them jointly. Initial versions of these documents and significant revisions of them will be presented to the GDB for approval.

2 LCG Services and Resources

The LCG ***Resources*** are defined as the ***equipment*** and ***software*** required to run currently available instances of production LCG services, and the ***data*** held on those services.
Included in the definition of ***equipment*** are processors and associated disks, tapes and other peripherals, storage systems and storage media, and networking components and interconnecting media.

Included in the definition of ***software*** are operating systems, supporting utilities, compilers and other general purpose applications, any software required to operate any equipment defined as an LCG Resource, software and middleware released and distributed by the LCG deployment team and any further software required to support any scientific application associated with LHC.

Included in the definition of ***data*** are data required to operate any equipment defined as an LCG Resource, data required to operate any LCG service, data intended to be processed or produced by any software defined as an LCG Resource, and any application data associated with LHC.

The production LCG services running at any time will be defined on the GOC website. These services may include but will not be limited to the following:

- Computing Elements (CE)
- Information Services (IS)
- Job Submission Services (JSS)
- Logging and Book-keeping (LB)
- Resource Brokers (RB)
- Replica Catalogues (RC)
- Security Infrastructure (SI)
- Storage Elements (SE)

3 Roles and Responsibilities

3.1 LCG Organisation

The various committees and other bodies defined as part of the LCG organisation are responsible for the ***Management*** of the LCG project.

They provide, through the adoption of this Policy and through the representations on the various approving bodies of the LCG organisation, the overall ***Authority*** for the position and actions defined herein.

3.2 Virtual Organisations

The Virtual Organisations (VOs), acting together with the LCG Organisation, Sites, and home institutes of the Users, provide the formal structure to support the several geographically dispersed associations of users and of service administrators. Their responsibilities include

3.2.1 User Registration

VOs are required to set up and operate a set of ***Registration Authorities*** and associated procedures for approving requests for joining the VO in accordance with the directions laid down by the LCG Security Group [1)] Approval must be restricted to individuals who are recognised as having legitimate rights to membership. VOs are subsequently required to maintain the accuracy of the information held and published about their members, and to promptly remove membership from individuals who lose their right to membership.

3.2.2 Controlling Access to Resources

Some LCG resources will be restricted to all members of certain VOs or to certain individuals within VOs. VOs will provide access to information about their members as necessary to enable such controls to be implemented and maintained accurately.

3.2.3 Applying Sanctions to Users

VOs are responsible for investigating reports of users failing to comply with the provisions of this Policy, and for taking appropriate action to ensure compliance in the future. This action may include the notification and involvement of the User's home institute. The ultimate sanction to be exercised at the discretion of the VO is the removal of membership, and hence the withdrawal of rights of access to LCG resources.

3.3 Sites

3.3.1 Quality of Services

Sites hosting LCG Resources recognise the trust the Users place in them in choosing to use their Resources, and they accept the responsibility for delivering reliable and well managed services to those Users.

3.3.2 Consequent Risks

Sites acknowledge that participating in LCG increases the risk of host compromise, to both LCG and non-LCG hosts on each site. Sites are responsible for minimising this risk.

3.3.3 Cooperation

Sites accept the duty to cooperate with the GOC and other participating sites in investigating and resolving security incidents, and to take responsible action as necessary to safeguard LCG resources during an incident in accordance with the Agreement on Incident Response [8)].

3.4 Resource Administrators

3.4.1 Site Policy

Resource Administrators must ensure their implementations of LCG services comply with both their site policies and this Policy.

3.4.2 Notifying Site Personnel

Resource Administrators are responsible for ensuring that all appropriate personnel concerned with security or system management on their site are notified of and accept the requirements of this Policy before implementing any LCG services.

3.4.3 Resource Administration

The Resource Administrators are responsible for the installation and maintenance of Resources assigned to them, and subsequently for the quality of the operational service provided by those Resources. This quality will be defined by the Service Level Agreement (SLA) for each Resource as published by the Administrator of that Resource.

3.4.4 Service Level Agreement

The Administrator of each Service instance must maintain an assessment of the risks inherent in their particular Service design or resulting from local services or operational practice which might affect that Service's Availability, Reliability or Performance, and publish the expected values of these service parameters in accordance with the GOC Procedures for Resource Administrators [3]. The publication of this information, together with other details described in the LCG Service Level Agreement Guide [7], constitutes the SLA with the user community for that service.

3.5 Users

All authorised Users of LCG Resources will be registered members of one of the LHC Experiment VOs or other approved VOs and are able to obtain suitable authentication credentials containing their identity which have been signed, directly or indirectly, by one of the Certification Authorities recognised [4] by LCG for that purpose.

The Users' Rules [2] sets out in detail the manner in which LCG resources may be used. They must be followed by Users at all times.

3.5.1 Safeguard Credentials and Private Keys

Users must ensure others cannot use their credentials to masquerade as them or usurp their access rights. The holder of a private key may be held responsible for ***all*** actions, whether carried out by the holder personally or not, carried out using credentials generated from that key. No intentional sharing of credentials for LCG purposes is permitted.

3.5.2 Observe Access Controls

Users must be aware that their jobs will often be running on equipment and using resources owned by others. They must observe any restrictions on access to resources that they encounter and must not attempt to circumvent such restrictions.

3.5.3 Observe Limitations on Use

LCG resources may be used only for legitimate professional purposes connected to the scientific exploitation of LHC. Personal use of any nature is expressly forbidden.

3.5.4 Applications

Applications software written or selected by Users for execution using LCG Resources must be directed exclusively to the legitimate purposes of LCG. Such software must respect the autonomy and privacy of the host sites on whose Resources it may run.

3.5.5 Respect for Others

Users must be aware that their work may be utilising shared resources and may seriously affect the work of others. They must show responsibility, consideration and respect towards other users in the demands they place on LCG.

3.6 Developers

The Developers are responsible for selecting or writing software to implement LCG Services, for preparing and releasing that software for installation by Resource Administrators and for subsequently maintaining that software. In selecting, writing, distributing or maintaining software, due attention will be paid to the following security-related areas as well as considering the general functionally, reliability and fitness for purpose of that software.

3.6.1 Facilitating Security Controls

The software should implement appropriate security techniques to control access to resources of all types.

3.6.2 Maintaining the Integrity of Services

Before distributing replacements, upgrades or patches to existing software, developers must ensure that adequate testing is carried out to ensure the functionality and reliability of existing Services will not be jeopardised. When carrying out tests, developers will follow current best practice. This requirement may be relaxed if it is imperative that a security-related patch be distributed urgently.

3.7 Grid Operations Centre

The Grid Operations Centre (GOC) is responsible for monitoring the overall operational quality of the LCG Services, and championing improvements. The responsibilities relating to security include

3.7.1 Contact details

The GOC is responsible for maintaining contact details of security personnel at each participating site and for facilitating LCG-related intercommunications between them.

3.7.2 Monitoring SLAs

The GOC is responsible for monitoring the operational performance of LCG Services and for publishing details of its findings for comparison with the published SLAs of those services.

3.7.3 Security Expertise

The GOC together with the LCG Security Group is responsible for establishing and maintaining expertise in LCG-related aspects of security in order to provide detailed advice and guidance to the community on avoiding and responding to internet security incidents.

4 PHYSICAL Security

All the requirements for the physical security of LCG Resources are expected to be adequately covered by each site's local security policies and practices. These should, as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards to levels consistent with those specified by the Resource Administrator in the associated SLA.

Stronger physical security is required for equipment used to provide certain critical LCG services such as recognised Certification Authority (CA) services. The technical details of the additional requirements are contained in the Procedures for operating and approving such services [4].

5 Network Security

All the requirements for the networking security of LCG Resources are expected to be adequately covered by each site's local security policies and practices. These should, as a minimum, reduce the risks from intruders and failures of hardware or software to levels consistent with those specified by the resource administrator in the appropriate SLA by implementing appropriate firewall protection, by the timely application of all critical security-related software patches and updates, and by maintaining and observing clearly defined incident response procedures.

It is LCG policy to minimise the security risk exposed by applications which need to communicate across the Internet; even so, the peripheral firewall on every participating site will be required to permit the transit of inbound and outbound packets to/from certain port numbers between a number of external and internal hosts in order to run or reach LCG services. These are defined in the LCG Guide for Network Administrators [5].

The LCG GOC, in collaboration with the LCG Security Group, will establish and maintain expertise in the security aspects peculiar to LCG networking. This expertise will be available on request to assist in improving the protection of a participating site and for investigating and resolving LCG-related security incidents.

6 Access Control

Access to all LCG resources is controlled by a common grid security infrastructure which includes both authentication and authorization components. The global components of this infrastructure must be deployed by all LCG sites and resources. The deployment of additional local security measures is permitted should the local security policies of the site or resource administration require this.

All LCG resource providers are required to comply with the LCG procedures, guidelines and rules [1] [2] [3] [4] [5]. LCG users are required to comply with the User Rules [2].

7 Compliance

7.1 Compliance with this Policy

Sites running externally accessible LCG services will be required to conduct a self-audit of their compliance with this Policy, following the Site self-audit Procedure [6] specified by the GOC, at intervals not exceeding 2 years. The GOC will in addition conduct or commission independent audits of compliance on sites failing to meet the requirement for self-audit, on sites appearing to be in breach of this Policy and occasionally on sites selected at random. Statements acknowledging the receipt and summaries (excluding security sensitive information) of both self and independent audits will be published on the GOC website. Such Audits of Compliance will be required for the continued recognition of the service being operated.

7.2 Compliance with Legislation

The areas of information systems security which are covered by legislation in many countries include encryption, interception of telecommunications and data protection. This legislation, where it exists, is not uniform or consistent across all the countries participating in LCG.

Wherever possible, LCG policies, practices and procedures will be designed so that they may be applied uniformly across all sites without violating the legislation in force in any participating country.

If this is not possible, country-specific exceptions or extensions will be made to this policy and its associated practices and procedures to ensure the legislation of all countries can observed. Such exceptions or extensions will be described explicitly in an Annex to the appropriate document and in the appropriate SLAs, with the reasons for the exception or extension clearly stated.

7.3 Exceptions to Compliance

In exceptional circumstances it may be necessary for LCG participants to take emergency action in response to some unforeseen situation which may violate some aspect of this Policy for the greater good of pursuing or preserving legitimate LCG objectives. If such a Policy violation is necessary, the exception should be minimised, documented, time-limited and authorised at the highest level commensurate with taking the emergency action promptly, and the details notified to the GOC at the earliest opportunity.

8 Sanctions

Participating Sites or Resource Administrators who fail to comply with this Policy, or its associated procedures and practices, in respect of a Service they are operating may lose the right to have that service instance recognised by LCG until compliance has been satisfactorily demonstrated again. The test of compliance will be an independent Audit.

Users, Administrators or Developers who fail to comply with this Policy, or its associated procedures and practices, may lose their right of access to and/or collaboration with LCG, and may have their activities reported to their home institute or, if those activities are thought to be illegal, to appropriate law enforcement agencies. The decision on what action should be taken will be made by an appropriate body, which may involve the User's home institute, set up by the VO.

VOs which fail to comply with this Policy, or its associated procedures and practices, together with all the Users whose rights with respect to LCG derives from that VO, may lose their right of access to and/or collaboration with LCG.

9 Associated Procedures, Rules and User Guides

The following referenced documents describe Procedures, Rules, User Guides and other more detailed documents which are required to implement this Policy. These explicitly referenced documents have the same force as the Policy itself.

1) LCG User Registration and VO Management
2) Rules for the Use of LCG-1 Computing Resources
3) LCG Procedures for Resource Administrators (to be written)
4) Approval of LCG-1 Certificate Authorities
5) LCG Guide for Network Administrators (to be written)
6) LCG Procedure for Site Self-Audit (to be written)
7) LCG Service Level Agreement Guide (to be written)
8) Agreement on Incident Response for LCG-1
9) Audit Requirements for LCG-1