LASER INTERFEROMETER GRAVITATIONAL WAVE OBSERVATORY

LIGO Laboratory / LIGO Scientific Collaboration

LIGO-M1000140-v7	LIGO	Thursday, February 10, 2011

LSC Computer Security Policy

Abe Singer
Warren Anderson
Thomas Nash

Distribution of this document:
LIGO Scientific Collaboration and others authorized to access LSC computing resources

California Institute of Technology
LIGO Project – MS 100-36
1200 E. California Blvd.
Pasadena, CA 91125
Phone (626) 395-2129
Fax (626) 304-9834
E-mail: info@ligo.caltech.edu

Massachusetts Institute of Technology
LIGO Project – NW22-295
185 Albany St
Cambridge, MA 02139
Phone (617) 253-4824
Fax (617) 253-7014
E-mail: info@ligo.mit.edu

LIGO Hanford Observatory
P.O. Box 159
Richland WA 99352
Phone 509-372-8106
Fax 509-372-8137

LIGO Livingston Observatory
P.O. Box 940
Livingston, LA 70754
Phone 225-686-3100
Fax 225-686-7189

http://www.ligo.caltech.edu/

1 Introduction

All members of the LIGO Scientific Collaboration (LSC), and others authorized to access LSC computing resources have a responsibility for the security of LSC computing and data, as does the Collaboration as a whole.

This policy establishes out the framework for coordinating security activities across the LSC, and defines the roles of the LSC Computer Security Officer, the LSC Operational Security Group and the LSC Incident Response Team. This policy also identifies the responsibility of LSC members to help in mitigating the risk created by insecure computer systems, and the responsibility of the LSC Operational Security Group to assist its members to that end.

Computing in the LSC involves systems at numerous institutions around the world. The responsibility for managing and securing these systems rests with the individual owners of the systems. However, participation in LSC computing activities creates trust relationships between systems at different institutions, resulting in a risk that a security compromise on one LSC member system can affect the security of other, possibly all, LSC member systems. Ultimately that risk creates a risk to science opportunities.

Security incidents can affect the ability of the LSC to do science. A compromise could lead to loss or corruption of science data and/or analysis results, and have an impact on availability of resources. An intrusion at the observatories could affect their ability to acquire and store interferometer data.

In addition, negative publicity resulting from security incidents, regardless of their severity, could result in onerous security requirements imposed on LSC computing resources and/or the LIGO Laboratory from government oversight agencies.

2 Scope

This policy applies to any LSC computing resource, managed, owned, or used by an LSC member, that has a trust relationship with other LSC members' resources, such that a compromise of the resource potentially has an impact on other parts or all of LSC computing infrastructure. This document refers to such resources as LSC Trusted Resources (LTRs). LIGO-M0900325, *LSC Policies and Procedures for LIGO Data Grid Tier N Centers,* defines these resources, specifically as the Tier 2 – 4 centers, and provides the requirement for those centers to acknowledge this policy and agree to comply with it. This policy also covers the data analysis systems at the LIGO Laboratory and other systems identified by the LSC Security Officer.

The LSC Security Committee will work with LSC members and groups to identify their resources covered by this policy, and maintain an active list of those resources for reference by LSC institution MOUs.

3 Philosophy

LIGO[1] takes the approach that security measures should support the scientific mission, not impede it. Ultimately, LSC members should consider computer security as something that enables them to work more effectively.

This policy adheres to the following principles in support of that goal.

3.1 Usability

Any security measures that involve user interaction should address usability; the measures must allow the user to understand the results of his/her decisions and actions. Security measures should work transparently to users wherever possible, and rely as little as possible on expected or proper user behavior.

3.2 Openness

Access controls should default to be as open as possible to LSC members. Restrictive access should only be applied when clearly necessary and justifiable. This will reduce negative impacts on productivity, and help users to understand that those access restrictions they may encounter have a compelling reason behind them.

3.3 Integrity and Availability

Security should enable science by assuring data integrity and system availability, by ensuring, to the greatest extent possible, that unauthorized behavior cannot corrupt data or disrupt system availability and utilization.

3.4 Support

LSC system administrators will carry a large part of the burden for maintaining security. LSC Security groups (defined below) should minimize the burden of security requirements on system administrators by providing tools, training, and resources.

3.5 Individuality

LSC members operate under varied sets of requirements, environments, and policies. LSC security implementations will respect individual member circumstances and constraints.

[1] "LIGO" refers to the LSC and the LIGO Laboratory. The "LIGO Directorate" consists of the LSC Spokesperson, the Director, and Deputy Director of the LIGO Laboratory.

4 Security Roles and Authorities

Coordination of security across the LSC requires particular roles tasked with the responsibility and authority to define and implement the requirements specified in this document. Section 12 (below) provides an organizational diagram.

4.1 LSC Security Officer

The LSC Security Officer, appointed by the LSC Spokesperson, has the overall responsibility for determining implementation of security policy, overseeing security auditing and monitoring, and leading incident response. The Security Officer has the authority to call on others to assist in responding to security incidents and to deputize others to take on the LSC Security Officer responsibilities when (s)he is unavailable.

The Security Officer will keep the LIGO Directorate and LTR PIs (or their designees) informed about the status of all security incidents.

The LSC Security Officer will work closely with the LIGO Laboratory Security Officer to ensure that LSC security efforts get coordinated with Laboratory security efforts.

4.2 LSC Operational Security Group

The LSC Security Officer appoints the members of the LSC Operational Security Group and the LSC Incident Response Team.

The LSC Operational Security Group has the responsibility for day to day monitoring of systems for signs of intrusion (intrusion detection), examination of systems for compliance with security requirements, and development of tools to support those activities.

4.3 LSC Incident Response Team

The LSC Incident Response team will manage responses to security incidents that potentially impact LSC data or LSC Trusted Resources, facilitate communications between LTR managers regarding LSC security incidents, and apprise LTR managers of LSC security incidents.

4.4 LSC Security Committee

The LSC Spokesperson appoints the LSC Security Committee, with input from the LSC Security Officer. The Committee will identify policy options and corresponding residual risks for the LIGO Directorate, and author LSC security policies, subject to approval by the LIGO Directorate. The committee will also work closely with the LSC Computing Committee to identify and evaluate security issues, keep the committee informed and solicit input on Security Committee activities. The Security Committee will also communicate with the LSC on relevant security issues and recommendations.

4.5 LIGO Directorate

The LIGO Directorate will approve security policies, accept associated residual risks and will approve all policy exceptions, with input from the Security Committee.

5 Responsibilities

In addition to the roles defined above, all LSC members and others authorized to access LSC resources carry some responsibility for security. The amount of responsibility varies with the role each member plays in the collaboration. This policy defines those responsibilities below, organized by role.

5.1 All Members and others authorized to access LSC resources

All LSC members and others authorized to access LSC resources, and any other persons managing LTRs, must maintain the security of their accounts and systems in a manner appropriate for the LSC, and must report security incidents involving LTRs (or with the potential to affect an LTR) to the LSC Incident Response Team (LIRT) as soon as they become aware of the problem. This notification will enable the LIRT to determine whether the incident has affected other LSC sites, notify those sites, and to take appropriate protective responses.

Users have a responsibility to manage their credentials properly –not to share them, not to expose them – and to take measures to prevent compromise of their laptop/home machines. Users have a responsibility to inform system managers when the user no longer requires access to systems so that their accounts can get closed in a timely manner.

5.2 System Administrators

Managers of LTRs have a responsibility to maintain the security of their systems in consultation with the LSC Operational Security Group. LTR managers also have a responsibility to manage user accounts so that account access gets terminated when a user leaves the organization or changes roles, and to notify the Operational Security Group of such changes to ensure closing other accounts of the person exiting.

During an incident response, persons with LTR system authority will carry out the actions requested by the LIRT, with priority for requests identified as urgent by the LIRT.

5.3 LSC Group Managers and PIs

Principal investigators and their designated managers have a responsibility to keep the rosters for their groups up-to-date and accurate. It is also the responsibility of PIs and group managers to ensure that the LSC Operational Security Group and the LSC Incident Response Team get the assistance they require from members of their LSC groups.

5.4 Center Managers

Any LSC member or institution with responsibility for a resource that hosts original science data has a responsibility to help preserve that data, and to hand over that data to LIGO when exiting the LSC or discontinuing support of the resource.

Center Managers should grant privileged access to their systems to the LSC Security Officer and appointed members of the Operational Security Group and Incident Response Team for the purposes of monitoring systems for intrusions and responding to incidents.

5.5 LSC Security Personnel

The LSC Security Officer and other LSC security personnel in turn have a responsibility to LSC members to assist members and LSC system managers in determining and applying security measures, monitoring for signs of intrusions, and responding to incidents.

6 Incident Response

All LSC members, others authorized to access LSC resources, and LSC sites have an obligation to immediately report security incidents to the LSC Incident Response Team (LIRT). The LIRT will in turn advise LSC sites of incidents within the LSC that could affect other LSC sites, work with managers of the affected systems to determine the nature and scope of the incident, and to determine effective response and recovery.

The LIRT will determine and document a procedure for incident notification.

Sites and members also have an obligation to work with the LIRT in responding to incidents, both those that originate at that site, and incidents at another site that may have an impact on their site.

7 Privacy

The LSC takes the privacy of its members seriously. LSC security monitoring and response activities will avoid unnecessary monitoring of user activities. As soon as it is possible without disrupting an investigation, the LSC Security Officer will notify PIs and individual owners of LTRs of any monitoring or incident response activity that may result in viewing of user data/activity.

8 Compliance with Institutional Policy

Whenever this policy conflicts with other LSC institutional computer security protocols and policies, those local institutional protocols and policies will take precedence over this policy.

The LSC Computer Security Officer will work with LTR institutions and the LIGO Directorate to make every effort to address compliance with local privacy, security, and incident response policies. To that end nondisclosure agreements will be established with LTR institutions when required.

9 Violations of this Policy

The LSC Security Officer will report serious violations of this policy to the LIGO Directorate. The Directorate will treat serious violations in the same manner as a serious violation of any other LSC policy or MOU.

10 Exceptions

All exceptions to this policy will require the approval of the LIGO Directorate and be documented in the participating institution's MOU.

11 Definitions

11.1 LSC Resource

A computer system, or particular software on a computer system, that provides data or services to LSC members. These resources will usually (but not always) be identified in the LSC member's MOU.

11.2 Trust relationship

A configuration between two systems whereby one system accepts assertions from the other system without verification. Another definition is where the configuration makes one system vulnerable to compromise from the other system.

11.3 LIGO Trusted Resource (LTR)

An LSC computing resource, managed, owned, or used by an LSC member, that has a trust relationship with other LSC members' resources, such that a compromise of the resource potentially has an impact on other parts or all of LSC computing

11.4 Incident

An event which gets investigated as a compromise, which may or may not actually be a compromise. The term "incident" covers the time from initial suspicion, through the determination of compromise, to cleanup.

11.5 Compromise

The state where an attacker has gained unauthorized access to a system.

11.6 Implementation

The application of policies to the configuration of systems.

11.7 LIGO

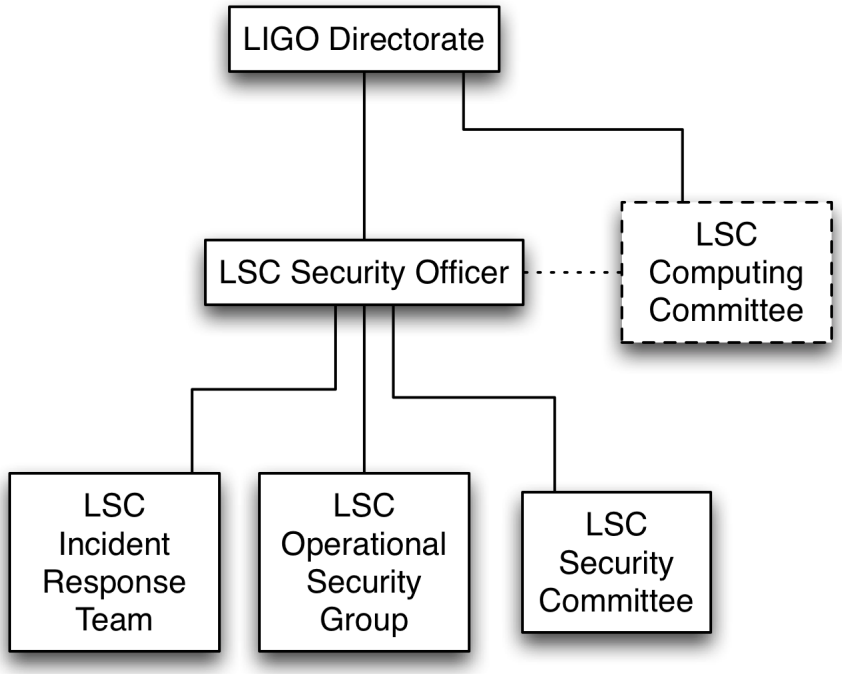
"LIGO" refers to the LSC and the LIGO Laboratory.

11.8 LIGO Directorate

The "LIGO Directorate" consists of the LSC Spokesperson, the Director, and Deputy Director of the LIGO Laboratory.

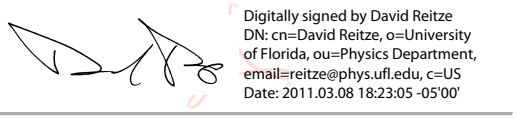
12 Organization of the security groups

The diagram below shows the organization of the security groups. While the Computing Committee is not a security group, it is included here to show it's relationship to the security groups.



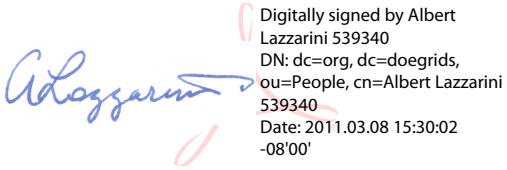
13 Approvals

Approval of this policy:



Signature *Date*

Dave Reitze
LSC Spokesperson



Signature *Date*

Albert Lazzarini

LIGO Directorate