LASER INTERFEROMETER GRAVITATIONAL WAVE OBSERVATORY

LIGO Laboratory / LIGO Scientific Collaboration

LIGO-M040352-v3 *LIGO* 2/3/2009

LIGO LABORATORY
COMPUTER SECURITY POLICY

LIGO Directorate

Distribution of this document:
LIGO Lab

This is an internal working note
of the LIGO Laboratory.

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 1970
Mail Stop S9-02
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/

Authorities

Submitted by:

Abe Singer
Digitally signed by Abe Singer
DN: cn=Abe Singer, o=LIGO Laboratory, ou, email=abe@ligo.caltech.edu, c=US
Date: 2012.05.21 18:26:21 -07'00'

____ Date____________________

Abe Singer, LIGO Laboratory Chief Security Officer

Acceptance and Approval by:

Digitally signed by David Reitze
DN: cn=David Reitze, o=California Institute of Technology, ou=LIGO Laboratory, email=reitze@ligo.caltech.edu, c=US
Date: 2012.05.09 08:55:59 -07'00'

____ Date____________________

David Reitze, Director, LIGO Laboratory

```
This document has been digitally signed, however the signature may
not be visible in all PDF viewers.  If you cannot see the signature,
please try viewing with Adobe Reader
```

1 Introduction

LIGO Laboratory has as its core mission fundamental scientific research in the field of observational gravitational waves, with the single overriding goal to maximize scientific output. This goal requires reliable operation of the interferometers, long-term integrity of the resulting data, and reliable access to the data.

The LIGO environment does not have strong secrecy requirements. LIGO publishes results openly to the scientific community, and does not handle any government classified or export controlled information. Nonetheless, during initial periods of data analysis, LIGO keeps the analysis and data from public view in order to avoid premature publication, potentially of not yet correct results. Thus LIGO requires minimal access controls for data, sufficient to restrict access until the LIGO Scientific Collaboration deems results to be publishable. Additionally, LIGO has institutional and legal requirements to preserve the confidentiality of certain personnel and student information.

Finally, LIGO has an interest in preventing the compromise of LIGO resources, or abuse of them for unauthorized or illegal activity, as that could disrupt the LIGO core mission with negative publicity and possible embarrassment to the government, or with outside networks blocking services to/from LIGO networks.

The essential mandate of this Computer Security Policy calls for the LIGO organization to identify risks that could interfere with meeting these goals and requirements, and to identify and implement strategies to mitigate the risks to a level acceptable to the LIGO management.

This policy addresses the management of LIGO networks and computers. Security implementations in many organizations often result in impediments to the organizational mission. In contrast, LIGO policy is to properly plan and implement security in a way that supports the scientific mission in a minimally intrusive manner that enables reliable access to data and use of LIGO resources at an acceptable level of risk.

1. Summary

This policy defines roles, responsibilities, and requirements for the management and implementation of computer security (“security”) at LIGO facilities. It addresses requirements for identifying risk, and implementing protection, monitoring, and incident response and reporting.

The LIGO Directorate signature above indicates agreement and acceptance of this policy.

A corresponding policy[1] addresses computer security for computing resources managed for the LIGO Scientific Collaboration, “LSC Trusted Resources” or LTRs. Principals at other institutions with responsibility for LTRs will indicate agreement with the LTR policy in their institution’s annual Memorandum of Understanding with the LIGO Laboratory.

2. Scope

This policy applies to the management of all LIGO Laboratory devices connected to a LIGO Lab network, and non-networked computers that control critical systems (defined below).

[1] LIGO-M040352-v3 –LIGO Laboratory Computer Security Policy

This policy also covers any device attached to a LIGO Laboratory network or system, whether owned by LIGO, an LSC institution, or an individual. Those systems may be subject to the requirements of security plans, and to security monitoring, scanning and other cyber security activities.

3. Goals

The LIGO Security program has the general goals of identifying risks to LIGO from unauthorized activity, developing strategies to reduce those risks, and providing the LIGO Directorate with a residual risk analysis for acceptance.

The LIGO risk analysis and security plan will address the following general categories of risks, ordered by importance:

- Disruption of operations, especially with regard to the generation and collection of scientific data.
- Corruption and loss of scientific data and research resulting from malicious activities.
- Malicious or unauthorized activity causing disruption of the LIGO Scientific Mission, resulting in negative publicity and possible embarrassment to the government.
- Exposure of data considered confidential by law, institutional policy, or LIGO research requirements.[2]

4. Requirements

Security measures resulting from this policy must meet the following requirements:

- Address usability of any security measures which involve user interaction; the measures must allow the user to understand the results of their decisions and actions. Congruent with this requirement, measures should work transparently to users wherever possible, and rely as little as possible on proper user behavior.
- Maintain uniformity as much as possible across all facilities in order to minimize effort and maximize comprehension.
- Take into consideration impediments to workflow to avoid unnecessary disruption of or impediment to the scientific mission.
- Enable science by assuring data integrity and system availability.
- Those implementing security must balance disruptions to science caused by intrusions with impediments to science caused by unnecessarily burdensome security measures.

[2] This confidentiality is not mission critical and so is a lower priority security goal that does not require exceptional access controls. Caltech provides support for LIGO's payroll, accounting, purchasing and other major business systems, covered by Caltech policies.

5. Roles, Responsibility and Authority

The responsibility for creating policy, analyzing and accepting risk, and compliance with policy and requirements rests with the following individuals.

1.1 The LIGO Lab Directorate

At the highest level, responsibility and authority for LIGO Lab security, including formal acceptance of risk, rests with the LIGO Laboratory Directors. The LIGO Laboratory Directors communicate issues of security to the National Science Foundation (NSF).

1.2 The Computer Security Officer

The LIGO Lab Directorate delegates day to day security oversight to a management level individual in the role of Computer Security Officer (CSO), who is appointed by the LIGO Directorate .

The CSO leads LIGO wide security oversight. In the name of the Directorate, and with their approval, the CSO establishes LIGO Laboratory wide security policies and has authority over the security of all LIGO Laboratory computing. This role parallels that of the Senior Safety Officer. The CSO will regularly maintain a LIGO wide security risk and vulnerability analysis, and from that analysis develop and maintain a security plan.

1.3 The Computer Security Coordinator

The Computer Security Coordinator (CSC) directly supports the CSO. The CSC coordinates implementation, advises and assists Laboratory staff on technical matters, and may initiate response to intrusions and other serious incidents under the leadership of the CSO.

1.4 System Administrators

The security of any system relies on maintaining the system consistent with the site security requirements. Thus, the responsibility for implementing and maintaining security on any given system rests with those who have the ability to make changes to that system. Therefore, while the CSO holds responsibility for leading the development of policy and requirements, the system administrators for each of these computing units hold ultimate responsibility for compliance with those policies.

1.5 General Users

An effective security plan should avoid relying on user compliance to maintain security as much as possible. However, security mechanisms which involve user interaction must necessarily depend on certain appropriate user behaviors, for example, keeping passwords secret.

Individuals and groups work in concert through the structure of the security organization to help assure the implementation of policies, risk management, reporting, communication and coordination necessary for security.

6. Computing Organizational Units

LIGO's computing falls under a diverse set of organizational units both within the LIGO Laboratory and at the external institutions that support the LIGO Scientific Collaboration. The support for computing within various computing environments such as general desktop computing, data acquisition, and different flavors of analysis computing crosses many of these organizational lines and may involve all or specific activities at one site or specific activities across a number of sites.

The CSO and CSC will work closely with the local system administrators and LIGO leadership to develop policy and requirements that fit the specific needs of each computing unit, in adherence with the principles listed above. This group will also identify the trust relationships between computing units in order to understand the impact of a security incident in one unit or one site may have on other units or sites.

1.6 Critical Systems

One class of computing must receive special attention: systems where an intrusion could cause an unrecoverable and significant loss of science opportunity through disruption or damage to equipment or irretrievable loss of data. The Director, Deputy Director, or Computer Security Officer (CSO) will designate specific systems Critical Systems and maintain a list of such in a separate document.

The Deputy Director or designee will appoint a person who will have responsibility for day to day oversight and management of the Critical System's security. This specifically includes the authority to stop operations or disconnect from the network if required because of a vulnerability, incident, or an urgent security need.

1.7 LSC Managed Resources

LIGO Lab manages certain designated LSC Trusted Resources primarily used for analysis of LSC data. As noted above, a separate document[3] covers computer security policy for LTRs . LIGO Lab will implement the practices and requirements indicated in the LMR policy document for resources managed by the LIGO Lab.

1.8 Non-critical Computing

Services used for day to day operations such as email, web servers, file servers, print servers, databases, etc. compose an important aspect of LIGO Laboratory's non critical computing infrastructure. Disruption of these services can cause damage both to productivity and reputation. These non-critical services should get reviewed on a regular basis for redundancy, versioning, patch level, vulnerabilities and prior incidents. Each new server established on a LIGO Laboratory network will be reviewed to assure that adequate security measures have been taken prior to the service going on-line.

[3] LIGO-M1000140 – LSC Computer Security Policy

1.9 Computers in Systems that Protect People Property, or the Environment

LIGO Lab as a matter of policy has always avoided relying on computers as an essential part of any system used to protect people from serious harm, to protect the environment from significant impact, or to protect property the loss of which would have a serious impact on the Lab's mission.

1.10 Personal Data

LIGO policy also forbids collection, distribution or storage of personal or sensitive data on LIGO computers. This includes social security numbers, credit cards, personal identity information, health or medical records. One exception has been made for activities necessary for personnel and payroll activities which may require handling of such information. In those cases the Lab relies as much as possible on institutional policy and services to minimize the use of that data on Lab systems.

1.11 User Managed Computers

Staff and visitors (users) will necessarily connect to the LIGO Lab networks computers owned and/or managed by the user. The CSO will identify services which rely on the security of the those systems and as necessary create policy for the management of those systems.

7. The Security Plan

The CSO will develop and maintain a Laboratory-wide security plan for approval by the Directorate. The plan will address the goals and adhere to the principles listed above. Additionally, all risk mitigation solutions must acknowledge their effectiveness in defending against that risk, to avoid implementation of unnecessarily wasteful or onerous measures.

The plan will naturally evolve over time as risks, technologies, and organizational priorities change. The plan will and address the people and processes required to maintain security in addition to the technology required.

The plan will address the following areas

1.12 Risk Assessment

Risk assessment will begin with identification of assets relevant to the risk assessment, including infrastructure architecture, systems and their division among organizational units, identification of critical systems, services provided, specific system and software configurations, and access controls.

The risk assessment will identify the trust relationships between assets, the threats to those assets, and the vulnerabilities found due to improper trust relationships and software flaws.

1.13 Protection (Mitigation)

The Protection section of the security plan will identify measures designed to mitigate the risks identified in the Risk Assessment. These measures may include requirements and processes for the installation, configuration and management of architectures, systems, networks,vand software.

The security plan will also lay out plans for review of software created or adopted for infrastructure use on Laboratory systems.

1.14 Residual Risk

Not all mitigation efforts will completely eliminate a given risk, or the truly effective mitigation will have an unacceptable impact on the LIGO scientific mission. And some risks have no mitigation available. The security plan will identify these residual risks for acceptance by the LIGO Directorate.

1.15 Policy

Some elements of the plan may require additional policies to support implementation, for example: authorization for network monitoring, acceptable use policy, etc. As necessary, the plan will identify policies required, and the CSO will develop those policies as separate documents.

1.16 Intelligence Gathering and Intrusion Detection

The security plan will identify technology and procedures for monitoring activity and collection data for the purposes of detecting intrusion and policy violations. The plan will also provide for routine collection of system and network data for support of incident response activities.

1.17 Incident Response

The security plan will provide requirements and procedures for responding to incidents. The plan will address determination of the nature of an incident, the means of intrusion, damages caused, and recovery methods. The plan will also address communication between responders and coordination of efforts.

1.18 Reporting, Communication, and Review

The security plan will establish the means for maintaining incident reports on all incidents identified as a successful intrusion and communicating those reports to the LIGO Directorate. The plan will also establish a means of reviewing incidents to provide feedback for improvement of the security plan.

1.19 Training

The security plan will identify requisite security training requirements for staff and users, and lay out outlines for training plans.

8. Reviews

Implementation of this policy will be based on a continuing risk and vulnerability assessment and evaluation of the balance between security measures and the need for openness for science and development.

The CSO will periodically assemble a Security Advisory board consisting of security experts, representatives of the Lab and the LSC. The board will review the LIGO security plan and policies and make recommendations to the CSO in a written report.

9. Incident Response

All persons covered by this policy must report security incidents (intrusions) immediately to the CSO, the CSC and the cognizant administrator of the affected system. The CSO shall in turn notify the LIGO Directorate and the Caltech or MIT security officer as required under institutional policy. In turn, the LIGO Directorate may need to report incidents to the National Science Foundation and the NSF Program Officer for LIGO Laboratory as specified in the LIGO Communications Plan[4].

The CSO will issue guidance from time to time on how to respond to an incident, and direct incident response.

The CSO will manage all LIGO Laboratory incidents (including any that involve a critical system or more than one computing unit) and will have full authority over all computers involved as well as authority to direct other individuals to assist when necessary and urgent.

The CSO will determine the severity of the incident and the appropriate level of response. If an incident is determined to be not serious by the CSO and CSC, the local unit will be advised to take appropriate remedial action on their own, with guidance from the CSO and CSC.

The CSC will lead investigations when the CSO cannot do so. The CSO may also delegate authority to lead incident response to other individuals in the even that neither the CSO nor the CSC can immediately respond. However, when a cognizant system administrator cannot reach an designated incident response leader, the individual may take appropriate action to mitigate damage to systems and interruption of services, until such time as the leader can respond. As soon as practical after exercising this authority, this person should inform the CSO and the Deputy Director of the circumstances.

Any Laboratory staff member or other person covered under this policy must assist the CSO in incident response as requested, and treat such response as their highest priority commitment, unless the Lab Directorate deems their diversion from regular duties will have a net negative impact on the LIGO Scientific Mission.

10. Exceptions from the Policy

Any variation from this policy on protection systems must have prior written approval of the LIGO Lab Director or Deputy Director. Any such approval will require a detailed risk analysis as specified in the LIGO Security Plan.

11. Enforcement

The LIGO Lab Directorate will treat violation of these rules in the same manner as similarly serious safety violations

[4] LIGO-M0900091 – *LIGO Communications Plan*