LASER INTERFEROMETER GRAVITATIONAL WAVE OBSERVATORY

LIGO Laboratory / LIGO Scientific Collaboration

LIGO-M020105-v6 *LIGO Laboratory* April 29, 2016

Computer Use Policy

Abe Singer

Distribution of this document:
LIGO Laboratory

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 159
Richland WA 99352-0159
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/

Signatures:

Electronic Signoff on this document can be found on the corresponding DCC entry
https://dcc.ligo.org/LIGO-M020105

- LIGO Laboratory Cybersecurity Officer
- LIGO Laboratory Directorate

1 Introduction

LIGO Laboratory (“LIGO Lab” or “The Lab”) 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; computer security addresses several facets of those requirements.

LIGO Laboratory strives to maintain as open an atmosphere of research as possible with regard to its computing infrastructure. The Lab tries to minimize restrictions that are deemed contrary to the established culture of open scientific research embedded in a university domain. In this vein, LIGO Lab tries to keep security measures transparent to the users (you). However, there are some security measures that the Lab cannot maintain without user cooperation.

2 Purpose

This policy identifies appropriate uses of LIGO Lab computing and network resources by faculty, staff, visitors and affiliates, and defines a small number of requirements that users must follow in order to help protect both themselves and LIGO.

However, this policy is not comprehensive. Caltech and M.I.T. also have policies that apply to computer use and computer based activities. Additionally, LIGO Lab has other policies about specific activities. You have the responsibility to be aware of your obligations under those policies in addition to this one.

3 Scope

3.1 What

The Lab computing infrastructure, including software, hardware, and networking, is purchased with U.S. Government funds. The various components and equipment are either the property of the U.S. Government, Caltech, or M.I.T.

This policy applies to activities conducted on any portion of that infrastructure. These systems are to be used for research and business in serving the interests of the Lab.

3.2 Whom

This policy applies to any person granted access to a Lab owned computer and/or network, at any LIGO Laboratory site. Additionally, this policy applies to the use of non-Lab computing resources by LIGO Lab employees and affiliates while conducting Lab business.

4 Authorization

LIGO Laboratory generally authorizes users to use Lab computing resources for any activity necessary and proper for the execution of their work with the Lab. LIGO Laboratory also permits personal, non-business use provided that it does not violate other provisions of this policy, is neither excessive nor interferes with Lab operations, and is consistent with Caltech and M.I.T. sanctioned policies.

5 Obligations

As stated above, LIGO Laboratory tries to minimize users' responsibility for maintaining the security of the LIGO Lab computing infrastructure. However, the Lab cannot enforce the few requirements below without the cooperation of its users.

5.1 Report security problems or suspicious activity immediately

The sooner we can respond to security incidents, the better the outcome; we can minimize the amount of damage, downtime, and spread of a compromise or infection.

The user is often the first, or only, person to observe suspicious activity on his or her computer. While LIGO Laboratory does some monitoring of the infrastructure for signs of security problems, we do not monitor all activity on all workstations and laptops.

Please report any suspicious activity or problems with your computer or account to your local system administrator, the security group (security@ligo.caltech.edu) and/or your supervisor as soon as possible.

5.2 Use a unique password for your LIGO Laboratory accounts

While it is convenient to have the same password everywhere, we require that you use a different password for your LIGO Laboratory accounts than you do for other accounts such as Gmail, etc. The people who compromise sites to steal passwords know that their victims often use the same password everywhere, and will try to use those stolen passwords at other sites to see what else they can get into.

This requirement is for your protection as much as for the Lab. Using the same password everywhere ris a very poor idea from the perspective of your personal information; it allows an information thief to quickly act as an impostor for a wide range of activities. If you use the same password at other sites, a compromise of your password at one of those sites could lead to a compromise of your LIGO Lab account. Conversely, a compromise if your LIGO account could lead to a compromise of your other accounts.

5.3 Protect your password and do not let others use your account.

LIGO Laboratory gives users accounts for their use, and their use only, with specific, limited exceptions. Do not give anyone else your password or otherwise let others use your account. If someone else has legitimate need to use Lab resources, we will give them their own account.

Do not write down your password where someone else can easily get access to it (but keeping written down in a relatively secure place such as a wallet or purse is acceptable). Do not store your password in unencrypted form on your computer.

5.4 Beware of Phishing, and other attempts to steal sensitive information or get you to install malware

Be cautious with email that asks you to send passwords or other private information, or directs you to a site that asks for the same.

Nobody should ever ask for your password in email, and passwords should never be sent over unencrypted email.

Likewise, be very careful about opening attachments that you receive in email, especially if you weren't expecting them.

5.5 Keep your systems up to date

Unpatched systems are the most common cause of compromises. LIGO Laboratory allows you to use your personally owned computers to connect to Lab resources for both your convenience and ours. A compromise of your computer can lead to theft of your password or otherwise be used to attack LIGO Lab computers. Keeping your system and anti-virus software up to date will greatly reduce the risk of security problems with your computer and reduce the threat to the Lab from the same.

5.6 Handle copyrighted and export-controlled information appropriately

Possession of copyright material or other intellectual property does not give one the right to distribute it. Unauthorized distribution of intellectual property may result in financial penalties to the user, and in some cases to the Lab.

Some technology used and/or developed by LIGO Laboratory is subject to export control laws. Additionally, export controls may apply to sharing information with foreign (non-U.S.) nationals visiting Lab sites. Before exporting any LIGO Lab technology or intellectual property outside of the United States, or sharing with visitors, consult with the Directorate on the appropriate means of doing so.

5.7 Backup data on a regular basis

Should your computer get compromised, we may require that it get erased and cleanly reinstalled. Computers and storage devices eventually fail, destroying stored data. And some times phishing and malware attacks use "ransomware," which encrypts your data and requires you to make a payment to unlock it (which sometimes works, and sometimes doesn't).

The lost work whether due to a malicious attack or simply a stolen or broken computer is very costly and can impact the work of others. We require that you backup your data either to LIGO Laboratory servers or to a backup hard drive on a regular, frequent basis.

5.8 Use appropriate remote access methods

Remote access to Lab systems is very useful when working away from the office. Enabling *insecure* means of remote access can easily allow outside attackers to compromise our systems. Use only Lab approved means of remote access.

5.9 Consult with local site system administrators

Consult with your site system administrators on how to comply with these requirements. In particular, you must coordinate with them:

- When installing new hardware
- Before connecting any device to the network
- On what software packages are approved and licensed for use in the Lab
- What software you're allowed to install on a personally owned computer
- On allowed remote access methods and software
- How to properly backup your system

6 Recommendations

In addition to the above requirements, LIGO Laboratory has some additional recommendations that will help both you and the Lab:

6.1 Keep personal email and files separate and private

LIGO Laboratory, Caltech, and M.I.T. respect the privacy of their users and of personal information that users might store on institute resources. We recommend that you keep your personal email and files separate from your work related documents, and make use of access controls to prevent other users from being able to read them.

When possible, we recommend that you use a separate email account for personal email.

Keeping your personal information separate and unreadable by others both helps protect your privacy, and make it easier for Lab staff to avoid seeing personal information in the event that we have to access your work related documents.

6.2 Encrypt sensitive data

To further protect sensitive information from unauthorized access, we recommend that you encrypt any data where exposure of that data could cause significant damage to yourself or the Lab.

We especially recommend not sending sensitive information over email, unless no other alternative is available. If you do have to use email for such information, encrypt the data when sending. Email by itself is not secure, it can be read by anyone who has access to the networks that the mail travels over, or to the servers on which the email transits or is stored.

7 Prohibitions

In complement to the to the requirements above, LIGO Laboratory expressly prohibits certain activities.

7.1 Bypassing access controls

LIGO Laboratory implements access controls as a means of restricting users' access to only those things the Lab has given them authorization to access. However, vulnerabilities or imperfections in the technology might allow users to bypass access controls. Having the capability to do such bypassing does not imply any authorization do to so, and any such activities will be considered unauthorized access.

7.2 Using another users' credentials

In support of the requirement above to not share passwords, should someone share his/her credentials with you in violation of this policy, you do not have authorization to use them.

7.3 Malicious and Negligent Activity

Activities that corrupt data, compromise systems, or interfere with operations (colloquially called "hacking"), either intentionally or negligently, are prohibited. Additionally, these activities may be considered violation of state and federal laws. Such activities include:

- Disrupting a network or system; conducting a denial-of-service attack on a system or user.
- Corrupting or deleting data without authorization
- Distributing copyrighted data without authorization
- Deliberately introducing malware
- Attempting to compromise a system or escalate privileges without authorization
- Scanning systems for vulnerabilities without authorization
- Interception of network communications without authorization
- Breaking the encryption of files or transmitted data

7.4 Unauthorized connection of devices to a Lab network

Connecting any networked device to the network imposes a security risk, and can disrupt the network if not properly configured. This not only applies to computers, but printers, instruments, switches, routers, wifi base stations, and anything else with networking capabilities. Additionally, it is important for the Lab IT and Security groups to be aware of what is on the Lab networks, and where. Do not purchase and install devices on Lab networks (including wireless networks) without first coordinating with your site system administrator.

7.5 Use of software without a license

Any software that you use for LIGO Laboratory business must have an appropriate license. The Lab prohibits use of "pirated" software or software otherwise obtained or used in violation of it's licenses. Such activities are also generally violations of the law as addressed in section 7.6 below.

7.6 Violation of law or Caltech/M.I.T. policy

This policy does not authorize any activities that are violations of applicable laws or institutional policies. LIGO Laboratory is governed by Caltech policies (for Caltech operated facilities) and M.I.T. policies (for M.I.T. facilities). Neither this policy nor any other Lab policy can supersede institutional policies.

7.7 Use of LIGO resources for another business or for-profit activity.

Institutional policies and LIGO Laboratory's federal funding requirements expressly prohibit the use of Lab resources for the operation of any private business or for-profit activity. The personal use allowed above in section 4 above is limited to truly personal use.

7.8 Sending of spam or other similar unsolicited email. Sending or forwarding chain letters, Ponzi schemes and similar.

Sending of unsolicited bulk email (colloquially called “spam”) can be a violation of federal law, some state laws, and institutional policy. Chain letters over email may be considered wire fraud and be a violation of federal law.

7.9 Forging email headers to impersonate another.

While email headers can be easily forged, we expect that mail from Lab servers that purports to come from a user actually comes from that user. LIGO Laboratory prohibits forging mail headers to impersonate another, or for any fraudulent or malicious purposes.

8 Expectation of Privacy

Caltech and M.I.T. reserve the right to access users electronic data and communications at any time, under appropriate circumstances. You should have no expectation of privacy with regard to Institution access to your electronic data and communications. However, Caltech, M.I.T., and LIGO Laboratory try to respect users’ privacy where possible, as dictated in the Caltech Computer Use Policy (http://hr.caltech.edu/policies/acceptable_use), the M.I.T. Policy on the Use of Information Technology Resources (http://web.mit.edu/policies/13/13.2.html) and the LIGO Laboratory Privacy Policy (https://dcc.ligo.org/public/0000/M080370/001/M080370-v1.pdf).

9 Enforcement

Violation of the terms of this policy can result in temporary or permanent suspension of your computer privileges.

Additionally, for visitors, violations may result in a suspension of your visiting privileges and be reported to your home institution/employer. For LIGO Laboratory employees and students, violations will be handled through the appropriate disciplinary procedures.

Violations of law may be reported to law enforcement for investigation and prosecution. For systems considered property of the U.S. Government, such violations may be subject to reporting to the F.B.I.

10 Related Policies

- LIGO Laboratory Computer Security Policy: https://dcc.ligo.org/public/0000/M040352/003/M040352-v3-LIGO-Lab-Computer-Security-Policy-signed.pdf
- LIGO Laboratory Privacy Policy:https://dcc.ligo.org/public/0000/M080370/001/M080370-v1.pdf
- LIGO Laboratory Authorization of Monitoring Activities by the Security Team: https://dcc.ligo.org/public/0000/M070072/001/M070072-v1.pdf
- LIGO Laboratory Copyright Policy: https://dcc.ligo.org/DocDB/0002/M090005/001/M090005-v1-CopyrightPolicy.pdf

11 Compliance with Institutional Policy

- Caltech Computer Use Policy: http://hr.caltech.edu/policies/acceptable_use
- M.I.T. Policy on the Use of Information Technology Resources: http://web.mit.edu/policies/13/13.2.html