LASER INTERFEROMETER GRAVITATIONAL WAVE OBSERVATORY

LIGO Laboratory / LIGO Scientific Collaboration

LIGO- M1700044-v3

LIGO Laboratory   June 28, 2018

LIGO.ORG Credential Acceptable Use Policy

Warren Anderson, Ryan Blair, Jonathan Hanks, Adam Slagell, Randy Trudeau

California Institute of Technology
LIGO Project – MS 100-6
1200 E. California Blvd.
Pasadena, CA 91125
Phone (626) 395-2129
Fax (626) 304-9834
E-mail: info@ligo.caltech.edu

LIGO Hanford Observatory
P.O. Box 1970
Mail Stop S9-02
Richland WA 99352
Phone 509-372-8106
Fax 509-372-8137

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

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

1. Overview

The purpose of this document is to protect the integrity and security of the computer resources of LIGO Laboratory (LIGO Lab), the LIGO Scientific Collaboration (LSC), and their collaborators. LIGO.ORG credentials are used to access systems and information which are vital to the mission of the LIGO Lab and the LSC (collectively, LIGO). It is the responsibility of every individual who has a LIGO.ORG credential (also known as an albert.einstein credential or account) to understand this policy and conduct their activities accordingly.

2. Scope

This policy applies to the possession and use of LIGO.ORG credentials by members of the LIGO Laboratory, the LIGO Scientific Collaboration, members of the VIRGO Collaboration, and all other persons who have a LIGO.ORG account. LIGO.ORG credentials include your albert.enstein@ligo.org username and password and all credentials derived from them, such as grid certificates, Kerberos keytabs, etc. They also include all special purpose credentials such as robot keytabs or certificates used to access LIGO Lab or LSC systems or information.

3. Use and Ownership

3.1 LIGO.ORG credentials are granted to individuals by LIGO (as defined in paragraph 1.1.1 of the LSC Bylaws). LIGO may suspend, limit or revoke the use of any LIGO.ORG credential at any time and for any reason it deems appropriate. LIGO may also grant authority to other individuals within LIGO to suspend or limit access for technical and/or security reasons.

3.2 LIGO.ORG credentials must be used in a manner that protects the security and integrity of the computer systems and information of LIGO Lab, the LSC and their collaborators. Measures to ensure this include (but are not limited to):
*   Using a unique password that is not used to access any other account or system.
*   Using a password that cannot be guessed (randomly generated passwords are preferred).
*   Only entering your password into websites or services that end in "ligo.org", "ligo.caltech.edu", "ligo-wa.caltech.edu" or "ligo-la.caltech.edu".
*   Never sharing your password with another individual, even if that individual is a LIGO Lab or LSC member.
*   Never writing your password to a file that is unencrypted on any system (eg, in a script or repository in an attempt to automate a process).
*   Never transmitting a password over an unencrypted network channel (eg, into a web page that does not have https at the beginning of its URL).
*   Reporting promptly to the LIGO Lab (security@ligo.caltech.edu) or LSC (lsc-seccom@ligo.org) security officers if you suspect theft, loss or unauthorized access of your LIGO.ORG password or any of the accounts that can be accessed with it.

3.3 Systems and information accessed with your LIGO.ORG credential must be used in a manner that protects their security and integrity. Measures to ensure this include (but are not limited to):

- Logging out of systems when you are done with them whenever possible (note that some web services do not permit logout, look for a logout button). This is especially important if you are using a computer that can be accessed by other individuals.
- Using a password protected screensaver that will autolock your session after a moderate period of inactivity (eg 10 minutes).
- Never allowing another person to access a system from your login session.
- Protecting private information by not copying it outside of protected areas, not sending it to open mailing lists, not putting it in public accessible repositories, and not accessing it in an environment where it can be seen by those not authorized to see it.

4. Unacceptable Use

LIGO.ORG credentials must never be used in any activity that violates the laws of any jurisdiction (nation, state, province, municipality, etc) in which they are used, nor may they be used in a manner or for activities that violate the policies of any university or research institution where they are used. LIGO.ORG credentials should not be used in a way that violates LIGO Laboratory or LSC policies for employment or membership. It is important to remember that inappropriate use of LIGO.ORG credentials can have negative impacts on the future of funding for LIGO Lab and/or LSC institutions.

5. Compliance

Compliance with this policy is mandatory for everyone who used a LIGO.ORG credential. If you feel that you cannot reasonably comply with this policy in the performance of your scientific or scholarly work, please contact the LIGO Lab and LSC directorate (ligo-directorate@LIGO.ORG). Exceptions may be granted in certain cases but must be explicitly made by the directorate. Failure to comply with this policy may result in the loss of LIGO.ORG credentials and may be grounds for further action on the part of LIGO Lab and/or the LSC.