LASER INTERFEROMETER GRAVITATIONAL WAVE OBSERVATORY
- LIGO –
CALIFORNIA INSTITUTE OF TECHNOLOGY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Document Type *Policy*	LIGO-M020105-04-E	09 April 2006
Computer Use Policy of the LIGO Laboratory		
LIGO Data and Computing Group		

California Institute of Technology
LIGO Laboratory - MS 18-34
Pasadena CA 91125
Phone (626) 395-212
Fax (626) 304-9834
E-mail: info@ligo.caltech.edu

Massachusetts Institute of Technology
LIGO Laboratory - MS NW17-161
Cambridge, MA 01239
Phone (617) 253-4824
Fax (617) 253-7014
E-mail: info@ligo.mit.edu

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

LIGO Computer Use Policy

TABLE OF CONTENTS

LIST OF TABLES

Table 1: Document revision history

Rev.	Date	Comments	Sign-off
M020105-00-E	17 October 2002	Initial Release	Initial release
M020105-04-E	09 April 2006	- various edits; - added guidance to LIGO visitors bringing their own equipment to Laboratory sites; - CDS and LDAS additions; - added guidance for systems administrators	 J. Marx  S. Whitcomb

1 INTRODUCTION

LIGO Laboratory constitutes a distributed organization of facilities and laboratories operated under a cooperative agreement between the California Institute of Technology (Caltech) and the National Science Foundation; Caltech shares with Massachusetts Institute of Technology (MIT) responsibility for oversight and implementation of the project. As such, the laboratory is bound by the policies and protocols imposed on enterprises operating on the respective university campuses. In addition, the LIGO observatory sites in Hanford, WA and Livingston, LA are considered Government facilities managed by Caltech.

LIGO Laboratory strives to maintain as open an atmosphere of research as possible with regard to its computing infrastructure. The intent is to minimize restrictions that are deemed contrary to the established culture of openness, trust and integrity. Nevertheless, LIGO must remain committed in working to protect its staff, collaborating researchers from the LIGO Scientific Collaboration (LSC), its own information management systems, and all other visitors to the Laboratory from illegal or damaging actions by individuals, either knowingly or unknowingly. For this reason, the Laboratory has established a LIGO Computer Use Policy. As part of the policy there should not be any expectation of privacy when using LIGO computing resources.

The LIGO Laboratory computing infrastructure, including but not limited to, computer equipment, networks, operating systems, storage media, user accounts, web servers, and application software, were all purchased using U.S. Government funds and are either the property of the U.S. Government, Caltech, or MIT. These systems are to be used for research and business in serving the interests of the Laboratory.

Security is a team effort involving the participation and support of every LIGO employee and associate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

All users are expected to be considerate of others and to be responsible in their use of LIGO equipment. Individuals are expected to follow the local acceptable use practices when dealing with LIGO resources.

If you have any questions concerning the policy fell free to contact anyone in the LIGO System Administration group.

2 PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment within LIGO Laboratory. These rules are in place to protect the employee, LIGO and its associates. Inappropriate use exposes LIGO to risks including virus attacks, compromise of network systems and services, and possible legal liabilities. It is the policy of LIGO to maintain access for the LIGO community to sources of LIGO information and to provide as well as to encourage open access to and the sharing of information.

The information resources must be used in accordance to with rules and regulations established by the LIGO management. This document contains a series of sections that address specific aspects of the overall policy:

- Acceptable use guidelines;
- Visitors use of LIGO IT resources;
- Use of wireless computer networking communications systems;
- Requirements for access by different groups of the LIGO Laboratory
- Remote access to LIGO Laboratory IT resources;
- System audits;
- Password usage;
- Use of anti-virus software.

3 SCOPE

This policy applies to all personnel either employed by the Laboratory or visiting LIGO Laboratory sites. The acceptable use policy (Section 6) applies to individuals at their respective LIGO Laboratory home sites. This policy also covers the use of any computing equipment that is not owned by LIGO but is used at any LIGO facility.

Three basic groups support the computing infrastructure of LIGO, General Computing (GC), Control and Data Systems (CDS) and the LIGO Data Analysis Systems group. Each of these groups are represented at each LIGO location. By default, this policy applies to all computing equipment operated by the groups. However, there are a number of specific systems operated by these groups that may fall outside the scope of this policy. Examples include, but are not limited to, the Observatory Security Critical Systems as defined in the LIGO Laboratory Cybersecurity Policy, M040352. Systems not covered by this policy will be considered on a case-by-case basis by the LIGO Laboratory Computer Security Officer and Computer Security Coordinator (refer to M040352).

All staff and visitors are required to read this document and then to sign a form acknowledging that they have read these materials and understand the policy as it applies to them

LSC meetings will be handled in the following manner. The web-based registration form will be modified to require MAC address registration and acknowledgement of the provisions of this Computer Use Policy as a necessary step in the registration process.

This version of the document supercedes previous versions. Other policies of the LIGO Laboratory Management may take precedence over this policy as noted.

4 EXECUITVE SUMMARY

A brief summary of “DOs and DON’Ts” is provided below. This does not substitute for a careful reading of this policy. Persons who agree to abide by the provisions of this policy are assumed to have read and understood it in its entirety.

- **Do** read and follow the LIGO Computer Use Policy
- **Do** become familiar with, and follow local computer use policies
- **Do** keep up to date on OS patches and virus protection software
- **Do** use only LIGO-approved equipment on the LIGO network
- **Do** use strong passwords and change them every 6 months
- **Do** contact the local system administrator for help with any questions or problems
- **Do** keep your computers and laptops in a secure location to prevent theft
- **Do** be courteous and use common sense when using LIGO resources.
- **Do** perform regular backups of LIGO data on your laptops.
- **Do not** use the same password for different accounts
- **Do not** share your password with others
- **Do not** install software or products not approved or licensed for use by LIGO, including personal software
- **Do not** engage in unauthorized use of other copyrighted materials (software, images, music)
- **Do not** use LIGO resources for non-LIGO activities
- **Do not** use mailing lists for personal agendas. Only LIGO business items should be posted to LIGO mailing lists.

5 DEFINITIONS

Application Administration Account
Any account that is for the administration of an application (e.g., IDEAS, Cadence…).

Cable Modem
Cable companies that provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet. Cable Modem service is currently available only in certain areas.

CDS

Control and Data Systems

Dial-in Modem
A peripheral device that connects computers to each other for sending communications via the telephone lines.

DSL
Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

EMI
Electromagnetic RF interference caused by transmitters that unintentionally interfere with other RF-sensitive devices.

LDAS

LIGO Data Analysis System

LIGO Directorate

For the purpose of this document, the LIGO Directorate is as the Director and Deputy Director of the LIGO project.

LIGO Management
For the purposes of this document, LIGO Laboratory Management will be considered to include the following: Directorship of LIGO Laboratory, managers and heads of observatories, and management of the several computing and IT groups within the Laboratory.

Remote Access
Any access to LIGO Laboratory networks through a non-LIGO controlled network, device, or medium.

Spam
Unauthorized and/or unsolicited electronic mass mailings.

Sponsors
A visitor's sponsor is the LIGO or associate employee who is responsible for the visitor or who is working or collaborating with the visitor.

User Authentication
A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

Visitors
There are three types of visitors covered by this policy:

A. LIGO Laboratory employees who are visiting Laboratory sites other than their home institutions;
B. Sponsored collaborators or invited collaborators who are members of the LIGO Scientific Collaboration (LSC);
C. Conference participants and other infrequent or one-time visitors who are staying a short period of time.

6 ACCEPTABLE USE POLICY FOR GENERAL COMPUTING RESOURCES AT ALL LIGO LABORATORY SITES

6.1 Summary of Acceptable use for General Computing

Use of LIGO equipment is restricted to official LIGO business. Personal use is allowed in accordance with Caltech and NSF guidelines for acceptable personal use.

Installing work related software on LIGO assigned computers is permitted.

Only authorized software is allowed to be installed on LIGO critical computers, this includes all CDS computers, all gateway machines, and all servers (refer to M040352),.

Only authorized software is to be installed onto CDS or LDAS computers (refer to M040352),

Approved software may be run on non-assigned general computing computers at Caltech and the Observatories with the following conditions:

- The normal user or administrator must be asked and give permission before installation.
- Any requests from the normal user/administrator not wanting it must be respected.

The person who installs the software must leave a message telling other potential users how to stop the program if there are problems.

6.2 Security and Proprietary Information

1. When appropriate, the user interface for information contained on Internet/Intranet/Extranet-related systems should be marked and protected as either proprietary and/or company confidential, as defined by LIGO management. Examples of LIGO confidential information include but are not limited to: LIGO financial information, employee human resources information, contracts in negotiation. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Passwords must be kept secure and should not be shared. Authorized users are responsible for the security of their passwords and accounts. System level passwords shall be changed on a regular basis with a few exceptions, user level passwords should be changed every six months. LIGO may decide to impose password aging in order to ensure this.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes or less, or by logging-off when the host will be unattended. It is preferred that the user log off the machine.
4. Laptops and other portable computers are especially vulnerable to loss and security breaches. Special care should be exercised to protect any proprietary information on these computers and secure network practices should be exercised.
5. Postings by employees from a LIGO email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of LIGO, unless posting is in the course of business duties. Non-LIGO postings and activities should be performed from non-LIGO resources.
6. All computers and related equipment, used by an employee, that are connected to the LIGO Internet/Intranet/Extranet, whether owned by the employee or LIGO, should be continually executing approved virus-scanning software with a current virus database, unless exempted by LIGO management.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

8. Employees should keep their equipment in a secure location to prevent theft. Any transferring of equipment or movement to a new location must be reported to the property manager as well as the local system administrator.
9. Data should be backed up on a regular basis. Employees ***are strongly encouraged*** to use the tools made available at each LIGO location to accomplish this. Employees who elect to store LIGO data on their laptops must accept the responsibility to regularly (e.g., weekly) back up those data. Refer to Section 14 (Policy Enforcement).

6.3 Unacceptable Use

Under no circumstances is an employee of LIGO authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing LIGO-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that may fall into the category of unacceptable use.

6.3.1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by LIGO or its management organization.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which LIGO or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question. (e.g., certain versions of Netscape are not permitted for use outside of the U.S.).
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing one's account password to others or allowing use of one's account by others. This includes family and other household members when work is being done at home.
6. Making fraudulent offers of products, items, or services originating from any LIGO account.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this

section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

8. Port scanning or security scanning is expressly prohibited unless prior authorization by LIGO and its management organization is made.
9. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network or account.
11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
13. Providing information about, or internal lists of, LIGO employees to parties outside LIGO.
14. Unauthorized use of LIGO resources for non-LIGO activities. ***This includes conducting business or other activities for profit.*** LIGO staff should use non-LIGO computing resources for any such activities.

6.3.2. Email and Communications Activities

E-mail is a major means of communication and is a necessary tool being used by LIGO. Use of e-mail, is governed by Caltech and MIT policies. Those policies should also be read. Waste or abuse of system resources is not tolerated.

The following are things not to do with e-mail:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within LIGO's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by LIGO or connected via LIGO's network.
7. All non-LIGO use of news groups is prohibited. This activity should be done through non-LIGO computing resources.
8. Distribution the internal LIGO mailing lists without management authorization.

9. Use of the mailing lists or other e-mail resources for personal agendas. (e.g., Sending a personal political statement to the main LIGO list). Use of major LIGO and LSC mailing lists, should be approved by a supervisor first. Any non-LIGO people needing to use the LIGO mailing lists, must have LIGO Lab Directorate approval.

The following procedures are encouraged:

1. Contact the local system administrator when receiving annoying e-mail or being harassed via e-mail.
2. Use Secure-Shell (SSH) or Secure Socket Layer (SSL/TLS)tunneling when using SMTP, POP or IMAP.
3. Each person is expected to do his or her part to halt the spread of internet viruses.
4. Check with LIGO management to find out which e-mail tools are supported.
5. Certain announcements are OK when appropriate and approved by management. (e.g., Births, weddings, death of an employee). Otherwise only LIGO business related items should be posted to LIGO mailing lists.

7 VISITORS AND PERSONAL EQUIPMENT USE AND SUPPORT POLICY

At any given time, LIGO Laboratory hosts a large number of visitors who are not members of the Laboratory. While the Laboratory appreciates that the practices will vary across different collaborating institutions, it has the reasonable expectation that visitors should comply with the Laboratory's computer usage guidelines while they are visiting LIGO Laboratory or even when they are remotely using its IT infrastructure for *legitimate* activities. Along the same lines there are times in-which LIGO staff may be permitted to use personal equipment for LIGO work. This policy outlines a number of requirements for visitors and their Laboratory sponsors when people visit any of the LIGO facilities as well as staff members using their own equipment.

7.1 Applicability

All LIGO employees are expected to follow this LIGO acceptable use policy (refer to Section 6) while they are at any LIGO Laboratory site. In addition, they are bound by additional policies that apply due to their visitor status when they are not at their home institutions. Use of personal equipment at any LIGO location needs to be approved by the local senior systems administrator and are also bound by additional policies as those of a visitor.

Sponsored Collaborators and short term visitors who use any LIGO computing resource during their stay are obliged to follow the LIGO acceptable use policy (Section 6), the policies of their home institutions, and the policies stated in this document.

7.2 General use and ownership

1. All user accounts; must be approved by LIGO management before the account can be activated. User accounts already active at one LIGO location may be activated at other locations with LIGO management or local System administration approval.

2. LIGO Laboratory system administration reserves the right to: delete, manipulate, or make publicly available any data stored on its computer systems if such measures are deemed necessary and beneficial to the proper operation of LIGO Laboratory. Because of this need to maintain the integrity of LIGO IT infrastructure, LIGO Laboratory is not able to guarantee the confidentiality of information that may be stored on any network device belonging to the Laboratory.
3. Visitors are responsible for exercising good judgment regarding the reasonableness of their own personal use. If there is any uncertainty, visitors should consult either their sponsor or the site system administrator.
4. LIGO recommends that any information which visitors may consider sensitive or vulnerable should be encrypted and stored on the user's local computer disk (note, however, that LIGO cannot guarantee that local disks are backed up regularly). There are a number of URL sites that provide guidelines on encrypting e-mail and other text documents, in particular, the reader is referred to Caltech's IT information site http://www.its.caltech.edu/
5. LIGO Laboratory reserves the right to authorize individuals on its IT staff to monitor equipment, systems and network traffic at any time, as outlined in the LIGO data audit policy (Section 8). Monitoring may be performed for security and network maintenance only by LIGO staff authorized by Laboratory Management.
6. Visitors who will be using Laboratory IT resources (IP numbers, wireless networks, printers, etc.) are obliged to register their MAC address of their computer with the local system administrator. The reader is referred to the following URL to learn how to determine a machine's MAC address: http://docuserv.ligo.caltech.edu/docuserv/computing/faq/faq.html
7. Visitors are responsible for the system administration of their personal computer. The PC user is referred to the URL http://docuserv.ligo.caltech.edu/docuserv/computing/pccmptr.html for hardware configurations that LIGO Laboratory recommends.
8. Long-term visitors may ask for limited support from the local system administrator if their hardware configurations are covered by the recommended hardware list. Site system administration need only provide support as time or priorities permit. Hardware configurations that are not covered under the LIGO recommended list, are considered exceptions. Exceptions; for support by LIGO system administration shall be authorized by LIGO Laboratory Management, on a case-by-case basis.
9. Visitors are required to follow the LIGO acceptable use policy (Section 6) while they are at a LIGO facility for any length of time.
10. Visitors should not use the same password they use at their home institutions for any LIGO account. The reader is referred to the LIGO password policy (Section 11) for more details.
11. Visitors and their sponsor should contact the local system administrator upon their first arrival before any computer related activity is performed. Sponsors may not issue passwords, IP addresses or other information without prior approval by the site system administrator.

12. Long-term visitors are urged to provide the local system administrator the root password to their personal machines. This may prove helpful in case of problems at some later time.
13. The General Computing IT group is not responsible for providing support for other LIGO Laboratory computing areas, such as CDS, GDS, or LDAS. Exceptions may be made on a case-by-case basis.
14. LIGO will not provide commercial software for any non-LIGO systems.
15. Visitors supported by the Laboratory are obligated to follow the employee guidelines for backup of LIGO-related work (please see above), or to copy work regularly (e.g., daily) to a Lab computer directly or via email attachments for subsequent backup.

7.3 Conferences and Short Term Visits

1. Personal computer usage is limited to designated conference areas while at a LIGO facility;
2. LIGO equipment or resources may not be used without prior approval;
3. Posted DHCP and wireless guidelines supercede other policies during a conference.
4. Check and install the latest security patches and virus updates before attending the conference.

LSC meetings will be handled in the following manner. The web-based registration form will be modified to require MAC address registration and acknowledgement of the provisions of this Computer Use Policy as a necessary step in the registration process.

8 WIRELESS COMMUNICATIONS POLICY

This policy prohibits access to LIGO networks via unsecured wireless communication mechanisms. Only wireless clients and hosts that meet the criteria of this policy, or have been granted a specific waiver by LIGO management to use Laboratory wireless networks are permitted.

This policy covers those wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) that can be used to connect to any LIGO internal IT computing network. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to LIGO IT networks are not subject to this policy (e.g., mobile phones). However, these devices do fall under other regulations at the Observatories regarding EMI. EMI policies are site-specific and readers will be informed of the constraints they impose when they visit LIGO Laboratory sites.

All LIGO Laboratory wireless network implementations must:

1. Maintain a hardware address that can be registered and tracked, i.e., a MAC address.
2. Support strong user authentication which checks against an external database such as TACACS+. RADIUS or a similar method may be enforced in the future along with encryption.

All wireless network communications outside office areas needs approval by the site LIGO Laboratory management. All lab areas are limited to documented and approved wireless

equipment. A published list of approved equipment is posted at each LIGO location. EXCEPTIONS: A limited-duration waiver to this policy for emergency situations has been approved, if specific implementation instructions are followed.

Conferences and related public meetings will not require users to use encryption. However, MAC address registration will be encouraged. Wireless coverage in these situations will be limited to the conference meeting area.

9 REMOTE ACCESS POLICY

This policy is to provide standards for connecting to LIGO's network from outside the LIGO network. This information is designed to minimize the potential exposure to LIGO from damages, which may result from unauthorized use of LIGO resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical LIGO internal systems, etc.

This policy applies to all LIGO employees and associates with a LIGO user account This policy applies to remote access connections used to do work on behalf of LIGO, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, and cable modems, etc.

The Caltech VPN information can be found at:

http://www.its.caltech.edu/its/services/networkra/vpn/index.shtml

9.1 General Policy

1. It is the responsibility of LIGO employees and visitors with remote access privileges to LIGO local area networks to ensure that their remote access connection is given the same consideration as a user's local on-site connection to LIGO.
2. Requests; for remote access privileges, must be approved by LIGO management. This includes the dial-in modems.
3. Requests; for home access via ISP and LIGO support, must be approved by the LIGO Directorate.
4. General access to the Internet by household members through the LIGO Network on personal computers is discouraged. Remote access to the LIGO systems should be used only for work related purposes. These resources are not intended for friend or family member usage.
5. The following information provides details for protecting data when accessing the LIGO network via remote access methods for acceptable use of LIGO networks:
   - The Caltech Virtual Private Network (VPN) Policy is available from the following URL: http://www.its.caltech.edu/its/services/networkra/vpn/index.shtml
   - Wireless communications policy discussed in Section 8 above.

- The LIGO Caltech Modem Use Policy (The 1-800 number is for those on travel) available from the LIGO internal web server at URL:
  http://docuserv.ligo.caltech.edu/docuserv/computing/ligonetwrk.html
  For other site specific modem access the site administrator should be contacted.
- Acceptable use policy, all visitors and LIGO employees are expected to comply with the provisions discussed in Section 6. Further, LIGO employees are responsible for ensuring that any family members using the LIGO network does not violate any part of this policy.
- Guidelines for remote users, described in Section 9.

6. All employees and visitors must obtain permission from LIGO Laboratory management before using any remote access to the LIGO network

9.2 Requirements

1. Secure remote access must be strictly controlled. The use of VPN, SSH, SSL or some type of protected communication should be used for all remote access.
2. At no time should any LIGO employee provide his or her login or email password to anyone, not even family members.
3. LIGO employees and associates with remote access privileges should ensure that their personal computer or workstation, which is remotely connected to a LIGO network, is not being used by another network at the same time. An exception is made for private personal networks that are under the complete control of the user. Client remote computers, which are not part of the LIGO IP address domain, are not to be used as gateways into the LIGO network.
4. Non-standard hardware configurations; should be approved by LIGO management and the local system administrator, prior to their use for remote access. The system administrator should be contacted for information concerning security configurations for access to LIGO networks.
5. All hosts that are connected to LIGO internal networks via remote access technologies should use the most up-to-date anti-virus software with weekly complete disk scans. Personal computers used from home are covered by this policy. If unable to comply with this policy, no files should be transferred.
6. Personal equipment that is used to connect to LIGO networks should meet the requirements of LIGO-owned equipment for remote access.
7. Individuals wishing to employ non-standard remote access methods form connecting to the LIGO network must obtain prior approval from LIGO management.
8. The use of a local firewall protection software and/or NAT router filtering is encouraged.

10 AUDIT POLICY

1. The LIGO system administration team is provided the authority by LIGO management to conduct a security audit on any system at LIGO. This policy covers all computer and communication devices owned or operated by LIGO. This policy also covers any computer and communications device that are present on all LIGO premises, which may not be owned or

operated by LIGO. As mentioned in the introduction of this document, there should be no expectation of privacy when using any of the LIGO computing or network resources.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to LIGO security policies
- Monitor user or system activity where appropriate.
- Check the integrity of backup tapes and other media.

2. When requested, and for the purpose of performing an audit, any access needed will be provided to members of the LIGO system administration group. Special, audit activities must be approved by LIGO management, before the audit is performed.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on LIGO equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on LIGO networks.

Special Audits may include:

Audit of ‘martian’ or private network units.
Audit of internal LAB units.

Normal auditing will be performed on a regular basis for servers and gateway machines.

3. MIT and Caltech central Information Services staff, and equivalent organizations at the Observatories, are authorized to, and regularly do, audit all data flowing over their networks. They have the authorization to use data they seize according to their own regulations and to revoke the right of a machine or a user to use their resources.

4. Any violation of the audit may result in the equipment being disconnected until the issue is resolved.

11 PASSWORD USAGE POLICY

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of LIGO's entire network. As such, all LIGO employees and associates are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of passwords, the protection of those passwords, and the frequency of change.

11.1 General

1. All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed on a regular basis.
2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months. (Password aging may be enabled to enforce this policy).
3. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user. Passwords should be different at each location the user has an account.
4. System and user account passwords must not be inserted into email messages or other forms of computer communication.
5. All user-level and system-level passwords must conform to the guidelines described below.

11.2 Guidelines

11.2.1. General Password Construction Guidelines

Passwords are used for various purposes at LIGO. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words “LIGO”, “Wilson”, “albert”, “caltech” or any form of them.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down in an easily accessible location or stored on-line. Passwords written down should be stored in a secure location. Easily remembered passwords

should be used. One way to do this is create a password based on a song title, affirmation, or other phrase, with suitable substitutions.

NOTE: For additional information on appropriate passwords check the local institution's password policy. A good source is http://www.its.caltech.edu/its/help/policies/passwords.shtml

11.2.2. Password Protection Standards

It is not permitted to use the same password for LIGO accounts as for other non-LIGO access (e.g., personal ISP account, CIT campus account, etc.). Where possible, don't use the same password for various LIGO access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

LIGO passwords must not be shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, LIGO information.

Here is a list of things that should not be done:

- Revealing a password over the phone to any non-authorized person.
- Revealing a password in an email message.
- Revealing a password to a supervisor, except when required as part of the job function.
- Talking about a password in front of others.
- Hinting at the format of a password (e.g., "my family name")
- Revealing a password on questionnaires or security forms.
- Sharing a password with family members.
- Revealing a password to co-workers.

If someone requests someone else's password, the requester should be referred to this document or he should contact one of the LIGO system administrators.

The "Remember Password" feature of applications should *never* be used (e.g., Eudora, OutLook, Netscape Messenger).

Again, passwords should *never* be stored in one's desk, office or un-secure location. They should *never* be stored in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Passwords should be changed at least once every six months. The recommended change interval is every four months. To date, LIGO has not enforced password aging, however it may elect to do so in the future.

If an account or password is suspected of having been compromised, the incident must be reported *immediately* to the local system administrator and all passwords suspected to have been affected must be changed.

Password cracking or guessing applications will be run in the background at random times by LIGO or its delegates. If a password is guessed or cracked during one of these scans, the user will be notified privately and will be required to change it.

11.2.3. Application Development

Application developers must ensure their programs contain the following security precautions:

- Applications should support authentication of individual users, not groups.
- Applications should not store passwords in clear text or in any easily reversible form.
- Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

11.2.4. Use of Passwords for Remote Access Users

Access to the LIGO Networks via remote access is to be controlled using a VPN or secure-shell (SSH) connection. Those with modem accounts and using the account on a regular basis should change their password every few months.

12 GUIDELINES ON THE USE OF ANTI-VIRUS APPLICATIONS

This provides a non-exhaustive list of recommended procedures to prevent virus problems:

- Laboratory standard, supported anti-virus software should be used. Sources of these applications include university IT services download sites (ITS at Caltech, IS at MIT). Current versions should always be used, and the latest set of anti-virus software updates should be downloaded and installed as they become available. Detailed information on installing the s/w can be found at the following location: http://www.docuserv.caltech.edu/
- Files or macros attached to an email from an unknown, suspicious or untrustworthy source should *never* be opened or downloaded. Such attachments should be deleted immediately, then "double deleted" by emptying the Trash. Some applications, such as Qualcomm's Eudora, automatically download attachments to an attachment download directory. Users must make sure to delete these files from the attachment directory and not only the e-mail message itself.
- LIGO system administrators and, if it is deemed appropriate, local campus IT services, should be notified whenever email is received that is suspected of being infected by software virus or worm.
- Spam, chain, and other junk email should be deleted without forwarding. At all times compliance with the acceptable use policy (Section 6) is required. Saving infected files should be done only when asked to do so by system administrators.
- Files from unknown or suspicious sources should never be downloaded.
- Direct disk sharing with read/write access is to be avoided unless there is absolutely a legitimate and unavoidable official need to do so.
- All floppy diskettes from an unknown source should be scanned for viruses before using it.

- Users should back-up critical data and system configuration files on their machines that cannot be backed up over the network as part of the nightly process. This should be performed on a regular basis and data should be stored in a secure place. Your IT systems administrator will help you find a suitable approach.
- If there are conflicts with anti-virus software, first run the anti-virus utility to ensure a clean machine, then disable the software and run the application. When finished with the specific application, re-enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered daily. Virus definition file updates need to be performed on a weekly basis. There are methods to automate the procedure. If there are any questions concerning a file or installing the virus-scan software, contact the local system administration.

13 PROCEDURES FOR DEVELOPERS AND PERSONS WITH SERVER AND NETWORK ROOT ACCESS PRIVILEGES

Certain individuals working on software and hardware development in LIGO Laboratory CDS, GC, and LDAS groups require root level access to servers, routers, switches, and other LIGO Laboratory hardware and LAN components. Root level access to these components is a *privilege* and not a right. The following actions are *expressly prohibited* without requesting and getting prior approval from the Senior Systems Administrators (SSA) at the various LIGO Laboratory sites where these activities may need to take place:

- All computers and network components that are needed for development activities and that require extraordinary privileged access by persons (from, e.g., CDS and LDAS) who are not members of the LIGO Laboratory General Computing systems administration group shall be assigned to a responsible administrator who shall be personally responsible to LIGO General Computing for appropriate operation of these machines.
- Root passwords on computer/network equipment shall be provided by the local Senior Systems Administrator and may not be changed without prior approval from the SSA. Local password files on servers shall be provided in a timely manner when requested by the SSA.
- All servers must be configured with permanent IP addresses with registered MAC addresses. New hardware may not be introduced to replace existing hardware by reusing the same IP address without prior approval of the SSA.
- New hardware may not be configured without prior approval of the SSA; DHCP may not be used to introduce new hardware on the network without prior consultation with the SSA.
- The LIGO Laboratory LAN topology *may not be altered in any manner* without prior approval of the SSA. All changes must be documented via a schematic showing the current and proposed change. This includes, but is not limited to:

- Introducing NAT routers or other firewall or gateway hardware;
- Setting up any form of VPN (IPsec, OpenVPN, OpenSSH, Cisco, etc.) or other forms of connections which would tunnel or otherwise make a machine appear to be a member of a "foreign" network;
- Private (‘martian’) networks may not be set up within any LIGO Laboratory LAN without prior approval of the local SSA. Root access to such networks, the MAC addresses of the hardware involved, and the physical location of such units must be provided to the local SSA as part of the approval process. Once set up these may not be altered in any manner without further contacting the SSA.

- Server OS configurations may not be changed without prior approval by the SSA. Such changes include, for example,

  - changing the SSH configuration to allow remote ssh login as root;
  - starting non secure processes on the servers, such as RSH, FTP, telnet, etc.;
  - setting up DNS, mail servers, web servers, etc.

14 ENFORCEMENT OF THE POLICIES

It is neither possible nor warranted for LIGO Laboratory to monitor all users all the time. LIGO expects that individuals who have been entrusted and privileged to use its IT infrastructure will comport themselves responsibly at all times. ***This includes taking proper measures to safeguard LIGO data or work through the regular use of backups.*** In the event that it is determined that one or more individuals have violated these policies LIGO Laboratory management reserves the right to block or shut down the computing equipment that was used in the violation. The laboratory management may also decide to close or block access to specific accounts or by specific users until the issue is resolved. Individuals who are the subject of such action will need to obtain the permission of LIGO management before they can resume their computing related activities. In certain exceptional cases, LIGO employees may be subject to disciplinary action by their respective home institutions.

15 ACCESS TO NON-GENERAL COMPUTING SYSTEMS

Access to CDS and LDAS is limited and only allowed on a case by case basis. Authorization to use these systems must be made by the managers of the systems at each LIGO location.