

Marine Biological Laboratory

Network Security Policy

Initiated by: Director, Information Systems Division
Approved by: MBL Computer Advisory Committee
Date: August 29, 1994
Revision: November 29, 2001
Distribution: All Users of the MBL Network

1.0 Policy Statement:

It is the policy of the Marine Biological Laboratory ("MBL") to prohibit the unauthorized use of the MBL Network itself and those computing resources connected to the network. The network utility at the MBL is dedicated to facilitating high speed communication between and among the research communities, various government organizations, information providers and other commercial vendors and companies. The MBL Network is the property of MBL. MBL reserves the right to change, modify or revoke this policy with or without notice, at any time.

2.0 MBLnet Security Policy Goals:

- 2.1 Availability - ensure that systems, networks, applications, utilities, and data are on-line and accessible when authorized users need them.
- 2.2 Integrity - protect user information, data or software from improper modification or access (i.e. virus or unauthorized access/modifications.)
- 2.3 Confidentiality - assure that sensitive data is read only by authorized individuals and is not disclosed to unauthorized individuals or to the public.
- 2.4 Propriety - ensure that the MBL Network is used only for its intended purposes and not for any prohibited activities and uses.

3.0 Conditions and Procedures For Use:

MBLnet users shall adhere to the conditions and procedures set forth in this policy. Violation of this policy will result in the loss of network privileges and may result in criminal or civil prosecution and/or disciplinary action for MBL employees up to and including discharge.

3.1 All users of MBLnet shall abide by the following conditions and procedures:

- 3.1.1 Users shall not make unauthorized copies of data or software, however, the user is responsible for ensuring that data under their purview is adequately and routinely backed up.
- 3.1.2 Users are to choose passwords wisely and to keep them secret (Policy No.H2.2).
- 3.1.3 Users are to access the system and data in an authorized fashion only.
 - 3.1.3.1 Users shall not allow access or use of their account to any other individual or group.
 - 3.1.3.2 Users shall not leave their computer logged in to networked services and unattended. Users shall use password protected screen savers and/or log out of applications before leaving the computer.
 - 3.1.3.3 Users shall not give system or site related information to an unauthorized person either in person in any manner, by telephone, email, written material, etc.
 - 3.1.3.4 Users shall not type a command or a password for an unauthorized person.

- 3.1.3.5 Users shall not send security related information (i.e. a password) over E-mail.
- 3.1.3.6 Users shall not give accounts on personal workstations to unauthorized users.
- 3.1.4 Security violations or unusual activity should be reported immediately to helpdesk@mbi.edu.
- 3.1.5 Unusual activity could include:
 - 3.1.5.1 mysterious or missing files
 - 3.1.5.2 attempted use of a user's account without his/her consent.
- 3.1.6 Users acknowledge the right of the organization to monitor system use for legitimate business purposes, including security purposes, as set forth in § 6.0.
- 3.1.7 The networked servers are not for personal use and the organization will not be held liable for safeguarding any personal data or programs placed on the servers.
- 3.1.8 Users are responsible for coordinating with the MBLnet Network Manager any network activity or additional connections that may affect MBLnet performance. Network connections may be obtained only in the authorized manner by contacting ISD.
- 3.1.9 Users are not to install or execute any programs or processes which are designed to gather information about the MBL network, the servers, or other machines on the Internet, both inside and outside of MBL.
- 3.1.10 Users are not to purposefully access MBLnet or any MBL or Internet servers or computers in a manner which disguises the user's identity, computer name, address, location, or other identification of the electronic source.
- 3.1.11 Users are to ensure that all use of computing and network resources is consistent with the educational and scientific mission of the MBL.
- 3.2 Information Systems Division ("ISD") reserves the right to remove user accounts and/or revoke network access privileges for cause. For purposes of this policy, "cause" is defined as the user's failure to adhere to the conditions or procedures set forth in this policy or engaging in any other inappropriate conduct with respect to the MBL Network.
- 3.3 System Administrators will be responsible for :
 - 3.3.1 managing and overseeing security to ensure privacy and integrity of user information.
 - 3.3.2 monitoring the system for security breaches and unauthorized activity using available security utilities and software.
 - 3.3.3 using available utilities to ensure secure movement of data within MBLnet and over the Internet.
 - 3.3.4 taking every precaution to minimize network and machine downtime.

4.0 Prohibited Activities and Uses:

- 4.1 The network shall not be used to transmit any communication where the meaning of the message, the content of the file, or the operation of the application, including its transmission or distribution, would violate any applicable law or regulation or would likely be offensive to the recipient or recipients thereof.
- 4.2 For example, the use of foul, obscene, discriminatory, unlawful or harassing language or images when sending or displaying messages on e-mail is prohibited.

4.3 Also, it is unacceptable to use the Internet to send, display, download or print offensive messages or pornographic materials or sexually explicit pictures, derogatory religious or racial or defamatory material.

5.0 Unsolicited advertising:

Unsolicited advertising may not be "broadcast" or otherwise sent to any user of the MBLnet network or any directly or indirectly attached network. However, when requested by a user of the networks, product information and other commercial messages are permitted to be transmitted over the network.

6.0 Monitoring:

MBL does not intend, as a matter of policy, to randomly monitor the use of technology (including e-mail), and will consider the individual user's limited interest in privacy to the extent feasible and consistent with MBL's institutional interests and goals set forth herein. A limited number of authorized MBL personnel will have unrestricted access to and may monitor information stored on the MBL Networked servers (including e-mail) for legitimate business purposes. These may include, but are not limited to, retrieving business information; trouble-shooting hardware and software problems; preventing system misuse and the unauthorized accessing of confidential, proprietary or trade secret information; assuring compliance with software distribution policies; security purposes; and complying with legal and regulatory requests for information. Given these business requirements, MBL cannot guarantee the privacy of documents and messages stored in the network. Accordingly, MBL reserves the right to access and review all information on the system for legitimate business purposes.

7.0 Security:

Users are hereby notified that access to the MBL network increases the vulnerability of whatever equipment is connected to the network. MBL makes no warranty either expressed or implied with respect to security measures implemented on the network or computing resources. Users shall be responsible for their own security measures to protect their hardware, software and data.

8.0 Virus Control and other Compromises:

8.1 Users must ensure that any media (i.e. disks, CDs or any computer equipment) brought into the MBL from outside is free of viruses, worms, or other compromises before used in a PC or connected to the network. If a user is uncertain how to check a disk or computer, he or she should contact the help desk.

8.2 If a virus, worm, or compromise is detected or suspected, the user should contact the help desk immediately.

8.3 Users should use **EXTREME CAUTION** when opening e-mail attachments. E-mail has become the most likely way viruses are spread. If a user does not know the recipient or is not expecting the attachment, then the attachment should **NOT** be opened.

8.4 Another frequently used "social virus" is in the form of an e-mail that urges the recipient to send everyone he or she knows a copy of the e-mail. Often it professes to protect against a new virus or serious incident. Users should **NOT** forward copies of such an e-mail, which often is a hoax. Users can, however, forward one copy to the help desk to verify the claim.

8.5 MBL Administrative computers are equipped with a corporate AntiVirus protection program by ISD. The computer user may not alter settings of this program.

9.0 Policy Updates:

Policy clarification and updates are available from the Information Systems Division.