Marine Biological Laboratory

Written Information Security Policy

Initiated by: Information Technology
Approved by: Director/CEO
Date: September 16, 2010
Revision: 
Distribution: MBL Community

1.0 Policy Statement:
Marine Biological Laboratory (MBL) developed this Written Information Security Policy (the “WISP”) to protect Personal Information, as that term is defined below, found on records and in systems owned by the laboratory. This WISP is intended as a comprehensive set of guidelines and policies that have been implemented in compliance with regulations issued by the Commonwealth of Massachusetts entitled “Standards For The Protection Of Personal Information Of Residents Of The Commonwealth” (201 Code Mass. Regs. 17.00) This WISP will be periodically reviewed and amended as necessary to protect Personal Information.

This WISP should be read in conjunction with other Laboratory record-keeping and privacy policies that are cross-referenced at the end of this WISP.

2.0 Purpose
The purposes of this document are to:

2.1 Establish a WISP for MBL with policies designed to protect the Personal Information of students, scientific staff, and other employees of the Laboratory that is maintained by the MBL.

2.2 Establish employee responsibilities in safeguarding data containing Personal Information.

2.3 Outline procedures to implement and administer this WISP, including administrative, technical and physical safeguards.

3.0 Definitions:

3.1 For the purposes of this WISP, MBL employees include all faculty, scientific staff, administrative staff, members of the collective bargaining unit, contract and temporary workers, and consultants.

3.2 Personal Information, as used in this WISP, means the first name and last name or first initial and last name of a person in combination with any one or more of the following:
- Social Security number;
- Driver’s license number or other state-issued identification card number; or
- Financial account number or credit or debit card number that would permit access to a person’s financial account number, with or without any required security code, access code, personal identification number, or password.
4.0 Responsibilities
4.1 The Information Security Officer (the ISO) is in charge of maintaining, updating, and implementing this Program. The ISO can be contacted at iso@mbl.edu.

The ISO reviews incidents of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Personal Information, and, when appropriate, convenes a team of employees (Security Committee) to form an incident response task force to determine appropriate responses when a breach occurs. The ISO documents all breaches and subsequent responsive actions taken. Records of breaches are retained in a file in the office of the ISO.

4.2 All employees and, to the extent relevant, students are responsible for maintaining the privacy and integrity of Personal Information, and are required to access, store and maintain records containing Personal Information in compliance with this WISP.

5.0 Reporting Attempted or Actual Breaches of Security
Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Personal Information, or of a breach or attempted breach of the information safeguards adopted under this WISP, must be reported immediately to the ISO.

6.0 Risk Assessment
6.1 In developing this WISP, the ISO identified, to the extent reasonably feasible, the locations of all Personal Information maintained by MBL.

6.2 Risk assessment takes into consideration risks in each relevant area of the MBL’s operations, including employee training, compliance with this WISP, and means for detecting and preventing security system failures.

6.3 The ISO, along with the Security Committee, has identified and continues to identify the reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Personal Information that could result in unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of such information. Among the foreseeable risks are external hacks, unauthorized access, thefts, inadvertent destruction of records, unintentional authorization of access, property damage from environmental hazards, and misuse of access by employees, faculty, students or business associates.

6.4 The ISO, along with the Security Committee, has assessed, and on a continuing basis reviews, the sufficiency of safeguards currently in place to control these risks.

7.0 Violations
Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Personal Information without authorization, or who fails to comply with this WISP in any other respect, will be subject to disciplinary action, up to and including termination in the case of employees and expulsion in the case of students.

8.0 Policies and Procedures for Safeguarding Information
To protect Personal Information, the following policies and procedures have been developed that relate to protection, access, storage, transportation, and destruction of records, computer system safeguards, and training.
8.1 Access
8.1.1 Only those employees or authorized third parties requiring access to Personal Information in the regular course of their duties are granted access to Personal Information, including both physical and electronic records.
8.1.2 Computer access passwords are disabled upon termination of employment.
8.1.3 Upon termination of employment, physical access to documents or other resources containing Personal Information is immediately prevented.

8.2 Storage
8.2.1 No MBL employee may store Personal Information on a laptop or on external devices (e.g., flash drives, mobile devices, external hard drives, SaaS applications, external servers) without express authorization by the ISO, and such authorization requires encryption of data and other appropriate safeguards.
8.2.2 Paper records containing Personal Information must be kept in locked files or other secure areas when not in use, and may not be removed from the premises of the MBL, without the express permission of the ISO.
8.2.3 Electronic records containing Personal Information must be stored on secure servers, and, when stored on authorized desktop computers, must be password protected.

8.3 Removing records from campus
8.3.1 When it is necessary to remove records containing Personal Information off campus, employees must safeguard the information. Under no circumstances are documents, electronic devices, or digital media containing Personal Information to be left unattended in any insecure location.
8.3.2 When there is a legitimate need to provide records containing Personal Information to a third party, electronic records are password-protected and encrypted, and paper records are marked confidential and securely sealed.
8.3.3 Marine Biological Laboratory takes all reasonable steps to select service providers that are capable of maintaining appropriate security measures to protect Personal Information as required by Mass 201 CMR 17.00.

8.4 Disposition
8.4.1 Destruction of paper and electronic records must be carried out in accordance with the MBL’s Records Management Policy, Chapter 93I of the Massachusetts General Laws, and any other applicable federal, state and local regulations.

8.5 Third-party vendor relationships
8.5.1 MBL exercises appropriate diligence in selecting service providers to determine that they are capable of maintaining appropriate safeguards for Personal Information provided. The primary budget holder for each department is responsible for determining those third parties providing services to the laboratory that have access to Personal Information. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect Personal Information consistent with this WISP and Massachusetts laws and regulations.

8.6 Computer system safeguards
8.6.1 The ISO monitors and assesses information safeguards on an ongoing basis to determine when enhancements are required. To combat external risk and secure the MBL’s network and data that contain Personal Information, MBL has implemented the following:
8.6.1.1 Secure user authentication protocols
• Unique strong passwords are required for all user accounts; each employee receives an individual user account.
• Passwords are required to be changed annually.
• Server/User accounts are locked after 5 successive failed password attempts within 5 minutes.
• Computer access passwords are disabled prior to an employee’s termination.
• User passwords are stored in an encrypted format; root passwords are only accessible by system administrators and direct back-ups.

8.6.1.2 Secure access control measures
• Access to specific files or databases containing Personal Information is limited to those employees who require such access in the normal course of their duties.
• Each such employee has been assigned a unique password, different from the employee’s password to the computer network or has been restricted by system server permissions.

8.6.1.3 Files containing Personal Information transmitted outside of the MBL’s network are encrypted.

8.6.2 The ISO performs regular internal network security audits to all server and computer system logs to discover the extent reasonably feasible for possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Personal Information.

8.6.3 All MBL-owned computers and servers are firewall protected and regularly monitored.

8.6.4 Operating system patches and security updates are installed to all servers at least every 30 days.

8.6.5 Antivirus and anti-malware software is installed and kept updated on all servers and workstations. Virus definition updates are installed on a regular basis, and the entire system is tested and checked at least once per month.

9.0 Training
Appropriate initial and periodic ongoing training is provided to all employees who are subject to policies and procedures adopted within this WISP or who otherwise have access to Personal Information. The ISO maintains appropriate records of all such training.

10.0 Policies referenced
The following Marine Biological Laboratory policies provide advice and guidance that relates to this WISP:

• Records Management Policy
• Password Policy
• Acceptable Use Policy
• Network Security Policy
• Archival Policy
• Access to Archival Records policy
• Financial Systems & Security Password Policy

11.0 Effective Date
11.1 The Written Information Security Program (WISP) is effective August 10, 2010
11.2 The MBL will review this WISP at least annually and reserves the right to change, modify, or otherwise alter this WISP at its sole discretion and at any time as it deems circumstances warrant.

12.0 Policy Clarification and Updates:
Policy clarification and updates are available from the Information Technology office.