# Department of Biochemistry and Molecular Biology
# Information Technology Security and Acceptable Use Policy

Scope: This policy is to be applied in addition to the current Michigan State University Acceptable Use of Computing Systems, Software, and the University Digital Network Administrative Ruling http://www.msu.edu/au/This policy will describe procedures and protocols for information security and systems management, incident response, disaster recovery, and operations and security.

## Procedures:

### I. Information Security and Systems Management

Electronic records containing confidential and proprietary information should be stored on centralized data servers whenever feasible. This can include databases or file servers. Computers used to access electronic records containing confidential and proprietary information shall be locked against unauthorized use when unattended (for example, employing a screen saver with a password lock). The storage of confidential and proprietary information on mobile computing devices, such as laptops or "smart" phones, is strongly discouraged. If such data must be stored on these devices, the use of data encryption to encode the information is strongly encouraged, to ensure its integrity in the event of theft of the physical device.

Refer to document "Securing Enterprise Data at Michigan State University" (secureit.msu.edu/sid/index.html) for policies and procedures.

Confidential Information

Examples of confidential information include, but are not limited to:

- Social security number
- Credit card/debit card number
- Bank account numbers, Automated Clearinghouse (ACH), Electronic Funds Transfer (EFT) account numbers and related information
- Driver's license number
- Names, addresses and phone numbers when used in conjunction with any of the above data and other personal data such as date of birth, mother's maiden name, or when restricted or protected by the individual
- Student records that are protected by the Family Educational Rights and Privacy Act (FERPA) or the University's Guidelines Governing Privacy and Release of Student Records (www.reg.msu.edu)

- Protected health information under the Health Insurance Portability and Accountability Act (HIPAA), including student number and student name pairings
- Personal financial information as defined and governed by the Gramm-Leach-Bliley Act (GLB)
- Research information-as defined and governed by federal regulation (45 CFR 46, 21 CFR 50, 21 CFR 56) and the university's Internal Review Boards (hrpp.msu.edu/)
- Proprietary information owned, used, or in the possession of the University, such as computer applications for which MSU owns the code or a license, or other intellectual property
- Employment data such as benefits enrollment, beneficiary data, and certain grievance, arbitration or legal proceeding documentation
- Security codes, combinations, and passwords

Proprietary Information

Proprietary information means information, records, or data whose value would be lost or reduced by disclosure or by disclosure in advance of the time prescribed for its authorized public release, or whose disclosure would otherwise adversely affect the University financially. Examples of proprietary information includes but are not limited to:

- Research data or results prior to publication or the filing of a patent application.
- Non-patentable technical information or know-how that enhances the value of a patented invention or that has independent commercial value.
- Information about the University's intention to buy, sell, or lease property whose disclosure would increase the cost of that property for the University or decrease what the University realizes from that property.

## II. Incident Response

In the event of a suspected compromise of a data system, the university's GUIDELINES FOR INTERNAL AND EXTERNAL REPORTING OF DATA SYSTEM SECURITY BREACHES (itservices.msu.edu/guidelines-policies/data-breach.html) will guide the departmental response.

A reportable incident occurs when (a) an unauthorized person is believed to have gained the ability to access confidential or proprietary data that is stored on a University data system, or (b) a person who is authorized to access confidential or proprietary data that is stored on a university data system misuses that data.

Upon discovery of the compromise of the data system, the following steps should be taken:

- Contact departmental IT administrator.
- Leave affected systems on and attached to the network until investigators direct otherwise
- Do not log on or perform administrative functions on the affected system until investigators arrive
- Record, in writing, all actions taken in connection with the discovery of the reportable incident-indicating date and time.

## III. Disaster Recovery/Business Continuity

The Departmental Research Emergency Defense (Information System) [REDIS] plan documents responses by individual laboratories and the BMB Stores. The plan is available through the BMB emergency response manager or through the university's Department of Public Safety. Departmental business functions will be re-constituted through the loading of back-up information onto a replacement server and individual PCs. All business function information is acquired through university sources (Contracts and Grants, HR, etc.) and does not represent information that is only housed in BMB. Therefore, back-up of primary information is available from non-departmental sources.

## IV. Operations and Security

The IT manager will oversee training of all users within BMB with access to confidential and proprietary information. Training will instruct users in topics such as: confidentiality, malicious software, and use of passwords. Periodic training updates will be conducted when necessary.

Information that is classified Confidential and Proprietary must be kept in a place that provides a high-level of protection against unauthorized access and not taken outside the University unless it can be assured adequate protection. In general, this means storing the information behind a physical or electronic lock, for example, in an office, filing cabinet, or desk that is kept locked when the User is not present, or on a computer that provides strong access controls and encryption. Encryption consistent with University standards is strongly recommended for information stored electronically on all computers, especially portable devices such as notebook computers or Personal Digital Assistants (PDAs) that are vulnerable to theft or loss.

It is the responsibility of all users to inform the IT Manager of any IT equipment purchases or transfers. It is the responsibility of the IT Manager to update the Departmental IT Asset Log. When equipment is to be disposed, it is the responsibility of the IT Manager will to ensure that all storage media has been properly cleaned and sanitized.

It is the responsibility of the IT Manager to conduct regular system back-ups and to maintain a secure, off-site storage location for back-up.