

Approved: August 8, 2008

University of Massachusetts

Data Security Breach, Unauthorized Data Disclosure or Compromise Incident Handling and Notice Procedures

I. Introduction

Several laws allow for the disclosure of electronic information (e.g., USA Patriot Act, Electronic Communications Privacy Act – ECPA, Digital Millennium Copyright Act -DMCA) while others restrict the disclosure of certain types of information (e.g., Family Educational Rights and Privacy Act – FERPA; Health Insurance Portability and Accountability Act of 1996 – HIPAA; Graham Leach Bliley Act – GLBA, etc.) usually referred to as personally identifiable or personal information. The disclosure of electronic information is based on a certain set of legal procedures, documents and protocols. In order for the University to fulfill both its legal responsibilities under the law and its obligations to notify impacted parties of data security breaches and unauthorized data disclosure/compromise, consistent procedures must be followed when responding to data security breach and unauthorized data disclosure/compromise related incidents and internal and external notice of these event. This Procedure addresses the following issues:

- General Information
- Data Security Incident Handling Process
- Disclosure of Security Breach and Unauthorized Disclosure/Compromise of Data

II. General Information

This Procedure is in compliance with state and federal laws, and University policies, standards and plans.

The University of Massachusetts stores, displays, uses and transmits various types of data/information to enable faculty and staff to perform necessary business and educational operations. The allowed disclosure of much of this data is controlled by federal law. Although these laws do not, in themselves, require external notification of a security breach or unauthorized disclosure/compromise of data, [Massachusetts General Law 93H](#) defines a subset of data for which external notification is required. This document outlines the situations in which external notification is required.

III. University Incident Handling

A. Data Security Incident

A **data security incident** is any event whereby some aspect of computer security or University data is threatened and/or adversely impacted. The significance/priority of a suspected/declared incident will determine who is notified and which steps are included in the incident handling process. For more information regarding incident priorities/levels see the [University Cybercrime and Data Security Incident Plan and Process](#).

B. Verification of Compromise

When a security breach or unauthorized disclosure/compromise of University personally identifiable or protected data (as defined in the [Data and Computing Definitions](#) document) is suspected, the appropriate Campus Incident Coordinator should be contacted. The Coordinator will direct the appropriate Investigating Team, based on the type and level of suspected incident, to verify the suspected breach/compromise.

An Investigating Team should be constituted to determine the legitimacy, priority and significance of the suspected incident, and whether personally identifiable or protected information has been compromised. If it is confirmed that PII or protected data was compromised, the Investigating Team should also determine whether the compromised PII or protected information was or was not encrypted, and whether the related encryption key has also been compromised.

Approved: August 8, 2008

In making this determination the Investigating Team should consider if there are indications that the PII or protected information:

- Is in the physical possession and control of an unauthorized person (e.g., lost or stolen laptop with personally identifiable or protected information stored on it).
- Has been downloaded or copied (e.g., an ftp log contains the name of a file containing personally identifiable or protected information).
- Was used by an unauthorized person (e.g., fraudulent accounts opened, identity theft reported).
- Was tampered with or modified in any way (e.g., changing admissions status).

The Investigating Team should also attempt to determine the duration of the exposure, the likelihood of substantial risk of identify theft or fraud to impacted individuals, and in the case of an attack, whether the attack, was a directed/targeted attack (e.g., the computer system was specifically targeted by the unauthorized individual), whether the attack intended to find and collect personally identifiable and/or protected data, if the unauthorized individual attempted to cover up their activity, or if the unauthorized activity has been publicized/announced by the perpetrator. This information will assist University management in determining whether any further internal or external notification is appropriate.

Incident investigation and follow-up shall be in compliance with the [University Cybercrime and Data Security Incident Plan and Process](#) (i.e., completing proper documentation, etc.) until the incident is officially closed. Investigation notes should indicate the steps taken to determine the nature and scope of the incident, including who did what, when, how and why specific steps were taken. The notes/documentation should be chronological and factual. Care should be taken to avoid speculation and assumption.

The first priority of the Investigating Team is to remove further unauthorized access/system compromise while maintaining a forensically sound system/data image for future analysis. The second priority is to restore service/operations to users in an expeditious manner, provided service/operations can be restored in a secure manner. As part of these priorities the Investigating Team needs to identify the evidence before they perform any tests/tasks on the suspect system.

The Investigating Team should keep track of any expenses incurred to investigate the suspected/declared incident and the number of hours spent investigating the incident.

If it is determined that **no data security incident has taken place**, the process ends and the incident is closed.

If it is determined that the incident is valid, notification to appropriate internal University staff shall occur.

IV. Internal Notice of Security Breach or Unauthorized Data Disclosure/Compromise to University Personnel

If the **incident is validated**, the Campus Incident Coordinator formerly declares the incident and notifies the following parties as appropriate:

- University CIO – Notify for all level 1 and 2 incidents. Level 3 and all other incident notification is at the judgment of the Incident Coordinator.
- Applicable Campus CIO(s) – Notify for all level 1 and 2 incidents. Level 3 and all other incident notification is at the judgment of the Incident Coordinator.
- Legal Counsel - Legal counsel should be notified at the onset of any incident investigation related to inappropriate use (e.g., access, storing or transmission of pornographic material, online stalking) or involving violation of law.

Approved: August 8, 2008

- Appropriate Campus Personnel based on incident handling contact lists.
- Law enforcement - Law enforcement should be notified immediately when the following incident types are detected: child pornography, online stalking, threatening/sexually harassing emails, counterfeiting, hate crimes, voyeurism, identity theft, fraud/theft and computer trespass.

If debit or credit card numbers are disclosed/compromised, the Treasurer's Office must be notified immediately.

V. External Notice of Security Breach or Unauthorized Data Disclosure/Comprise to Impacted Population

Based on the information compiled by the Investigating Team, who the "owner" of the data is (i.e., Does the University maintain or store, but does not own or license the compromised data; or does the University own or license the compromised data), the potential damage (safety, risk of identity theft or fraud) to impacted individuals and the University if no notification is made, and the potential damage to the University if a notification is made, the CIOs and University Legal Counsel will determine if, how, when and to whom an external notification will be sent.

A. External Notice Requirements for Data the University Maintains/Stores But Not Owner or Licensor

Massachusetts General Law 93H requires notification of the breach of security or unauthorized acquisition or use of compromised PII data to the owner or licensor if the University is NOT the owner or licensor.

Notification should be made in the most expedient time possible and without unreasonable delay. The notification shall include the date or approximate date of the incident and the nature thereof, and any steps the University has taken or plans to take relating to the incident.

This notification does not require the University to disclose confidential business information or trade secrets, nor does it require the University to provide notice to any resident that may have been affected by the breach of security or unauthorized acquisition or use. Notice to the impacted resident(s) is the responsibility of the data owner/licensor.

Such instances include:

- Debit or Credit card numbers- The Treasurer's Office must notify its Acquirer (i.e., the bank handling credit card transactions) immediately. The Acquirer or the Payment Brand (i.e., Card Company such as Visa, MasterCard, etc.) is responsible for notifying the customer.
- External agency for which the University is performing services – e.g., Medicare, Masshealth, etc.

B. External Notice Requirements for Data University Owns/Licenses Compromised Data

[Massachusetts General Law \(i.e., M.G.L.\) 93H](#) requires external notice when the University knows that:

- There has been breach of security including unauthorized acquisition or use (e.g., used for unauthorized reasons) of encrypted or unencrypted information that creates a substantial risk of identity theft or fraud OR
- Personal information, as defined in M.G.L. 93H and detailed below, of a resident of the Commonwealth has been acquired or used by an unauthorized person OR
- Personal information, as defined in M.G.L. 93H and detailed below, of a resident of the Commonwealth has been used for an unauthorized purposes.

Approved: August 8, 2008

There is no minimum number of impacted Residents so a breach of security or disclosure of information relating to a single resident may require notice under this law.

M.G.L. 93H defines personal information as an individual's first name or first initial, **and** last name in combination with one or more of the following data elements:

- Social Security Number,
- Driver's License Number
- State-Identification Card Number,
- Financial Account Number Or Credit Or Debit Card Number, **With Or Without Any Required Security Code, Access Code, Personally Identifiable Identification Number Or Password, That Would Permit Access To A Resident's Financial Account.**

External notice is made to the Attorney General and State Director of Consumer Affairs and Business Regulations (i.e., the Director) and the impacted individual(s). The notice provided to the attorney general and to the Director shall include, but is not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of Massachusetts residents affected by the incident at the time of notification, and any steps the University has taken or plans to take relating to the incident. Attachment 1 is the standard letter to be sent to the Attorney General. Attachment 2 is the standard letter to be sent to the impacted individual(s).

As required by M.G.L. 93H, the CIOs and University Legal Counsel will, upon request, also notify the consumer reporting agencies and state agencies identified by the Director. This would normally occur if the breach could result in possible identity theft or impact an individual's credit history.

The CIO or their designee will oversee the notification posting/mailing.

C. Notice of Security Breach or Unauthorized Data Disclosure/Compromise for Data Not Included In M.G.L. 93H

This Procedure is not intended to impose any further data security breach/compromise notice requirements other than those dictated in M.G.L. 93H however, there may be incidents involving PII or protected data for which Campuses determine external notification is prudent. This is especially true if multiple data elements are compromised which, when taken as a whole present a significant risk of safety, identity theft or fraud to impacted individuals. The need for such notices will be determined by the Campuses, in coordination with University legal counsel, and as authorized by the Campus CIO.

VI. Requirements of Notice Distribution and Content

A. Notice Format and Distribution Requirements

M.G.L. 93H requires that the external notice be as soon as practicable and without unreasonable delay unless a law enforcement agency determines that the sending of a notice may impede a criminal investigation. If law enforcement makes such a determination they must notify the attorney general, in writing, and inform the University. If notice is delayed due to such law enforcement request notice must be sent as soon as the law enforcement agency determines and informs the University that notification no longer poses a risk of impeding an investigation. Notice to the impacted individuals shall include:

- Written notice;
- Electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 (c) of Title 15 of the United States Code; and M.G.L. Chapter 110G; or
- Substitute notice, if the University demonstrates that the cost of providing written notice will exceed \$250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the University does not have sufficient contact information to provide notice.

Approved: August 8, 2008

“Substitute notice”, shall consist of all of the following:

- Electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents;
- Clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and
- Publication in or broadcast through media or medium that provides notice throughout the commonwealth.

B. Notice Content Requirements

M.G.L. 93H requires the following content be included in the breach of security or unauthorized data disclosure/compromise notification:

- The date or approximate date of the incident.
- Who was impacted and the timeframe of the incident (e.g., the computer contained information on individuals who applied to graduate school between 2000 and 2006).
- A description of the personally identifiable or protected information that was or may have been acquired or used.
- An indication of the likelihood that the personally identifiable or protected information was acquired or used.
- The individual’s right to obtain a police report, where applicable.
- Statement of University’s commitment to data security and privacy.
- Statement of actions being taken or planned to be taken (e.g., taking the steps necessary to safeguard the data; implementing controls to safeguard the data).
A list of resources that affected individuals could use to check for potential misuse of their information and how a consumer can request a security freeze.
- An email address and phone number of a suitable University representative with sufficient knowledge of the incident to be able to handle questions from affected individuals.

VII. University Notice Procedures

The University requires external notice as dictated by M.G.L. 93H, when the University knows that:

- There has been breach of security including unauthorized acquisition or use (e.g., used for unauthorized reasons) of encrypted or unencrypted information that creates a substantial risk of identity theft or fraud OR
- Personal information, as defined in M.G.L. 93H and detailed below, of a resident of the Commonwealth has been acquired or used by an unauthorized person OR
- Personal information, as defined in M.G.L. 93H and detailed below, of a resident of the Commonwealth has been used for an unauthorized purposes.

The University will notify impacted individual(s) via direct mailing unless circumstances require and laws allow a different method (e.g., substitute notice for high cost direct mailing notifications).

This notice should be made in the most expedient time possible and without unreasonable delay. Notices should be sent no more than two weeks after the incident is validated and determined to fall under M.G.L. 93H.

In order to maintain a consistent approach and legal response to security breaches and unauthorized data disclosures/compromise the University will use a standard notice letter for external notification to impacted individuals. Attachment 2 is the standard University of Massachusetts notice letter that shall be used to notify impacted individuals as required by M.G.L. 93H. Internet sites URL’s and phone numbers should be verified prior to the mailing of any security breach notice.

Approved: August 8, 2008

**Attachment 1
University of Massachusetts
Standards Notice to Attorney General – Compromise of Personally Identifiable Information**

Date
Attorney General *name*
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Dear Attorney General *name*:

Pursuant to G.L. CH. 93H, we are writing to notify you of *(a breach of security/an unauthorized access or use of personal information)* involving *(number)* Massachusetts resident(s).

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

(This paragraph should provide the date of the incident, a summary of the nature of the incident, a description of the categories of personal information involved in the incident, and whether the personal information that was the subject of the incident was in electronic or paper form).

NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED

(This paragraph should specify the number of affected individuals residing in Massachusetts whose personal information was the subject of the incident. This paragraph should also indicate that these Massachusetts residents have received or will shortly receive notice pursuant to G.L. CH. 93H, § 3(b) and should specify the manner in which Massachusetts residents have or will receive such notice. You should also include a copy of the notice sent to affected Massachusetts residents in your notification to the Attorney General).

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

(This paragraph should outline all the steps you have taken or plan to take relating to the incident including, without limitation, what you did when you discovered the incident; whether you have reported the incident to law enforcement; whether you have any evidence that the personal information has been used for fraudulent purposes; whether you intend to offer credit monitoring services to consumers; and what measures you have taken to ensure that similar incidents do not occur in the future.)

Finally, your letter should indicate whether you have provided similar notification to the Director of Consumer Affairs and Business Regulation. You should also include the name and contact information for the person whom the Office of the Attorney General may contact if we have any questions or need further information.

Sincerely,

Name
CIO
University of Massachusetts - *Campus*
Address

Approved: August 8, 2008

**Attachment 2
University of Massachusetts
Standard Notice**

Date
Name
Address

Dear (*insert name*)

This is to alert you that on *date*, a breach of *personally identifiable/protected data* occurred and some of our *students/staff* may have had their data compromised. An unauthorized individual could have accessed your *specify type of personally identifiable/protected data*. An investigation into this incident is ongoing.

At this time, *state situation (e.g., we have no evidence that an unauthorized person retrieved any personally identifiable/protected data, evidence indicates that an unauthorized person acquired personally identifiable/protected data) and if individual can obtain a copy of any related police report.*

The University takes its obligation to safeguard *personally identifiable/protected data* entrusted to it very seriously, and therefore, deem it necessary to bring this situation to your attention. Please monitor your email in the coming days for messages from the University. You may also want to avail yourself of the following web sites and telephone numbers that make available useful information on identity theft and consumer fraud:

- University Of Massachusetts Information Security And Awareness Web Site With FAQ
<http://www.massachusetts.edu/SecurityAwareness/securityawareness.html>
- Federal Trade Commission's Web Site On Identity Theft
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- Identify Theft Victim Checklist
<http://www.privacy.ca.gov/sheets/cis3english.pdf>
- Social Security Administration Fraud Line: 1-800-269-0271
<http://www.ssa.gov/oig/hotline/>
- Credit Bureau Numbers:
 - Equifax 1-800-525-6285
 - Experian 1-888-397-3742
 - Trans Union 1-800-680-7289
- Security Freeze Information
<http://www.consumersunion.org/pdf/security/securityMA.pdf>.

We deeply regret that your information may have been subject to unauthorized access and have taken remedial measures to ensure that this situation is not repeated. The University is committed to maintaining the privacy of *personally identifiable/protected data*. Please be assured that we are taking the steps necessary to safeguard the *personally identifiable/protected* information we maintain. In response to incidents like this one and the increasing number of internet-enabled computer attacks, the University is continually modifying its systems and practices to enhance the security of personally identifiable and protected data. We sincerely regret any inconvenience this incident presents to you. If you have any questions about this matter, please feel free to contact *name, email address and telephone number*.

Sincerely,

Name
CIO
University of Massachusetts - *Campus*
Address