Division of Graduate & Undergraduate Education

Policy on Protecting Personally Identifiable Information (PII) and Other Sensitive Data

Our Collective Responsibility

The Division of Graduate and Undergraduate (GUE) is committed to safeguarding the Personally Identifiable Information (PII) of MIT employees, students, parents and outside consultants or agencies with whom we work. It is important that each GUE employee understands what personally identifiable information is, where it resides, and how to secure, protect and/or destroy it. We all play an important role in protecting this sensitive data.

Definition of Personally Identifiable Information

Massachusetts state law defines personally identifiable information as an individual's first name or first initial and last name coupled with any of the following: Social Security Number, Bank Account Number, Debit Account Number, Credit Card Number, Driver's License or State Issued ID Numbers[1]. This information, if exposed, may put the identified individuals at risk of identity theft. Affected individuals must be notified when this information is exposed as a result of unauthorized use or a security breach.

Personally identifiable information can be found in many formats including paper hard copy, electronically or in any other media where it is collected, edited, manipulated, reviewed, reported, disposed of or stored.

Responsible Handling of Personally Identifiable Information

- ***Minimize the collection and storage of Personally Identifiable Information****. The actions of collecting, accessing, using, destroying, or disclosing personally identifiable information may only occur within the scope of responsibilities of your employment and be used for MIT business purposes only. If you discover that you have access to information outside the scope of your normal responsibilities, you must notify your supervisor immediately.*
- *You must exercise reasonable effort to* ***secure and protect from disclosure*** *any personally identifiable information downloaded to or stored on* ***any type of electronic device*** *(computer, smart phone, etc.) or peripheral (memory stick, flash drive, external drive, etc.)[2]. This includes using GUE-recommended tools and software such as encryption (PGP or FileVault), laptop cables and security tags, and IdentifyFinder. Personally identifiable information downloaded from GUE systems or shared with an external vendor must be transferred securely and deleted when no longer used.*

[1] Some offices have the responsibility to develop additional policies and procedures that pertain to special types of data (e.g., student biographical information and grades or staff salaries) or other laws (e.g., HIPPA and FERPA).

[2] Information on physically securing your electronic devices is available from IS&T Service Desk (servicedesk@mit.edu).

- *Reasonable efforts must also be made to protect personally identifiable information found in **paper documents or other non-computerized files** including physically locking cabinets or other areas containing these files, redaction, or secure file destruction using a cross-cut shredder or certified shredding service.*
- ***Your password** acts as a signature to access personally identifiable information and should be updated frequently[3]. **Under no circumstances should you share or provide your password to anyone at any time.** If you believe that the confidentiality of your password has been violated, you are requested to notify your supervisor immediately and ensure that your password is promptly changed.*
- ***Upon termination of employment,** the rights and access associated with your user ID and password will also be terminated. You must immediately return all documents and/or materials containing personally identifiable information to your supervisor. It is expected that following cessation or employment at MIT, you will continue to treat confidential information as confidential, and refrain from disclosing it or using it for any purpose.*

MIT policy requirements

- If you are handling sensitive data, it is your responsibility to adhere to the GUE policy above and to familiarize yourself with MIT Policies 11.0 and 13.0.
- GUE employees whose behavior is inconsistent with the **GUE Policy on Protecting Personally Identifiable Information (PII) and Other Sensitive Data** will be subject to MIT disciplinary action, up to and including termination.

By signing below, you acknowledge that you read this document and understand both the GUE policy and consequences for failing to adhere to it. This document will become part of your Personnel record.

Any questions related to this policy and the protection of sensitive data should be sent to Patrick Curtis, Sr Manager, IT Client Services, IS&T at pcurtis@mit.edu.

_____	_____	_____
Signature	*Printed Name*	*Date*

_____

GUE Department

[Please mail this signed document to: Y-Chie Primo, Bldg. 7-141]

[3] Information on protecting passwords is available from IS&T at http://ist.mit.edu/security/passwords.