

Office of Institutional Research and Policy Studies

Data Security Policy and Procedures

Prepared by Jennifer Brown, Director

Updated by Jim Castiola, Data Specialist

April 9, 2009

The University of Massachusetts has documents concerning Data and Computing Policies, Standards, and Procedures for non-IT Departments and for University Employees that we as a Department at UMass Boston and as employees of UMass Boston are under obligation to follow. These and other documents pertaining to the security of university data can be found at the following website:

<http://www.massachusetts.edu/policy/datacomputingpolicies.html>

The following document is a summary of policies and practices to be followed as we go about our work in the UMass Boston Office of Institutional Research and Policy Studies (OIRP). As employees with the responsibility of preparing and maintaining the official university reporting data (see our mission statement <http://www.oirp.umb.edu/>) we have access to, and frequently use data that includes Personally Identifiable Information (PII). Such information is classified as CONFIDENTIAL and obligates us as follows;

University departments and employees have a duty to ensure that personally identifiable and protected information created, collected, used, maintained, or disseminated in the process of providing services to the public and the University community are safeguarded against loss or theft. (University of Massachusetts Data and Computing Policies, Standards and Procedures Summary Non-IT University Departments, created November 29, 2007; UMass website)

Implementation of UMass Policies within OIRP.

Within OIRP we have Data Specialists who have security access through the UMass Information Technology System (UITS) to admissions, student, and human resources data necessary for the performance of their duties. These data users download data from UITS using Cognos software. The security of the transfer of this data depends on UITS security. Census data (which is produced every term) is sent FTP from UITS to the Registrar's Office. The security of these datasets is dependent on the security of the Registrar's Office server.

The downloaded data which contains PII data elements, becomes part of the university's historical reporting data, saved as SAS data sets and backed up onto server space provided by the university IT department.

At any given time, our data may contain PII and may reside on desktop computers within the department. In addition, the data created and maintained by the Data Specialists is often provided in the form of unit record data with PII to department Research Analysts (including the director) and Research Fellows, as well as to departments in other parts of

the university for their use (*see policy below concerning provision of individually identifiable information*).

In order to prevent unauthorized access to this data we take the following precautions:

- Password policy - set strong passwords for the administrator account on all office computers. Users' passwords are now the same as users' email passwords, the complexity of which depends directly on IT email security policy.
- Password protected screensavers – All screensavers are password protected and come into effect within 5 minutes of leaving the screen.
- Passwords are changed every 180 days, which is the policy set by university IT.
- Laptops are password protected. It is office policy not to save ANY data containing PII on any laptop computers. If PII data are saved on any of our laptops, the computer will have the data properly wiped off of the hard drive. Storage of any confidential data on departmental laptops is strongly discouraged within the office and prohibited when the laptop is outside the IR office.
- When transporting confidential data from the campus to other locations where university work must be conducted OIRP staff will use encrypted jump drives provided for that purpose by OIRP. These drives are also password protected.
- Data containing PII will not be delivered via e-mail. Transmission of PII data will be through the shared I drive (office internal transfers) and Xythos (external transfers). OIRP discourages constituents from sending data that contains PII to us. We make an effort to work with constituents to transfer data securely.
- No printed materials with PII (confidential information) should be left on or near public printers in the OIRP office area. Individuals printing PII should retrieve their printouts immediately after printing.
- As it is not possible to lock our desktop CPU's to the floors/walls, offices with hardware that contain confidential data must be locked when employees are out of the office.
- For desktop machines that are not in offices (machines located in the hall), data sets containing PII will not be stored on desktop computers once the work is completed and/or at the end of each work day. This data will be stored on the shared (I) or personal (M) drives, both of which are located on IT servers and are password protected.
- Paper reports or CD/DVD's that contain PII must be shredded after use or must be stored in a secure (locked) location.

Where to store data:

OIRP rents drive space from IT. Our space 'umbfs' (known to us as the I drive) exists on an IT server to which we have no physical access.

Access to the drive is protected by users' e-mail passwords. Therefore, the password to the I drive is dependent on the university's e-mail password policy. Only OIRP staff members have access to OIRP service space. It is IT's responsibility to ensure that the servers are secure and that the data on them are backed up regularly, including off-site backups.

OIRP staff also have individual access to personal work spaces on IT servers (our M drives). Only that individual has access to his/her space using UMB e-mail address as a username and their e-mail password.

Surplus OIRP computers (desk and laptop):

IT requires that the non-IT department (OIRP) is responsible for ensuring that all PII are erased from computer hard drives and unreadable before computers are surplus. Software available in OIRP will be used to comply with this regulation.

Policy regarding confidential data to other departments, and agencies:

- Providing individual employee and student data is not the responsibility of OIRP but of HR and the Registrar's office.
- There are some cases in which OIRP is permitted to provide individual student records to others on campus (to Dean's offices or Dean's designees or department heads for specific work purposes, i.e. collection of work load data, provision of listing of majors, student records for reporting purposes in cases in which the College/Department has some of the data necessary for reporting in their own records, not available to OIRP).
- State mandated requirements for unit record data are also permitted (HEIRS II is required by the Department of Higher Education). Data are uploaded to DHE through their secure website.
- Other circumstances include federally mandated surveys (e.g. NPSAS) or university approved surveys (e.g. NSSE, CIRP), which have received IRB approval at their own campus or at UMass Boston. The data are uploaded to the password protected site of the requesting agency.

Potential problem

HEIRS II data verification reports from the Board of Higher Education

The Department of Higher Education HEIRS II data submission system sends datasets containing PII to us via e-mail. This is a security risk. Recently, the DHE began blanking out social security numbers in the datasets that they send.