

University of Michigan-Flint

Information Security Incident Response Process

The University requires notification to any person whose personal private information has been breached. **Personal Private information** is defined as personal information such as social security number; driver's license number or non-driver identification card; bank account number, credit or debit card number (in combination with password or access code); grades and/or other similar entities. Private information does not include information publicly available from federal, state or local government records. A breach of private information can occur if someone successfully hacks into a database or obtains it via the loss or theft of a computer, laptop, personal digital assistant (PDA) device (such as a Blackberry, Palm Pilot), etc. that contains private information.








The best way to lessen the likelihood of having private information lost or stolen is to minimize storing this type of private information in your local system, especially on portable devices that can be misplaced or stolen easily. If you **must** store private information, always be sure that it is encrypted. As soon as you become aware that personal or private information has been compromised you must do the following.

First and foremost you need to immediately report the theft/loss to the Department of Public Safety (DPS) and Information Technology Services (ITS). You can reach DPS at 810-762-3335. After you report the incident to DPS please contact ITS at 810-762-3123. If the incident occurs after hours or on the weekend please ask the DPS dispatcher to contact the ITS Director.

DPS and ITS must know the nature of the personal and private information that has been compromised and will ask the following kind of questions.

- Did any media contain personal sensitive data?
- Did the media contain student or patient personal data?
- Were passwords stored on your computer?

Examples of Sensitive/Protected Information:

-  Passwords
-  Student Grades
-  Addresses
-  Birthdates
-  Social Security Numbers
-  Student ID Numbers
-  Other

If your laptop, phone, media, or documents contain any of the sensitive information listed above or other information viewed as sensitive or protected, please contact DPS and ITS IMMEDIATELY.

If you have passwords saved on your laptop or phone, please follow the steps below to change ALL of your passwords as soon as possible. If you have any questions or encounter any problems, please contact the ITS HelpDesk for assistance at 810-766-6804:

- LAN Password: <http://www.umflint.edu/helpdesk/articles/215>
- Kerberos Password: <http://www.umflint.edu/helpdesk/articles/68>
- SIS Pin: <http://www.umflint.edu/helpdesk/articles/218>
- Bank Accounts
- Credit Card Accounts
- Tax records
- Email Accounts (not university issued)
- Social Networking Sites

After speaking with ITS, if it is determined that your device contained PPI, the following process will apply.

It is important to remember that all security incidents are to be treated on a “need to know” basis. Do not discuss the incident with anyone who does not have a need to know.

The ITS Director will schedule a meeting as soon as possible with you, your immediate supervisor and that person’s supervisor to go over the next steps as follows:

1. You or someone in your department will need to try to re-create the list of people whose data was exposed. To do this you may need to work with the Administrative Information Management Systems department on campus which is centrally responsible for creating reports as they may be able to create these lists of people for you.
 - a. When you have a final tally of the number of people that should be receiving notification letters, you need to report this information to the ITS Director.
2. The University Relations Director will provide you with a template notification letter.
 - a. You will need to adapt this letter for the specific incident.
 - b. You will determine who will sign the letter. (Usually the chair, director or dean)
 - c. You will need to identify someone in your department who will take any initial phone calls from people who receive a notification letter. You should put their name and phone number on the letter.
 - d. The University Relations Director will provide the person taking the phone calls with a FAQ and additional instructions on how to handle any phone calls they may receive.
 - e. When you have completed the draft of the customized letter you should send it back to the University Relations Director for review.
3. Once the letter is approved you will need to print a copy to each person requiring notification on your official department letterhead, sign and mail.
 - a. You should send the letters out with a DO NOT FORWARD notice on the envelopes.
 - b. You will need to let the ITS Director know when all the letters have been sent.

Please see the following for more information

http://www.umflint.edu/its/lost_or_stolen_data.htm

<http://spg.umich.edu/pdf/601.25.pdf>

<http://spg.umich.edu/pdf/601.27.pdf>