Protocol for Incidents Involving Compromised Confidential Information August 2016

Step 1 – **Notify a person from the data breach contact list below**

- Information Technology (IT) to determine the nature of the exposure, systems involved, data elements involved, etc.
- Contacts:
  - Chick Blue, VP and Dean of Academic Services and IT; ext. 12035
  - Sue Korzinek, IT Director; ext. 12035
  - John Klein, Associate Director of Academic Systems; ext. 12777
  - Bill Fisher, Associate Director of Technical Services; ext. 12132
  - Ben Rapin, Web Manager; ext. 18014

Step 2 – **Meet with the response team**

- A committee comprised of representatives from the following offices will be convened immediately upon notification and confirmation from IT that confidential information entrusted to the university has been compromised:
  - Academic Services, Chick Blue; ext. 12035
  - IT, Sue Korzinek; ext. 12035
  - IT, John Klein; ext. 12777
  - IT, Bill Fisher; ext. 12132
  - Institutional Marketing, Ben Rapin; ext. 18014
  - Legal, Compliance & Risk Management, Pat Smith; ext. 12067
  - University Communications, Mary Eilleen Lyon; ext. 12221
  - Risk Management, Mick Doxey; ext. 12284
  - Public Safety, Renee Freeman; ext. 13255
  - Registrar, Sherril Soman; ext. 13327 or 12987
- Depending on the department or office(s) impacted by the potential breach of confidential information, the Senior Management Team member affiliated with that office or department and a representative from the office or department if not already listed above will be included in the committee.
- One of the team members will be assigned the responsibility of creating the Security Incident Response Report Form.

Step 3 – **Assess the data**

- Determine the relevance and scope of the exposure and come to a course of action. Determine whether internal and/or external communication of the incident is called for.
- Determine if corrective measures to the systems are warranted.

Step 4 – **Corrective Measures**

- Prepare letters and press releases.
  - Letters from the university to persons impacted by the breach will be prepared using a generic template previously drafted by the committee that will be modified to fit the situation at hand. A news release will be prepared and timed to be released to coincide with the receipt of notification letters. Notification letters will be sent by email or first class mail as soon as possible using addresses obtained from the most up to date university sources available.

- Prepare response script and phone contact.
    - A previously dedicated phone number – (616) 331-7000 – will need to be activated by IT and this number will be included on the notification letter as the appropriate number to call with questions. The phone number will be staffed by permanent or temporary staff who will be provided a detailed question and answer script to address incoming phone calls.
- The committee will evaluate if state or federal law requires any additional steps be taken in response to the incident and whether the credit reporting agencies are to be notified.

Step 5 – **Complete and review Security Incident Response Form**

- Review all aspects of the response and update/refine as needed.
- Complete and review Security Incident Response Form