UNIVERSITY OF LOUISIANA AT MONROE
POLICIES AND PROCEDURES MEMORANDUM

Title: **Computing Systems Security Breach policy**
Effective Date: **10/29/2014**
Update Responsibility: **Computing Center**
Update Date: **12/02/2014**
Cancellation Date: **NONE**
Application: **ULM Employees and Students**

In the event of a known or suspected security breach to any University based computer system, it is expected that the Computing Center be contacted immediately with the details of the matter.

Security breaches can initiate through a number of paths and are most often triggered by failure to maintain privacy of login and password information. The utmost importance of protection is for data of the format containing Personally Identifiable Information (PII).

The following are summaries of potential threats with perceived severity to ULM operations:

1. Virus/spyware -- Would need to identify types of infections and identify if they compromised security (ie, sent files to external address, Trojans, encrypting/destroying files). If it does, then it would be identified as a security breach. Since these are found outside of the TrendMicro AntiVirus protection system, this would require the Helpdesk/IT Staff to track what is found during other scans and someone has to research each that are found.

2. Physical breach -- Procedures for a ULM computer that has been stolen or physically tampered with, such as a student breaking into an office and accessing information. Disgruntled employees would also fall into this category. In this situation, University Police are contacted immediately to file a criminal case. The primary occupant of the device(s) are contacted and account access should be reviewed as to mandate account lockdown if needed. Then IT Staff can engage to assist UPD in investigations.

3. Unsecure transfers or publicly accessible PII info -- Any unsecure transfers of PII data should be treated as a security breach. Also any PII files that may be put on public webpages would be a security breach. Any PII files that are stored outside of ULM's control, using personal email account or Google drive, skydrive, icloud, dropbox, etc. would also be considered a security breach. ***Also, if an employee takes home PII files and stores it on their home computer, this would also be suspect. Would need research as how to identify.***

4. Desktops without recent patches -- Any desktop that isn't patched with the latest patches, Microsoft or Mac, could be pron to a security breach, especially if an identified vulnerability hasn't been patched. Would need software to track and report it. Vulnerability scans will assist in monitoring this as well.

5. Third party breach -- Any 3rd party that has ULM PII data that has a security breach (or access to any of our systems) would trigger our security breach response.

6. Email phishing -- From time to time, Phishing or SPAM email is received to one or more ULM email recipients. Most SPAM is blocked at our Barracuda Email service, but a small percentage of messages leak through the known database or modified filters. ULM patrons have fallen victim to some of these phishing email in the past which ask through some "threatening" type of dialog to provide the users username/password. In the event the user does fall victim before IT resources have been able to identify the suspect message, a victim may provide this private information. The response may be in the form of a simple email response to the suspect or by visiting the suspect's published website.

For any of the above threats, the following actions and review processes may also be engaged:

As soon as the Computing Center is made aware of the phishing email or other breach, we immediately begin to review firewall and email server logs for abusive activity. If the user has in any way fallen victim, we will contact them immediately to change their account passwords or lock the account until such time we are able to communicate with the victim either in person or by phone. Measures to monitor inappropriate account activity continues by monitoring outbound bulk SPAM email attempts via hijacked access.

In the event that a suspect has gained access to an account, we identify that access via logs and then block the associated IP network range through immediate firewall filtering. The hijacked account is immediately locked and all sessions terminated. The suspect user is contacted to determine the exact nature of the process. Review of contents in fileshares and email are done to determine what was stored in the user's account. The appropriate department head and executive vice president are also contacted to alert them of this issue. Once reviewed thoroughly, it may be determined that PII could have been compromised by the suspected hijacker. If so, the compromised data is reviewed for target parties and following the state code at http://www.legis.la.gov/legis/Law.aspx?p=y&d=322027 and http://doa.louisiana.gov/osr/lac/16v01/16v01.doc, the respective department is obligated to inform outside parties and the Attorney General of the related security breach along with the details of the incident.

Anytime a mass delivery email is received, we make attempts to notify the ULM Employee and Student population of the incident in hopes to remind our user base to always be on guard of SPAM or other attempts to acquire account/password information.