

The University of Mary Hardin-Baylor

Date: December 2008

SUBJECT: SECURITY INCIDENTS

The purpose of The University of Mary Hardin-Baylor's policy on security incidents is to minimize both the frequency and the severity of information security incidents within the University environment. All *users* are responsible for and must maintain their University computing devices and data in as safe a manner as is reasonably possible. In the event of an incident, the standards outlined in this document as well as the related procedures must be followed.

STANDARDS

Compromises in security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems on campus. Incidents can be accidental incursions or deliberate attempts to break into systems and can be benign to malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of individuals, *sensitive information* and the campus as a whole.

The accelerated pace of technological change and concurrent reliance on electronic information systems has greatly increased both the potential exposure of *sensitive information* to the world at large via electronic means and the motivation of some to exploit computing devices, computing infrastructure and software either for gain or to cause organizational difficulties. Governmental authorities, regulatory bodies and standards organizations have recognized this new reality and responded with laws, regulations and other measures to motivate organizations to take the steps necessary to minimize or prevent security incidents before they occur.

For the purposes of this policy a "Security Incident" is any accidental or malicious act with the potential to

- result in misappropriation or disclosure of sensitive information,
- affect the functionality of the information technology infrastructure of the University,
- provide for unauthorized access to university resources or information,
- allow University information technology resources to be used to launch attacks against either other internal resources or the resources and information of other individuals or organizations.

This document outlines the standards and process individuals should follow to report potentially serious security incidents. University staff members whose duties include managing computing and communications systems have even greater responsibilities. This document outlines their responsibilities in securing systems, monitoring and reporting IT security incidents, and assisting individuals, administrators, and other IT staff to resolve security problems.

Administrative standards:

Dealing with Viruses, Worms and other common "Malicious" Software

- Individuals and information technology support professionals are not required to report IT security incidents involving viruses, worms, and other common malicious software *if self contained and completely removed by anti-virus, anti-spyware or other software*. If, in the judgment of technical support personnel, the software could pose a risk to university data and was not successfully removed the incident must be reported. Please follow the standards in the next section, "Reporting and Responding to IT Security Incidents."
- Because malicious software can reduce the functionality or otherwise affect the campus computing and communication environment, individuals and information technology support professionals are expected to:
 - prevent computer equipment under their control from being infected with malicious software by the use of preventive software and monitoring (see the "Protection from Malicious Software" policy and standards), and
 - take immediate action to prevent the spread of any acquired infections from any computers under their control.
- Assistance is available from UMHB InfoTech.

Reporting and Responding to IT Security Incidents

- Individuals
 - Should attempt to stop any further damage from an IT security incident by powering-down the computer and disconnecting it from the campus network.
 - Report IT security incidents to InfoTech at infotech@umhb.edu. InfoTech will help you assess the problem and determine how to proceed.
 - If the incident has potentially serious consequences and requires immediate attention, individuals should report the incident to the InfoTech Help Desk at 254-295-4658. If your call goes to voicemail, please follow the directions on the voicemail to have your message marked "emergency."
 - Following the report, individuals should comply with directions provided by IT support staff to repair the system, restore service, and preserve evidence of the incident.
 - No retaliatory action should be taken against a system or person believed to have been involved in the IT security incident. All response actions

should be guided by the IT Security policy and all other applicable university policies.

- IT Support Professionals

Department, university, or unit information technology support professionals have additional responsibilities for IT security incident handling and reporting for both the systems they manage personally for their units and the systems of users within their units. In the case of an IT security incident, IT support staff should:

- Respond quickly to reports from individuals.
- Take immediate action to stop the incident from continuing or recurring.
- Report IT security incidents the Information Security Officer. They will help you assess the problem and determine how to proceed.
- If the incident has potentially serious consequences and requires immediate attention, individuals should report the incident to the IT Help Desk at 254-295-4658. If your call goes to voicemail, please follow the directions on the voicemail to have your message marked “emergency.”
- Notify the appropriate university or department administrator that an incident has occurred and that InfoTech has been contacted.
- Refrain from discussing the incident with others until a response plan has been formulated.
- Follow InfoTech guidance to repair the system, restore service, and preserve evidence of the incident.