Collection of Personal Contact Data for Emergency Notification System

Date Instituted: June 3, 2009
Last Revised: June 3, 2009

Description

1. Overview and Statement

Marshall University has contracted with an outside vendor to provide the University community with emergency notification services in times of emergency. These emergency notices will be broadcast by voice mail, e-mail and text messages. This system will only be used in the case of an emergency in which the safety and well being of our Marshall University community is threatened or the normal operations of the campus are disrupted. Therefore it is important that as many members of the campus community as possible participate in this system. The University also respects the right to privacy of all its students and employees. Therefore, as part of the emergency notification system, the University will defer to anyone's decision not to have personal contact information, beyond their University e-mail address, included in the system.

2. Procedure

Marshall University will, as a matter of course, collect and maintain contact information (including, but not limited to, e-mail address and cell phone number) for all current students and employees. Student information will be collected each year as part of registration. Employee information will be collected through the Banner Self Service system. Information on both students and employees will be stored in the Banner system and uploaded by the University into the emergency notification system. The University will upload whatever contact information it has on students and employees, but it is the responsibility of each person to manage their own contact information and preferences through the vendor's Web site. Regular updates from the Banner system will be scheduled in order to add new students and employees, as well as to delete those who have left the University.

Individuals can manage their contact preferences through the myMU university portal and can choose to remove contact information for personal phone or e-mail accounts. However, the e-mail address for each individual that is provided by the University will always remain in the system. If no reply is made, then the individual will default into the emergency notification system with whatever contact information has been provided by the University. Marshall University will maintain a link on its Web site with information on the emergency notification system and individuals will be able to manage their contact information in the system at any time through this site.

3. Responsible Offices

University Communications will oversee the emergency notification system and the communication processes associated with notification. The Office of Information Technology will be responsible for managing the transfer of data from Banner to the emergency notification system and for maintaining the University's emergency notification Web site.

4. Responsible Executive

The Senior Vice President for Communication/Chief of Staff, Senior Vice President for Information Technology/CIO and the Chief Information Security Officer will be responsible individuals for the overall administration of the emergency notification system. The Directors of Public Safety and Health and Safety, Dean of Students and the Director of Residence Services will work as communication conduits for the constituent areas.

MU's Commitment to Privacy and Confidentiality

Marshall University is committed to protecting the privacy and confidentiality of personal information provided to the campus by faculty, staff, and students. Therefore, all the data provided to MU Alert as part of the campus Emergency Notification System will be stored in secure electronic systems located within the campus data center.

Partnership with Everbridge to Ensure Availability of Emergency Messaging

To ensure MU Alert will be able to communicate with the campus during an emergency, MU Alert will transmit emergency notification information to its partner, Everbridge (please visit www.everbridge.com for additional information). Everbridge will store this data in two remote (non-campus) sites to ensure the availability of emergency messaging functionality during a crisis.

Everbridge Commitment to Privacy and Confidentiality

Everbridge is required to provide a secure environment for MU data, using appropriate technologies to safeguard campus information. In addition, as part of MU's agreement with the vendor, Everbridge agrees never to sell any MU information to another vendor / organization. In the event MU terminates its relationship with the Everbridge the vendor is required to purge MU's information from its database.