MARSHALL UNIVERSITY INFORMATION TECHNOLOGY COUNCIL

GUIDELINE ITG- 3

Collection of Personal Contact Data for Emergency Notification System

1. General Information:

1.1. Scope:
Marshall University.

1.2. Authority:
Marshall University Information Technology Council

1.3. Effective Date:
June 3, 2009

1.4. Revision Date:
August 19, 2019

1.5. Controlling over:
Marshall University

2. Overview and Statement

Marshall University has contracted with an outside service provider to deliver emergency notification services to the University community 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.

3. Guidelines

Marshall University's Emergency Notification System is authorized to collect and maintain contact information (including, but not limited to, e-mail address and cell phone number) for all current students, employees and affiliates. Subscriber information will be collected each year as part of a self-service registration process. Subscriber information will be entered directly into the emergency management system with a local export copy maintained for backup purposes. It is the responsibility of each person to manage their own contact information and preferences through the designated MU Alert registration web page. Marshall University will periodically review and purge contact information for those subscribers 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 official Marshall University e-mail address will be the default contact as long as the subscriber is a current student or employee. 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.

4. 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 exchange of data between on-campus systems and the emergency notification system. University Communications will manage the University's emergency notification web site.

5. Responsible Executive

The Senior Vice President for Communication and Marketing, the Chief Information Officer 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.

5.1. MU's Commitment to Privacy and Confidentiality

Marshall University is committed to protecting the privacy and confidentiality of personal information provided to the emergency notification system by faculty, staff, and students. Data provided to the MU Alert system will be protected according to applicable University data protection standards.

5.2. Partnership with External Service Provider to Ensure Availability of Emergency Messaging

To ensure MU Alert will be able to communicate with the campus during an emergency, the University will transmit emergency notification information to its external service provider. The Service Provider is authorized to store this data in two remote (non-campus) sites to ensure the availability of emergency notification services during a crisis.

5.3. Service Provider Commitment to Privacy and Confidentiality

University service providers are 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 provider, they agree to never to sell any MU information to another vendor / organization. In the event MU terminates its relationship with the service provider, they are required to purge MU's information from their databases.