EMERGENCY NOTIFICATION

Policy Number: G.01.01

SCOPE

All staff, faculty, students.

PURPOSE

This policy describes the guidelines for use of the Connect-ED Notification System. These guidelines are intended to provide the University with procedures and instructions for the use of the Connect-ED Notification System.

DEFINITIONS

Crisis Team
A small group of administrators who are authorized to report emergency events through the Emergency Notification System. Connect-ED® requires the use of the term "Crisis Team" or the dial-in ENS will not work.

Emergency events
Events defined by the Institution Emergency Response Plan. Examples include:
- Natural Disasters (Tornadoes, Floods, Thunderstorms, Winter Storms and Extreme Cold, Extreme Heat)
- Aircraft Accidents
- Biological, Chemical, Nuclear, or Radiation Spills and Threats
- Explosions, Fires, Laboratory Emergencies
- Bomb Threats or other imminent violent threats

ENS
Acronym for the Emergency Notification System

Emergency Response Team
A team whose function is to deal with critical or potentially dangerous situations.

Recipient data
Data defined as data provided to the Connect-ED® application for use in notifications. This includes multiple phone numbers and email addresses. PeopleSoft data is the source system of record for this information.

Recipient groups
Groups are defined as a function provided by Connect-ED® which allows for segmentation of Recipients to meet individual campus needs.

Recipient type
Type is defined as a function provided by Connect-ED® which allows for categorization of Recipients to meet individual campus needs.
Routine emergencies
Routine emergencies are defined as emergencies impacting an individual or small group of individuals. Examples include: medical emergencies, contact with a hazardous material, and individual criminal activity (theft, assault or other violent act). The use of this system for routine emergencies reduces its effectiveness in a real emergency; therefore this system will used for emergency use only.

Routine utility failures
Routine utility failures are defined as a failure of a utility service impacting a specific building or small area of the campus. Examples include: localized fire alarm, building power outage, elevator failure, plumbing or steam line failure. The use of this system for routine utility failures reduces its effectiveness in a real emergency; therefore this system will used for emergency use only.

POLICY/PROCEDURE

1. Appropriate Use of Connect-ED® Emergency Notification System (ENS)

   The Connect-ED® service is used to transmit brief urgent messages to a large segment of UST’s population as quickly as possible. The use of this system during a declared campus state of emergency must be authorized by a member of the Crisis Team.

   It is strongly recommended that this system be used only for unplanned Emergency events which have the potential to affect the entire campus. The use of this system for planned events, Routine emergencies and Routine utility failures reduces its effectiveness in a real emergency. Use of this system for specific building closures which impact a subset of the campus is also discouraged.

   Emergency notifications may include but are not limited to:
   - Bomb threats or other imminent violent threats
   - Fire alarms, natural gas leaks and hazardous spills affecting the entire campus
   - Building evacuations and lock downs affecting the entire campus
   - Biological or pandemic emergency notifications
   - Natural disasters
   - Power outages and utility failures resulting in an imminent threat
   - Campus closure due to declared civil emergency
   - Severe Weather

2. Access Control

   A. Crisis Team

       The Crisis Team is defined as a small group of administrators who are authorized to report emergency events through the Emergency Notification System. The primary and backups are as follows:

<table>
<thead>
<tr>
<th>Director of Marketing Communications</th>
<th>Primary</th>
</tr>
</thead>
</table>
EMERGENCY NOTIFICATION  POLICY NUMBER: G.01.01

University of St. Thomas Policies

<table>
<thead>
<tr>
<th>President</th>
<th>Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President of Student Affairs</td>
<td>Backup</td>
</tr>
<tr>
<td>Vice President of Information Technology</td>
<td>Backup</td>
</tr>
<tr>
<td>Chief of Security</td>
<td>Backup</td>
</tr>
</tbody>
</table>

The Director of Administrative Computing and Institutional Research and Director of Central Computer Services are responsible for the Crisis Teams’ credentials/access to the system.

B. Training Requirements

The Crisis Team will attend training twice a year prior to the start of the fall and spring semesters. During training each member will practice sending messages to the team members.

3. Connect-ED® Recipient Data

The Office of Administrative Computing and Institutional Research will provide both initial load and nightly updates of Recipient data. PeopleSoft has been selected as the source system of record for Recipient data for Connect-ED®.

A. Recipients

Recipients are defined as currently employed faculty and staff and currently enrolled students.

B. Recipients Types

The current Recipient types defined in Connect-ED® are:

- All
- Student
- Faculty (Full and Part-time)
- Staff (Full and Part-time)

C. Recipients Groups

The recipient groups are defined as a specific subset of recipients of any type. The current recipient groups defined in Connect-ED® are:

- Group 1: Crisis Team
  The Crisis Team recipients will include the following people: President, Special Assistant to the President and Vice President for Information Technology, Vice President for Enrollment Management and Marketing, Director of Marketing Communications, and Director of Campus Security.

- Group 2: Emergency Response Team (ERT)
  The ERT recipients will include the following people: President, Vice President for Academic Affairs, Special Assistant to the President and Vice President for Information Technology, Vice President for Student Affairs, Vice President for...
D. Updating Recipient Data - DATA MAPPING

Below are the data elements mapped from the PeopleSoft database to Connect-ED.

<table>
<thead>
<tr>
<th>Connect-ED Data Elements</th>
<th>PeopleSoft Data Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Students</td>
</tr>
<tr>
<td>HomePhone</td>
<td>HOME</td>
</tr>
<tr>
<td>WorkPhone</td>
<td>BUSN</td>
</tr>
<tr>
<td>MobilePhone</td>
<td>CELL</td>
</tr>
<tr>
<td>HomeAlternate</td>
<td>OTHER</td>
</tr>
<tr>
<td>WorkAlternate</td>
<td>N/A</td>
</tr>
<tr>
<td>MobileAlternate</td>
<td>N/A</td>
</tr>
<tr>
<td>PrimaryPhone</td>
<td>HOME</td>
</tr>
<tr>
<td>TTYPhone</td>
<td>TTY</td>
</tr>
<tr>
<td>EmailAddress</td>
<td>CAMPUS</td>
</tr>
<tr>
<td>EmailAddressAlt</td>
<td>HOME</td>
</tr>
<tr>
<td>SMSAddress</td>
<td>TXT</td>
</tr>
</tbody>
</table>

E. Opt Out Process

Opt Out functionality is NOT currently available to recipients at this time due to the nature of emergency notifications.


A. Planning Emergency Notification

- Prepare emergency notifications in advance in writing only.
- It is NOT recommended that emergency messages be pre-recorded in the Connect-ED application in advance; as it is very, very easy to accidentally send these messages.
- Train Crisis Team two times per year.
- Conduct regular tests of the Emergency Notification System.
- Publish information about the Emergency Notification System on [www.stthom.edu](http://www.stthom.edu) and myStThom and update as appropriate.
B. Sending Emergency Notification Message
   - Only initiate the Emergency Notification System based on requests from authorized personnel.
   - Call and/or notify as many of Crisis Team together.
   - Call a meeting with Emergency Response Team, if necessary.
   - There are 2 mechanisms for sending out emergency notifications: web-based and phone-based. Connect-ED® users can immediately evacuate if required and initiate the message via phone. If sent by phone, please note recipients will receive the message on their phones only. Email and SMS/text messages will not be sent.

C. Evaluating Emergency Results
   - Evaluate notification results after emergency notification.
   - Be prepared for feedback both positive and negative.
   - Have a Recipient Data Update Process in place and communicate it within your Emergency Results Email.
   - Share results with Senior Administration, Crisis Team and Emergency Response Team.
   - Communicate to all recipients of the emergency notification after evaluation of the results.
D. Emergency Response Flow Chart For Triggering the Emergency Response System

Emergency Incident: Life Threatening to the larger community. Examples: Person in extreme violent distress, Bomb Threat, Flood, Person with weapon on campus, Severe weather

Critical Incident: Non-Life Threatening to the larger community. Examples: Suicide attempt/hoat, Injured person, Person intoxicated, Person in emotional distress, Campus Death, Assault

Incident Occurs

Emergency Incident

Call 911

Call UST Security

Security sends ENS Message to Crisis Team

Crisis Team: Those with the permission to send an ENS Message to the Entire Campus.

Crisis Team Conference Call

Use ENS

Assemble Needed Emergency Response Team Members

Don’t Use ENS

Assemble Needed Emergency Response Team Members

Note: For critical yet non-immediate threats (such as severe weather), the process will begin at this (*) stage and initiated by one of the Crisis Team Members

APPROVED: Dr. Robert Ivany

Date of Original Formation: 9/1/2010

Revision Number:

Revision Date:

Effective Date:

EMEGENCY NOTIFICATION

POLICY NUMBER: G.01.01