**Information Technology – Emergency Management Best Practices**  
**A Path to Maturity**

**Background**

Information Technology (IT) and Emergency Management (EM) intersections in institutions of higher education (IHE) are critical and at times fragile. The dependence of EM on IT capabilities has increased as the field and expectations on IHE to be responsive to emergency situations have matured. The role of information technology, its use, and its importance in institutional protection, prevention, preparedness, response, and recovery strategies, however, has not been fully explored or clearly defined. A symbiotic and effective working relationship between IT and EM can yield a more prepared and resilient university. IT is an essential component of all IHE and is may only be eclipsed by power, air conditioning, and food, as the most important ‘utility’ in contemporary society and arguably the most essential function for education and business. As such, institutions must ensure that IT and EM are appropriately integrated and orchestrated in manners that produce the greatest potential for IHE to respond and recover from emergency situations.

**Goal**

The purpose of this project is to produce a road map and corresponding resources that can assist IHE IT and EM units in developing a robust and comprehensive approach to preparing for, responding to, and recovery from emergency situations. This project aims to provide a scalable, generic, and at times detailed overview of the partnership between IT and EM in terms of functions, activities, and responsibilities.

The foundation of this project is a structured template that can be applied to IHE, regardless of size, complexity, or classification (i.e., public, private, or community college). This solution seeks to address information technology’s role in all phases of emergency management and its importance in routine or unforeseen disruptions to institutional operations.

**Method**

To satisfy the goal, this paper sets out strategies and resources as suggested by comments and discussions recorded during the November 7th, 2013 SURA IT Committee meeting in Washington D.C. Additionally, it is the Committee’s goal to provide a repository of resources and best practices accessible to all members of SURA that can facilitate the development of an IT and EM partnership.

**A. Forum to share best practices:** This forum should be a virtual on-line forum replete with a repository of existing artifacts of best practices and a discussion board through which members can post questions, suggestions, or provide commentary. The forum can be hosted and managed by one of the SURA IT Member institutions. Ownership and/or management can be assigned on a revolving schedule determined by the Committee. A designated forum administrator appointed by the SURA IT Committee should moderate the contributions and postings.

**B. Information Technology/Emergency Management Path to Maturity Checklist:** This checklist will serve as the overarching document that guides the architecture of the on-line forum and organization of best practices. The ‘Path to Maturity’ document will provide step-by-step guidance on how to establish an effective partnership between Information Technology and Emergency Management and a reference to the best practices that have been developed and are recommended for each step. The ‘Path to Maturity’ document will consist of a checklist of action items arranged in a sequential and progressive order to facilitate the development of a mature information technology/emergency management partnership. This ‘Path to Maturity’ constitutes the major milestones in progressing towards a contemporary and effective emergency management program that meets Department of Education guidelines.
The Checklist

1. Getting Started
   a. Establish routine meetings with your institution’s office of emergency management.
   b. Create a list of contact numbers (and alternates) for IT personnel and departments.
   c. Ensure that Information Technology is reliably represented in the institution’s Emergency

2. Protection
   a. Evaluate website as well as internal, external and local (i.e., emergency management
      crisis center) communications systems to ensure they have the capacity to manage
      increased volume during a crisis.
   b. Create a secondary website with limited functionality designed to be used in the event of
      an emergency. The secondary site will be used to communicate essential emergency
      information to a significantly increased number of users.
   c. Consider alternative methods for providing application reliability and data protection and
      systems access in the event of an emergency circumstance.
   d. Identify vital records and consider the role of an enterprise document management
      solution in supporting continuity of operations.
   e. Collaborate on the requirements, process for evaluation and selection and implementation
      and on-going management of an emergency notification system.
   f. Jointly develop institutional security strategies, with specific attention paid to the
      implementation and use of surveillance equipment and access controls.

3. Prevention
   a. Identity lead roles for IT and Emergency Management and support the review of existing
      systems’ strengths and weaknesses, including those applications, infrastructure, or
      employee training dependencies informing and institutional strategy and risk mitigation.
   b. Prioritize and implement identified infrastructure improvements, training, software
      upgrades, or other procedures to mitigate risk.
   c. Ensure that the Emergency Operations Center is equipped with the necessary IT
      resources.

4. Preparedness
   a. Identify critical business functions.
   b. Map emergency plans and capabilities to critical business functions.
   c. Document critical business functions and alternate procedures in the institutions COOP.
   d. Enlist the office of emergency management to help develop a formal emergency response
      plan for IT.
   e. Conduct and document cross-training exercises for employees on critical functions.
   f. Test and exercise critical functions on a routine basis. Document gaps and adjust plans
      based on process improvement needs.
   g. Participate in Emergency Operations Center trainings and exercises.
   h. Establish Disaster Recovery Site procedures and test them on a periodic basis. Develop a
      Continuity of Operations Plan (COOP) for IT.
   i. Participate in the establishment of recovery time objectives for functions dependent upon
      IT systems.

5. Response
   a. Participate in Emergency Operations Center activities.
   b. Monitor IT infrastructure and provide routine updates to the Emergency Operations
      Center.
   c. Utilize analytics to glean a clearer picture of response efforts, utilization of IT resources.
   d. Engage external partners/vendors as necessary to assist in response procedures.
e. Establish IT Task Forces that can be deployed in an emergency to troubleshoot or repair IT systems.

6. Recovery
   a. Engage external partners/vendors as necessary to assist in recovery procedures.
   b. Assist units in establishing alternate work locations in the event that work spaces are uninhabitable due on going response activities, damage, or

C. Existing Documents or Documented Best Practices: SURA IT Committee members and institutions are encouraged to share and post examples, practices, policies, procedures, and best practices that have contributed to a strong collaboration between their Information Technology units and office of emergency management.

D. Contacts for Additional Information or Guidance: The forum provides contact information for emergency managers at SURA IT Committee institutions. This is intended to provide member institutions opportunity to contact and discuss the resources and concepts presented on the on-line forum. Volunteer emergency managers and information technology professionals from SURA IT Committee will moderate the forum. ‘On-call’ staff will rotate through alternating two-year terms and provide general information or additional guidance as to resources and best practices available in the forum.

E. IT/Emergency Management Blog: Create a blog that is either free standing or embedded within the recommended website that features monthly or bimonthly contributions of SURA IT committee institutions/members that highlights emerging trends, current projects, and examples of successful IT/EM partnerships.

F. Webinar: Annual or semi-annual webinars hosted by SURA IT Committee members that provide an overview of the SURA IT Committee IT/EM on line forum, best practices, or emerging trends in IT/EM partnerships. This webinar can be made available to all SURA institutions.