The priorities that the University established when the University was preparing for potential problems related to Y2K remain applicable today.

**PRIORITY 1:** Health and safety of faculty, staff, students, patients, contractors, renters, and any other people on University premises.

**PRIORITY 2:** Delivery of health care and patient services: admissions, diagnostic tests, outpatient appointments, surgery and other procedures, patient records availability, etc.

**PRIORITY 3:** Continuation and maintenance of research specimens, animals, biomedical specimens, research archives.

**PRIORITY 4:** Delivery of teaching/learning process and student-related services such as registration, faculty assignments, classroom scheduling, drop/add, financial aid services, government reports, grades, admissions, and housing.

**PRIORITY 5:** Security and preservation of University facilities and equipment.

**PRIORITY 6:** Maintenance of support for community/University partnerships. In its business continuity plan, each unit should consider these priority functions and describe its business continuity measures to ensure that the processes supporting these functions continue to work.

We are committed to supporting the University with objective assurance and advisory services that assess risk and promote a strong internal control environment.

**Wolverine Tower, 3rd Floor**  
3003 South State Street  
Ann Arbor, MI 48109-1286  
audits.umich.edu

**ADDITIONAL RESOURCES:**

  spg.umich.edu/pdf/601.12.pdf

- **ITS Disaster Recovery and Business Continuity Planning Template and related documents:**  
  www.mais.umich.edu/methodology/disaster-recovery-business-continuity/templates.html

- **Emergency Management, Business Continuity, and Disaster Recovery Planning:**  
  www.mais.umich.edu/projects/drbc_methodology.html

- **U-M OSEH Department:**  
  www.oseh.umich.edu

- **U-M Emergency Preparedness:**  
  umemergencypreparedness.umich.edu/about

- **Emergency Procedures Flipcharts:**  
  umemergencypreparedness.umich.edu/epp/flipchart.shtml

- **UM-F EHS Department:**  
  umflint.edu/ehs
WHY?

Standard Practice Guide Section 601.12, Institutional Data Resource Management Policy states:

“Contingency plans will be developed and implemented. Disaster Recovery/Business Continuity plans and other methods of responding to an emergency or other occurrences of damage to systems containing institutional data, including electronic protected health information (ePHI), will be developed, implemented, and maintained. These contingency plans shall include, but are not limited to, data backup, disaster recovery, and emergency mode operations procedures. These plans will also address testing of and revision to disaster recovery/business continuity procedures and a criticality analysis.”

“Disasters have affected university and college campuses with disturbing frequency, sometimes causing death and injury, but always imposing monetary losses and disruption of the institution’s teaching, research, and public service. Damage to buildings and infrastructure and interruption to the institutional mission result in significant losses that can be measured by faculty and student departures, decreases in research funding, and increases in insurance premiums. These losses could have been substantially reduced or eliminated through comprehensive pre-disaster planning and mitigation actions.”

From: Federal Emergency Management Agency (FEMA), Building a Disaster-Resistant University

WHAT?

Commitment by top-level officials
Management shows support to properly prepare, maintain, and practice a continuity plan. Adequate resources, people, and budgeted funds are assigned to the continuity plan and process.

Risk assessment and mitigation
Potential risks due to threats such as fire, flood, etc., are identified along with the probability and potential impact to the University and the units. The continuity plan incorporates data collected from the “All hazards” planning.

University impact analysis
Identifies critical processes that are integral to keeping the University functioning in a disaster and to determine how soon these integral processes should be recovered following a disaster.

Recovery and continuity strategies
Addresses actual steps, people and resources required to recover a critical University process.

Disaster recovery for IT
Supports restoring operations critical to the resumption of University business (identified by the Impact analysis), including regaining access to data (i.e., records, hardware, software), communications (i.e., e-mail, phone), workspace, and other business processes after a disaster.

Deploy, verify, and maintain
Capabilities and documentation are kept current with changes to the environment in order to remain effective and align with University priorities. Scheduled drills serve as training and ensure effectiveness.