



SPACE INSTITUTE

UT Space Institute Policy: IT0128-SI –Contingency Planning	
Version: 1	Effective Date: 09/18/2019

Objective

Per System-Wide policy IT0128, the University of Tennessee Space Institute (UTSI) is tasked with establishing a Contingency Planning (CP) policy for managing the risk of information asset failures and service disruptions. The CP program is intended to address security best practices with regard to business continuity and disaster recovery.

Scope

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by UTSI.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the Institutes IT resources.

Information transmitted or stored on UTSI IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles

This policy is UTSI specific. Each User is required to be familiar and comply with University policies. Acceptance of this policy is assumed if the User accesses, uses, or handles UTSI IT resources.

The Chief Information Officer (CIO) is the Position of Authority (POA) for IT at UTSI and is responsible for IT security at UTSI.

Program

1. The UTSI CIO has overall responsibility for the CP program at the Space Institute, and makes sure:
 - a. The program is developed, documented, and disseminated to appropriate UTSI personnel per the University policy.
 - b. The program is reviewed and updated annually.
 - c. In the event the primary storage location and processing site becomes inoperable, an alternate data storage and processing site has been established in the Propulsion Research Facility Control Building.
2. The UTSI CIO ensures appropriate system procedures are implemented.
3. All business systems supporting mission-essential functions are included in the CP program.
4. Documentation exists for the alternate storage and processing site, and their requirements.
5. User and system level back-ups are consistent with system recovery time and recovery point objectives
6. Conduct an annual Disaster Recovery scenario to test the system. Document the results.
7. Identify essential business functions that must continue and/or be restored in the event of an outage.



SPACE INSTITUTE

UT Space Institute Policy: IT0128-SI –Contingency Planning	
Version: 1	Effective Date: 09/18/2019

8. Provide recovery objectives and restoration priorities.
9. Address roles, responsibilities, and assign individuals with contact information.
10. Conduct and document annual staff contingency training.
11. Test backup quarterly.

References:

1. NIST Special Publication 800-53
2. IT0128

Last Reviewed: N/A