Catastrophic Events Policy

Interim Policy Approved: February 3, 2025

This policy is heavily informed by the College's plans governing critical incidents, non-delivery of services, and information technology.

The Allowance for Non-Delivery of Services addresses the College's response to course cancellations, program cancellations, and residency cancellations.

The Critical Incident Management Plan is a comprehensive plan that addresses College response and potential alternate operations for staff, faculty, and students.

The Information Technology Disaster Recovery Plan addresses the College's response to disruptions in data and other IT services.

Protection of Instruction

From the Allowance for Non-Delivery of Services: In the event that extenuating circumstances prevent Randolph College from delivering services for which students have paid, or which comprise a required part of a program already begun, the College will take steps to ensure that students either receive said services in an alternate form or receive reasonable financial compensation.

If a catastrophic event requires alterations to the normal operations of the College, services to students, faculty, staff and the public should be continued. The following are examples of how the Critical Incident Management plan addresses continuing operations for students:

- provide alternate study locations within the college confines.
- allow the use of alternate study locations off campus: including at home or in other venues off campus.
- change instructional modalities, including shifting to online or hybrid formats.
- or provide reasonable financial compensation.

In the event that program is cancelled because of a catastrophic event, the College will follow the guidance of SACSCOC and our Allowance for Non-Delivery of Services policy:

- provide students with a programmatic teach-out plan, which, in keeping with SACSCOC requirements, "ensures [that] the institution has a plan and process to provide students reasonable completion options that minimize disruption and additional costs."
- or provide reasonable financial compensation.

Protection of Records & Operational Systems

Randolph College's Information Technology Disaster Recovery Plan (IT DRP) follows best practices adhering to National Institute of Standards and Technology's SP 800-34 standards.

Within the scope of the plan, The Central Incident Response Team (CIRT) is responsible for timely evaluation of a disaster and implementing the activation, notification, recovery, and reconstitution phases of the IT DRP.

The Department of Information Technology maintains a backup policy and procedure for all production systems stored on-premises. Randolph College maintains a redundant data center and immutable backups in the cloud. Backups are periodically restoration-tested.

The College's guidelines for managing access controls to protect the confidentiality and integrity and availability of data and systems adhere to applicable regulatory requirements.

These guidelines follow the National Institute of Standards and Technology's SP 800-53 rev 5 and speak to account management and enforcement, and remote access, wireless access and mobile device management.