Disaster Recovery Policy for Chicago State University Systems

Policy Statement

To meet the enterprise business objectives, respond to a major incident or disaster, and restore the organization's critical business functions, Chicago State University (CSU) shall adopt and follow wellC S U

Scope

This policy applies to all facilities of CSU that operate, manage, or use IT services or equipment to support critical business functions.

Definitions

- are University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University.
- is someone officially attached or connected to the College who is not a student or employee (e.g., Extra Help, vendors, interns, temporary staffing, volunteers.)
- - include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, security, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
- is a major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.
- is the individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making

Responsibility

It is the responsibility of CSU's ITD management to ensure that appropriate DR plans are developed, documented, and periodically tested to ensure that ITD operations can be recovered relative to specific RTO/RPO specifications in the event of unscheduled interruption of those services.

Policy

Documentation

The documentation shall consist of Disaster Recovery Policy, and related procedures and guidelines.

Document Control

The Disaster Recovery Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the prev (f r,)11.1 c -0.-4 (re)--4 (re)--48opehBD0veguideli0pontr.t.4 (o)01.cTd[a (if)-4 (i)]TJ0.)3 rd3 ( )1

Policy Exceptions and Maintenance

Waivers from certain and specific policy provisions may be sought following the CSU ITD approval Process. There are no exceptions to any provisions noted in this policy until and unless a waiver