UNIVERSITY OF HOUSTON-DOWNTOWN

UHD IT BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING

1. SCOPE AND PURPOSE

This procedure addresses Business Continuity and Disaster Recovery planning for university operations that rely on major information systems.

The purpose of Business Continuity and Disaster Recovery planning in the context of critical application systems is to minimize disruption and ensure continued availability of critical applications and the primary business processes they support following a major interruption or disaster.

2. BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING PROCEDURES

The Chief Financial Officer (CFO) and the Director of Emergency Management, in coordination with university leadership, will develop and maintain a Business Continuity plan that incorporates the components listed below.

Business Continuity Plan Components:

A) Identification/validation of potential interruption types

B) A business impact analysis that identifies critical business processes and services which rely on major application systems. The business processes and services should be ranked by priority
(in the event of a major interruption or disaster). Downtime tolerances should also be clarified.

C) Formulation of contingency options/plans for the critical business processes and services.

This component of the plan should be specific enough to allow for preparatory activities to take place. However, it should not be overly detailed or prescriptive. It should be flexible enough to apply in many different situations and serve as a guide, providing useful, actionable, options for university leaders. It should also be designed to work in conjunction with the university's decision making processes and communication plans.

This component of the plan should be updated at least annually, and should be tested with tabletop exercises biennially.

The Chief Financial Officer (CFO) and the Chief Information Officer (CIO), in coordination with university leadership, will develop and maintain a System/Application Continuity plan that incorporates the components listed below.

System/Application Continuity and Recovery Plan:

A) Definition of critical application systems and their fundamental technical infrastructure components, ranked by priority in the event of a major interruption or disaster.

B) Identification of steps and procedures to restore critical applications and systems

and implement appropriate security and controls in the event of an interruption or disaster.

This component of the plan should be updated and tested at least annually.

Both the Business Continuity plan and the System/Application Continuity and Recovery Plan should be based on risk assessment, business impact analysis and risk management decisions validated by university leadership.