

Memo To: All UH-Downtown/PS Holders

UH-Downtown/PS 08.A.02

Issue No. 4

From: William Flores, President

Effective date: 05/01/10

Page 1 of 2

Subject: Information Technology Policies, Procedures, Standards, and Plans

1. PURPOSE

The purpose of this PS is to establish the process by which policies and procedures governing the use of UHD's Information Technology resources are developed, published, enforced, and reviewed.

2. DEFINITIONS

There are no definitions associated with this policy.

3. POLICY

3.1 The Chief Information Officer, acting in consultation with all appropriate user constituencies, including Academic leadership and the Academic Computing Committee, shall develop and periodically review the following policies, procedures, standards, and plans:

3.1.1 A policy for establishing project priorities as described in [PS 08.A.01](#);

3.1.2 Procedures for controlling access to Information Technology facilities by all user groups as denoted in [PS 08.A.05](#);

3.1.3 Security and access policies and procedures for hardware and software as specified in [PS 08.A.04](#);

3.1.4 Procedures for recommending university software and hardware standards and establishing an approved technology list, Exhibit A, Software and Hardware Standards.

3.1.5 Procedures and standards for the application development environment, Exhibit B, System Development Life Cycle & Project Management for IT Development Projects.

3.1.6 A business continuity plan and disaster recovery procedures, Exhibit C, UHD Information Technology Business Continuity and Disaster Recovery Procedures; and

3.1.6 University Information Technology strategic and operating plans.

- 3.2 The Chief Information Officer is responsible for publishing and enforcing the policies and procedures developed under 3.1 above.
- 3.3 Objections to the policies and/or procedures developed under 3.1 above must be made to the Chief Information Officer. If those objections cannot be resolved by the Chief Information Officer, they will be referred to the appropriate vice president(s) for resolution.

4. PROCEDURES

There are no procedures associated with this policy.

5. EXHIBITS

Exhibit A: Software and Hardware Standards

Exhibit B: System Development Life Cycle & Project Management for IT Development Projects

Exhibit C: UHD Information Technology Business Continuity and Disaster Recovery Procedures

6. REVIEW PROCESS

Responsible Party: (Reviewer): Chief Information Officer

Review: Every three years on or before May 1st.

Signed original on file in Employment Services and Operations.

7. POLICY HISTORY

Issue #1: 01/15/82

Issue #2: 12/15/87

Issue #3: 03/23/94

8. REFERENCES

[PS 08.A.01](#)

[PS 08.A.04](#)

[PS 08.A.05](#)

UNIVERSITY OF HOUSTON-DOWNTOWN **SOFTWARE AND HARDWARE STANDARDS**

The University of Houston-Downtown will develop and maintain a Supported Technology List for basic software and hardware products which are frequently used on campus. The purpose of this list is to assist users in selecting the computing or communications products that are tested, proven, maintainable and can be supported by Information Systems. The process will also ensure that departmental purchases are consistent with the university's short and long term information technology plans.

1. The Chief Information Officer will maintain a Supported Technology List for the university.
2. Departments are encouraged to select from the Supported Technology List when applicable. Requests for university-funded software/hardware purchases which differ from established university technology standards will require written justification and must be approved by the Chief Information Officer in order for the product to be supported by Information Technology.
3. As funding becomes available, Information Technology will negotiate site license agreements with various vendors for basic desktop productivity software.

UNIVERSITY OF HOUSTON-DOWNTOWN
**SYSTEM DEVELOPMENT LIFE CYCLE &
PROJECT MANAGEMENT FOR IT DEVELOPMENT PROJECTS**

1. PURPOSE

System Development Life Cycle (SDLC) methodology, coupled with UHD's IT Project Management processes, provide a context and toolset for controlling and managing activities which produce software or application system products as authorized by the University of Houston-Downtown. The objective is to imbed a set of controls and practices to ensure that Information Technology products are secure, reliable and conform to applicable requirements, standards and procedures.

2. PROCEDURES

2.1 Information Technology is responsible for developing, maintaining, and utilizing a SDLC process for UHD. The process must be implemented within the context of the IT Project Management processes, and utilize the SDLC guidelines included in the Statewide Project Delivery Framework as a resource.

2.2 Where applicable, the following areas should be addressed in the SDLC and/or Project Management Processes for system development or application system projects:

- Preliminary analysis or feasibility study
- Risk identification and mitigation
- Requirements definition and analysis
- Scope definition & management
- Design and development
- Technical environment analysis, set-up and configuration
- Change management
- Functional configuration and access management
- Technical and functional testing
- Security
- Data integrity
- Code integrity
- User acceptance
- Separation of duties in production implementation
- Production implementation
- Service level agreement(s)
- Disaster recovery and business continuity planning

Post implementation review

- 2.3 Use and customization of the UHD SDLC process is to be determined on a program/project basis, and is the responsibility of the IT Compliance and Project Management Office, in coordination with the Chief Information Officer.

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 Chief Information Officer (CIO), in coordination with university leadership, will develop and maintain a plan that incorporates the components listed below.

Business Component: (Business Continuity)

- 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.

Technical Component (System/Application Continuity and Recovery)

- 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 and Technical components of the Business Continuity and Disaster Recovery Plan should be based on risk assessment, business impact analysis and risk management decisions validated by university leadership.