

**FIRST FOLLOW-UP REPORT:
A RECORD OF PRESIDENTIAL APPROVAL
TO TASK FORCE RECOMMENDATIONS FOR
Networking and Telecommunications, 4/15/08**

With input from the Cabinet, the President makes final approval of program review recommendations. This report articulates those decisions. Approval of task force recommendations requiring funds beyond the base budget of the reviewed unit is not tantamount to receipt of additional funds. Those funding requests must be channeled through the institutional budget process. Nonetheless, special consideration will be given to requests stemming from program review recommendations.

A progress report toward implementation of recommendations must be drafted one year following completion of the task force report by the chairperson. The report will be sent electronically to the Special Assistant to the President for Strategic Planning & Analysis for college-wide distribution and archiving. Recommendations not achieved within a year are to become "objectives" in the corresponding unit plan to ensure a continued focus on their achievement.

The President accepts the recommendations of the task force with modifications specified in recommendations #3 and 12. Underlined phrases are additions and ~~strikethroughs~~ are deletions.

Recommendations

- 1)** Develop and publish an HCC approved IT hardware and software list in order to improve delivery of service and reduce support costs. Investigate the feasibility of including an OIT review for all procured hardware/software not included in applicable hardware/software standards college wide.
- 2)** In partnership with Academic Technology analyze OIT and College technical support resources to recommend a plan for more efficient and appropriate allocation of human, fiscal, and technological resources to academic and administrative technology support needs.
- 3)** In conjunction with Administrative Systems and ~~Institutional Research~~ the Department of Management Information Systems develop and recommend for adoption a formal Program Delivery Process. The process should ensure the following areas, at a minimum, are addressed as part of all information systems or network affecting projects or academic programs:
 - i.** Program definitions and objectives.
 - ii.** Document all areas impacted by the project.
 - iii.** OIT notification of all new hardware and software. This would not stop employees and staff from using new hardware and software but would ensure OIT awareness and support system and network integrity.
 - iv.** Document monitoring and control procedures for the new project.
 - v.** Document ownership, access, back up and retention requirements for data.
 - vi.** Document Disaster Recovery/Business Continuity requirements.
 - vii.** Establish metrics to evaluate system/network performance.
 - viii.** Data security.
 - ix.** Support roles, i.e. service level requirements, daily operation, access permission and ID's, procedure definition, etc.

4) Partner with Professional Development Services to develop and implement strategies to increase the level of communication between unit and college users.

5) Create an IT policies/procedures committee to:

- i. Create, modify, recommend, and implement IT related policies/procedures
- ii. Educate the HCC community of current IT policies/procedures.
- iii. Conduct an annual review of all IT policies/procedures.
- iv. Develop policies/procedure for new systems.

6) Partner with Web Services to expand the OIT web site to assist customers in understanding the responsibilities of OIT and include a FAQ page(s) to assist the user community in obtaining information technology services.

7) Immediately address findings of the 2007 Operational Audit that have no budget impact and provide cost estimates for findings that do have budget impact to be considered for funding:

- i. **Policies and procedures.** (Complete development, approval, and implementation of applicable IT policies/procedures.)
- ii. **Security awareness and training.** (Approve and implement a security awareness and training program for all users of IT resources.)
- iii. **Physical access controls.** (Transfer access control authority for the datacenter and communication closets to OIT management, restrict access to only those persons who have legitimate need, continue with plans to implement an electronic access system.)
- iv. **Logical access controls** (Implement a biannual audit of all user account databases, strong passwords and industry password change frequency will be required for all capable systems, implement this security warning banner for all potential users for all systems that are capable.)
- v. **Change management controls.** (Implement change management controls, automate if possible)
- vi. **Service continuity controls** (Complete a comprehensive service continuity plan driven by a formal risk assessment and business impact analysis.)
- vii. **Environmental controls** (Address environmental risk to data center and associated computing facilities.)
- viii. **Risk analysis and security plan** (Conduct a formal risk analysis and business impact analysis to highlight actual exposure and drive the security/DR plan).
- ix. **Incident response and monitoring controls** (Ensure appropriate security incident response and performance monitoring procedure are developed and implemented.)

8) Seek cabinet approval of the request in the 2007-2009 unit plans to add funding of helpdesk operations into departmental budget. Investigate costs for a hybrid model where the community could receive technology assistance after core hours from a 3rd party and add this initiative to the strategic planning cycle for 2007-2009 planning cycle.

9) Through the IT policies/procedures committee develop and implement a College wide Service Level Agreement to be recommended to cabinet for enterprise approval.

10) In partnership with Institutional Research seek modifications to the Faculty/Staff survey instrument that will allow a more direct evaluation of select networking operations (e.g. networking, server, desktop, help desk, telephone).

11) Develop a recommendation outlining organizational and fiscal impact for the establishment of a dedicated information security and audit arm for the College that would be dedicated to ensuring the availability, confidentiality, and integrity of electronic data and applicable regulatory and institutional policy compliance.

12) Partner with Institutional Research, Management Information Systems, Student Services, Finance, Purchasing, Public Safety, Human Resources, and Legal to develop a data classification scheme/data ownership and implement a backup policy relevant to the scheme. The Network and Telecommunications unit is ultimately responsible for the protection of all electronic data at HCC. To provide this protection the unit needs direction regarding business operation, regulatory requirements and legal considerations from the data owners.

13) Conduct a formal risk and business impact analysis to highlight actual exposure and drive the security/DR plan.

14) Partner with the Office of Strategic Planning and Analysis to evaluate current enterprise technology initiative prioritization in order to develop and recommend a process that will lend itself to prioritization of technology initiatives as they relate to overall College objectives and strategic initiatives.