Chapter 4: Central Services

Central services are those that are used by or affect the campus as a whole, and often require collaboration across multiple units. Traditionally on the CU-Boulder campus, those services have been provided both by the central IT unit (ITS) and by departments. In some instances, this mix of central and departmental provision of services has resulted in greater flexibility for departments and the ability for departments to tailor IT services to local needs more effectively. In others, central and departmental services may be duplicative at best, competing at worst.

The recommendations in this chapter include a call for greater central management and/or coordination of certain services, including integration of departmental services with the Enterprise Directory, email server management, and software licensing and distribution. This does not change the fact that central provision of services will be balanced by services that are provided in a more distributed fashion. Although many of the recommendations require greater collaboration and cooperation between ITS and departmental IT operations, departmental IT personnel are the keystone in the provision of services and support that is both close to end users and tailored to their particular needs. As such, it is imperative that increased centralization and collaboration coexist with appropriate departmental autonomy and that, even as the campus implements greater centralization in critical areas such as security, it concomitantly seeks to maintain and enhance distributed services in areas such as desktop support. Chapter five discusses issues of authority and coordination more fully.

As with recommendations in other chapters, those in Chapter four have security, reliability, and cross-unit collaboration and cooperation as their foundation and top priorities. Recommendations include:

- Enhancement of existing services such as email, the four-tier IT support model, and assistive technology;
- Better management of existing services such as software licensing and application standards;
- Development of a security and a web-based services infrastructure;
- Development of e-payment and file system solutions;
- Coordinated preparation for the next generation of SIS and PeopleSoft; and
- Development of best practices, policies, and guidelines critical to the successful implementation of these recommendations.
4.1 Email

Recommendation: Provide enhanced and new email services to all faculty, staff, students, and designated affiliates so that email is: convenient to access from on- and off-campus, easy-to-use, reliable, highly available, and secure. Centrally-managed systems must be enhanced to further combat unsolicited commercial email and viruses; the central infrastructure must be augmented to ensure high-availability and redundancy to reduce the need for distributed systems which may be expensive, proprietary, and complex; reliance on client desktop software should be reduced in favor of new web-based, feature-rich interfaces; new methods should be provided to facilitate group collaboration in both real-time and via more traditional message-based and web-based delivery. Key components, including bulk delivery, address lookup, and delivery mechanisms should be integrated with the Enterprise Directory.

Discussion of the Recommendation

Current Situation
All students are required to have CU-Boulder email accounts and are responsible for reading email sent to them\(^1\). No similar policy exists for faculty and staff and access for them is uneven, with some having excellent email access through central or departmental servers while others have poor or no access. Group and bulk email communication methods are inconsistent, sometimes slow, and often unwieldy to use and manage. Unsolicited commercial email (UCE, often called “spam”) is rampant and there is no campus-wide, comprehensive effort to eliminate and prevent the spread of electronic viruses. Email is routinely used to send sensitive information yet most email is sent without any verification of sender and without content encryption. The centralized and departmental costs associated with providing email services on campus are not widely recognized or understood.

Rationale
Email has become a ubiquitous means for communication within the campus community and beyond. It is quicker and cheaper to send email than to deliver hardcopy mailings and its colloquial nature promotes a sense of community unmatched by traditional paper mailings. Email has become mission critical and the infrastructure needed to support this function must be further developed and established.

Specific Recommendations Include

- Develop and encourage the use of a reliable and redundant email infrastructure that provides all faculty, students and staff with:
  - Robust, standards-based service that uses secure authentication integrated with the Enterprise Directory; the service should include a full-featured web-based interface requiring no client software besides a campus-endorsed web browser.
  - Online access to messages with adequate storage capacity to accommodate the variety of needs and roles of campus constituents.
  - Integration with future web-based services offerings for the variety of constituent groups (e.g. faculty, students, administrators, researchers, instructors, alumni, etc.).

\(^1\) Many students have and use an alternate email provider instead of or in addition to the CU-Boulder service.
• Further develop and promote the centralized campus email gateway for use in processing all incoming and outgoing email; on this gateway perform real-time anti-virus processing and filter unsolicited commercial email.
• Develop and promote a uniform, campus-wide, scalable email addressing scheme that is integrated with the Enterprise Directory for lookups and is designed to enable graduating students and designated affiliates to keep their CU-Boulder email addresses forever, if they so choose.
• Provide role-based email identities to enable an individual and/or individuals to receive and send email from a non-personal identity that is linked to the individual(s).
• Develop and promote mechanisms for small group collaboration via easy-to-use email lists and/or threaded discussions.
• Develop and promote mechanisms to enable rapid and efficient delivery of messages to large segments of selected campus populations for both urgent and routine messages.
• Develop and promote best practices and policies governing use of email for performing transactions and sending confidential information and for appropriate retention, backup, and restoration of email.

Steps

Implementation
• Establish service level goals for the campus email infrastructure, including the central gateway and central servers, by considering requirements for:
  o Capacity and scalability.
  o Redundancy and reliability.
  o Universal availability.
  o Features, including client software, anti-virus, and content (UCE) filtering.
• Design and develop a centrally-managed infrastructure to meet the established service goals.
• Perform anti-virus and anti-UCE processing on all incoming and outgoing email by routing all email through the central campus gateway.
• Establish an efficient mechanism for delivery of urgent messages to sender-specified populations.
• Develop a web-enabled group message environment for collaboration.
• Incorporate security into the campus email infrastructure to provide non-repudiation of sender and recipient identities (to guard against forgery and spoofing), guarantee message integrity, and safeguard message content.
• Leverage the Enterprise Directory and IT service provisioning infrastructure to provide role-based email identities.
• Evaluate needs for campus-wide instant messaging systems.

Communication
ITS and appropriate campus departments and individuals will collaborate on development of policies, best practices, and service level agreements. Additional communication and input-gathering will be performed via surveying faculty, staff, and students; by talking with campus IT representatives; by offering presentations at committee meetings and other gatherings; and by communicating via traditional channels such as ememos, print media, and hardcopy mailings.

Policy & Standards
• Establish policies regarding: anti-virus and UCE filtering on servers that accept incoming email; use of email for official notification to faculty and staff; use of email for distributing sensitive or critical data; requirements for appropriate backup and retention of email.
• Establish guidelines and methodologies for administration and management of central and departmental email servers.
As part of the service provisioning infrastructure initiative, establish campus-wide standards for email addresses.

**Required Involvement**

**Governance & Authority**  
The Office of the Associate Vice Chancellor for Campus and Academic Technology.

**Required Departmental Involvement & Responsibilities**

- IT Council to provide guidance and programmatic direction.
- Legal Counsel for guidance on policies.
- Human Resources and Faculty Affairs for guidance on policies relating to faculty and staff.
- ITS to develop and promote service level goals in cooperation with campus departments.
- ITS to lead the design, development, and implementation of a centrally-managed email infrastructure in cooperation with campus departments.
- ITS to develop and promote best practices in cooperation with departmental IT and email providers.
- ITS to design, maintain, operate, and manage the campus gateway and central email servers.
- ITS security coordinator and working group to guide development of secure messaging.
- ITS, Mailing Services, and Registrar to collaborate on bulk delivery mechanisms.
- ITS to partner with campus email providers to help them leverage a centrally provided email gateway for processing incoming and outgoing email services to better meet their departmental messaging needs.
- ITS, UCSU, and student fee allocation committees to address spending of student fees.

**Expected Costs**

**Annual IT Infrastructure Investment**  
Costs include hardware and software needed to deploy a fault tolerant operating environment, including the central email gateway and central email servers, backup subsystems, redundant power environment, and software.

Student fees currently support the non-personnel costs associated with the central email systems dedicated to students. Ongoing costs are approximately $180,000 per year and cover operating expenses (server software, hardware maintenance), small capital improvements, and renewal and replacement of existing systems. Fees currently do not contribute to any cost associated with the central gateway system.

- One-time cost to augment the email gateway to ensure high-availability and reduce viruses and UCE - $220,000. Ongoing costs for renewal and replacement (based on a 4-year replacement cycle), operating (10%/year), small capital improvements (10%/year) - $99,000.
- One-time cost to augment servers used by faculty/staff to provide service equivalent to that provided to students - $350,000. Ongoing costs for renewal and replacement (based on a 4-year replacement cycle), operating (10%/year), small capital improvements (10%/year) - $157,500.

Costs for providing non-repudiation and security of message delivery should be included as part of the overall campus security plan.
Personnel
Personnel exist within ITS to lead the design and development of the infrastructure enhancement as well as its operation; no new personnel are required. If campus departments choose to convert from locally-maintained email servers, particularly Microsoft Exchange-based, to centrally-provided services, existing ITS personnel up to 0.5 FTE for 6 months can be made available to assist with the migration. Enhancement and development of group collaboration will require 0.5 FTE for 2-3 months that can be found within existing ITS personnel. Personnel to provide backup subsystems also exist within ITS.

Funding
Email and electronic collaboration are essential and increasingly mission-critical for all students, faculty, and staff. A combination of institutional funding, student computing fees, and cost recovery should be used to provide campus-wide email services.

Student fee revenue, either by reallocation or additional, should be identified in the amount of $5/student (assume 26,000 students) to contribute to the one-time cost of augmenting the campus email gateway - $130,000. Student fee revenue in the amount of $2.25/student/year should be identified to contribute to the ongoing cost of the central email gateway - $58,500.

The balance of the one-time cost for augmenting the email gateway and the full cost of augmenting faculty/staff services should be identified through cost recovery. A mandatory one-time assessment of $74 per FTE (assuming 6000 FTE) should be made. Ongoing fees of $2.75/month/FTE should be assessed as part of a new basic services infrastructure fee that would provide services such as email, security infrastructure, departmental web services, and basic file services.

The campus will see cost savings if departments migrate from departmentally-provided email to a centralized service. For an average department of 40 FTE, annual savings of $7,000 – 20,000/year for system acquisition, renewal and replacement, software licensing, and operating could be realized along with reduced personnel requirements of .2 FTE. Assuming 20 such departments, the campus-wide savings will be $140,000 – 400,000 per year plus 4 FTE.

A one-time special budget allocation should be identified to explore and develop instant-messaging services for the campus. If successful, ongoing costs should be recovered as part of a basic services infrastructure fee.

Timing
Development of a robust email gateway should begin immediately to shield the campus from the risk of email viruses and reduce the personnel time wasted by attending to unwanted, unsolicited commercial email. A web-based email system should be deployed in AY 2002-03 for all faculty and staff to match the service provided to students since 1999. Email list delivery should be improved in AY2002-03 followed by evaluation and potential deployment of collaborative environments. Methods to ensure non-repudiation and message integrity should be carefully monitored and deployed when the technology supports it.
4.2 IT Security

Provide an Information Risk Management (IRM) function that establishes a secure campus Information Technology (IT) environment, employs best practices to ensure reliable and secure electronic communication, maintains a secure and robust computing and network environment, data integrity and reliability, and encourages proactive IT security management.

The IRM function includes developing security policies and procedures that address authentication, access control, non-repudiation, and authorization, plus planning and oversight for data integrity and privacy, disaster recovery, network security, intrusion detection, firewalls, and incident response.

Discussion of the Recommendation

Current Situation
The campus is well underway in the effort to develop security-related policies, best practices, and guidelines. However, much of the campus lacks awareness of and understanding of these policies and guidelines. Consequently, system administrators and users often make uninformed decisions that have a detrimental impact on the security and integrity of the campus IT infrastructure and other IT systems.

The Network Security Proposal, drafted by the ITS Security Working Group, was developed specifically to address campus network security weaknesses, and is in the process of being implemented.

CU-Boulder has recognized the need for an IT risk assessment process to ensure the security and continuity of the University’s IT resources. The results of the risk assessment process will help to mitigate vulnerabilities of campus mission critical, IT-dependent services. In addition, data collected and lessons learned from the risk assessment will provide the foundation for setting the future directions for campus IT security. The early stages of the current risk assessment cycle have shown that business continuity planning and disaster recovery is significantly lacking at CU-Boulder. Many IT units either do not have disaster recovery plans or have not tested existing plans.

Rationale
The IT resources impacted by IRM include information, services, and equipment. More to the point, the qualities of these resources that the campus seeks to secure are privacy, integrity, authenticity, and availability. Attacks, human errors, and system malfunctions threaten these qualities. Any IT resource on campus has the potential to negatively impact a wide variety of other IT resources on- and off-campus; therefore establishing an IRM strategy is a campus-wide function.

The increased reliance on IT as part of the university business and academic communications infrastructure requires technical solutions to ensure the integrity and authenticity of electronic communication. Maximum benefit from these solutions will only be achieved if they are implemented under an overall IRM strategy.

---

2 Current policies can be found at http://www.colorado.edu/its/security/policy.html
3 The proposal can be found at http://www.colorado.edu/ITS/security/SWG/NetworkSecurityPositionPaper.doc
The reasons to provide secure means for electronic communication are many. While there is no question that email as a delivery mechanism has proven to be easy, economical, and fast regardless of the message content, there are risks in sending sensitive or critical data via email. It is relatively easy for an attacker to capture email thus gaining access to private or sensitive information. Additionally an increasing number of attacks involve social engineering that deceives users by falsified “official” university communications. A campus-wide mechanism to protect both the privacy and integrity of the data is needed.

Finally, while desktop anti-virus scanning is still an integral part of worm, virus, and trojan-horse defense, experience has shown scanning to be less effective than necessary for a number of reasons. Foremost, the software is only as effective as the user or administrator configuring the product. All too often, software is installed and not updated, or users just do not understand the need to use such defensive software. Anti-virus software is increasingly both hard to understand and to manage.

Without the basic IT security infrastructure, it is impossible to have effective IT security.

**Specific Recommendations include establishing a campus IRM function by:**

- Continuing efforts to improve security awareness and practices through establishment, communication, and enforcement of policies, best practices, and guidelines.
- Providing campus risk assessment processes and business continuity planning guidance to mitigate vulnerabilities in critical systems and to provide data to better determine future campus security needs.
- Providing effective campus solutions for worm, virus, and trojan-horse defense.
- Implementing solutions providing integrity and verification of electronic communication and communicating secure and effective uses for electronic communication.
- Proactively improving security though campus intrusion detection and vulnerability assessment.
- Improving the campus incident response process and formalizing the ITS incident response team.

**Steps**

**Implementation**

- The ITS Security Working Group and ITS core experts will evaluate and develop IT best practices and policies and provide the campus with training opportunities.
- Continue with the existing risk assessment process.
- Provide IT business continuity & disaster recovery templates for campus departments. Provide an anti-virus licensing option or a campus site license; build supporting infrastructure; implement a campus anti-virus policy; publicize best practices; and offer training for desktop protection strategies.
- Campus infrastructure servers already support the encryption of authentication and sensitive data. This technology should be extended to other campus or departmental servers. Reconfigure or replace client-side application to utilize server security features.
- Develop and implement a secure email environment that enables non-repudiation of sender and recipient identities and guarantees integrity of electronic communication.
- Implement a network vulnerability assessment service for use by the campus Tier 2 computing support partners.
- Evaluate different intrusion detection system solutions and approaches; resolve policy and legal issues; and implement a campus intrusion detection solution.
- The ITS Security Working Group will develop and implement an incident response process.
Communication
Build on the existing security communications team to develop and implement a security communications program with the goal of increasing awareness of and adherence to security policy and guidelines.

Policy & Standards
- Develop campus Anti-Virus Policy.
- Continued best practices and standards for existing and new technologies.

Required Involvement

Governance & Authority
- The Office of the Associate Vice Chancellor for Academic and Campus Technology.
- IT Council to provide guidance and programmatic direction.

Required Departmental Involvement & Responsibilities
- Tier 2 Computing Support Advisory Team to provide input and review IT security initiatives.
- ITS to provide core leadership in the design, maintenance, operation and management of the IT security infrastructure.
- Office of the Associate Vice Chancellor for Academic and Campus Technology and ITS to provide core risk assessment core team members.
- Boulder Campus Health and Safety, and Risk Management as well as the University Internal Audit to provide input into Business Continuity and Disaster Recovery templates.
- Legal Counsel to provide clarification of liability and other legal concerns regarding aspects of IT security.

Expected Costs
All funding requests require new funding.

Annual IT Infrastructure Investment
- Ongoing $5,000 for continuing communications support.
- Campus anti-virus site license upfront costs of up to $250,000 depending on licensing and technical strategies chosen.
- Web based secure shell application $15,000.
- Hardware and software for secure electronic communication supporting infrastructure. Depending on the scope of the effort costs estimated to be between $250,000 and $2,000,000\(^4\). The campus will focus on implementing a smaller scale solution that may require more internal staff effort thus keeping costs closer to $250,000.
- $250,000 for firewall hardware\(^5\).

Operating and Maintenance
- $100,000 annual maintenance for anti-virus software licensing (exact costs dependant on licensing and technical strategies chosen). Costs for this should be recharged.
- $4,000 hardware maintenance and $1,500 administration for vulnerability assessment of systems.

\(^4\) The variation is based on the specific technical solution and possible broader campus objectives for enterprise authentication as addressed in the IT Provisioning Strategic Plan.

\(^5\) The variation based on the specific tactical solution and the current state of the technology.
• $25,000 hardware maintenance and $4,500 administration for intrusion detection systems.

Funding
All of the above funding items above require new funding. A combination of institutional finding and cost recovery should be identified to fund IT Security initiatives. Potential cost recovery sources include network fees (e.g., network security, intrusion detection, incident response), student fees (e.g., secure electronic communication), and e-memo (e.g., secure electronic communication) funding mechanisms.

Timing
Specific timing will vary based on funding and tactical level decisions. The timing listed represents implementation priorities for the objectives in this plan.

- Security Awareness: in progress and an ongoing effort.
- Risk assessment process: in progress and an ongoing effort.
- Provide business continuity & disaster recovery templates for campus departments: Fall 2002.
- Anti-virus solutions: Winter 2002
- Encryption of authentication and sensitive data: Winter 2002
- Secure electronic communication: AY 2003-2004
- Network vulnerability assessment: Spring 2003
- Intrusion detection system: AY 2002-2003
- Incident response process: Fall 2002
4.3 Electronic Payments

Recommendation: Provide a trusted, robust, and secure method of accepting electronic payments.

Discussion of the Recommendation

Current Situation
Handling credit card payments is widely accepted on campus by auxiliary operations as an effective means of payment. However, formal policies, guidelines, and/or best practices are not established, widely disseminated or routinely followed. Though campus departments are increasingly interested in accepting e-payments, they are rarely equipped to handle the issues and the technological considerations that are part of doing business on the web. A uniform e-payment solution can resolve these issues and is one of the web-based services most frequently requested by departments.

To begin addressing the issues of accepting e-payments and doing business on the web, CU-Boulder established a review process described in the university’s Web Publishing Policy. (See: http://www.colorado.edu/webcom/webpolicy/) The need to address issues created by the absence of a campus-wide e-payment solution was a key element in the framing of this policy.

The review process for e-business and e-commerce activities is meant to ensure compliance and appropriateness in the following areas:

- Alignment with the campus academic mission.
- Consideration of and attention to business/financial/licensing issues.
- Marketing/communications.
- Legal review, contractual arrangements, etc.
- Technology/infrastructure integration (most importantly related to security).

The University Treasurer’s Office has set up robust and secure methods of e-payments and has negotiated financial arrangements and very competitive rates to handle e-commerce transactions. In addition, the office publishes information and best practice guidelines that are meant to ensure that good business processes are in place before a department accepts cards for payments. Most of the requirements in the Treasurer’s Office documents are either mandated by law or are dictated by prudent business practices. See: http://www.cusys.edu/~treasury/.

Despite the Web Publishing Policy and the Treasurer’s Office guidelines, recent survey information shows that departments have implemented a disparity of payment solutions, most of which did not go through the review process outlined above. It has been identified that approximately 40 departments on campus accept e-payments in some form, although these solutions vary greatly.

Rationale
There is significant customer demand for electronic payment for campus products and services (e.g. tickets for the Artist Series and other theater events, athletics tickets, and tuition and fee payments). E-payment clearly provides a competitive position for many services. The financial and technical aspects of the campus solution should be developed based upon generally accepted business practices, adopted by the appropriate campus constituencies, and enforced by a designated authority. In accepting any form of e-payment, a department is assuming a

---

6 Electronic Payments are defined as the acceptance of payment for goods and services where the sale is negotiated over the Internet. Payments are tendered in the form of credit cards or funds transfers.
significant responsibility. In the event that a department does not meet its responsibilities to the
sponsoring merchant bank, the credit card system, the customer and the university as a card
accepting merchant, not only is the department potentially liable, but also the university as a
whole may face significant financial risks.

Specific Recommendations Include

- Develop and communicate policies with specific statements to include that:
  - The business and technological aspects of all e-payment solutions must be
    approved by the Office of the Director of Budget and Finance.
  - All e-payments must be handled through the Office of the Treasurer for banking
    and accounting purposes.
  - All electronic transactions must be made using secure connections to secure
    services. On-campus servers must meet ITS requirements for security to ensure
    payments are accepted in a consistent, secure and controlled manner.
- Formalize CU-Boulder campus approval process by ensuring that:
  - A department contacts the Department of Budget and Finance, which will
    facilitate the review required by the web policy.
  - Upon approval, the department will be referred to ITS for technical support, ITS
    requirements, and advice.
  - Upon approval of the department’s e-payment proposal the department will be
    referred to the Treasurer’s Office.
  - The Treasurer’s Office will implement banking and accounting arrangements.

Steps

Implementation

To achieve this recommendation the development of four components are required: campus-wide
policies; the Budget and Finance process; campus-wide, web-based authentication tools using
the Enterprise Directory Service; and formal financial arrangements with the university’s financial
institutions.

Communication

- Detailed communication plan to be developed after pilot deployment occurs.
- Ongoing training programs on e-payment opportunities, responsibilities and changes
  through Treasurer’s Office.

Policy & Standards

- Periodic update of the Web Publishing Policy (which includes the e-business review).
- Treasurer’s Office Requirements and Policies for departments accepting electronic
  payments (to include Visa / MasterCard, bank, and other regulatory requirements).
- Treasurer’s Office Standards for initiation of ACH debits (currently under development).
- PSC / Treasurer’s Office Standards for initiation of ACH credits (currently under
development).

Required Involvement

Governance & Authority

The CU-Boulder Chancellor should issue a directive that all departments wishing to accept e-
payments must adhere to campus and system-level policies. The AVCACT and the Director of
Finance and Budget have joint coordinating responsibility for the program.

ACH is the Automated Clearing House Network, which is a nationwide batch-oriented electronic funds transfer system. The American Clearing House Association, Federal Reserve, Electronic Payments Network, and Visa act as ACH Operators.
Required Departmental Involvement & Responsibilities

- Budget and Finance will facilitate the process of providing consultation and guidance to departments wishing to accept e-payments.
- ITS will provide technical consultation and guidance to departments who express interest in developing e-payment applications.
- Web Communications will provide guidance, standards, and best practices for the development of web applications.
- Treasurer’s Office will set standards for e-payment acceptance and required regulatory business standards, as well as to setup and maintain banking and card system relationships.

Expected Costs

Annual IT Infrastructure Investment
Annual IT Infrastructure costs will be integrated into the operating budgets of ITS and UMS for the base system support.

Departments accepting any form of e-payment will be responsible for any and all incremental costs related to supporting the service.

Operating and Maintenance
Same as above.

Personnel
Same as above.

Funding
Use existing budgets for funding.

Timing
January 1, 2003 for limited campus deployment.
June 30, 2003 for full implementation of policy, including review of existing electronic payment relationships.

Existing contracts should be honored until the end of the contract periods.
4.4 Software and Software Licensing

Recommendation: Improve the processes used to identify, acquire, and manage software licenses, making software tools available to the CU-Boulder campus community at the lowest possible cost.

The CU-Boulder campus must develop selection criteria for software tools; investigate and identify appropriate products; negotiate advantageous purchase programs; communicate information and best practices to campus users; and provide resources to improve the management of software assets. These responsibilities should be assigned to existing units based on their established roles, competencies, and resources.

Discussion of the Recommendation

Current Situation
The campus has many computing systems and therefore, a significant need for software products. The campus acquires software products from a large number of developers/vendors who provide a wide array of products, with a wide variety of features and capabilities, technical requirements, and licensing terms.

The university faces special challenges in acquiring software products because software contracts are not like contracts involving ordinary goods. Software contracts transfer intangible assets and often provide a right to use rather than to own the product. Therefore, people involved with software licensing on campus must take time not only to identify appropriate products but also to understand complex licensing and purchasing terms, both of which change frequently.

Rationale
The availability of software tools is critical to the business, instructional, and research activities of the university. However, many in the campus community are seemingly unaware of existing campus-wide licenses or purchase programs; information about our current programs has not been effectively communicated. As well, many departments, academic units in particular, report that they are unable to afford the software tools required to do their work. Improving the processes used to identify, acquire, and manage software licenses will improve software availability while lowering ownership costs.

Specific Recommendations Include
- Develop selection criteria, such as the demand for software, the value of software, the compatibility of software with other computer systems, and the cost of software.
- Develop best practices and guidelines for managing software assets.
- Identify funding sources to acquire essential software tools for faculty.
- Improve student access to software tools, especially those used in teaching and learning.
- Identify funding sources to support activities related to the administration of software licenses, coordination of purchase programs, dissemination of information about software, and distribution of licensed software products.

• Define computer system ownership at an appropriate level (deans, directors, department heads), considering the funding organization of the campus and delegate responsibility for ensuring license compliance accordingly.
• Identify and clearly define roles and responsibilities for:
  o Decision makers, including technical and subject matter experts, who will determine which software products will be acquired.
  o License agreement interpretation and guidance for legal compliance.
  o Procurement, distribution, asset management and related business activities.
  o Coordination of license and purchase agreement and communication regarding existence, availability, and terms and conditions of use.
• Participate in consortia with other universities to share information and possibly gain advantages through coordinated negotiations with vendors.
• Promote coordination of software selections for use across academic, business, and research areas.
• Negotiate and promote purchase agreements for the campus, focusing initially on products that are ubiquitous or essential, and based on IT and campus initiatives.

Steps

Implementation
• Survey and assess the software products that have been purchased and are in use on the CU-Boulder campus.
• Determine the cost of providing and maintaining software tools and make this information available for inclusion in budget projections.
• Perform a gap analysis to determine how well the software needs of the campus are being identified and addressed.
• Review the current software licensing processes and procedures, identifying specific opportunities for improvement.
• Assign responsibilities and establish timelines for developing selection criteria and best practices for managing software assets.
• Identify a funding source specifically for providing software for faculty.
• Identify specific roles and responsibilities in cooperation and consultation with faculty, the Tier 2 support community and IT Council.
• Create and staff two positions to support the administration of software-licensing programs.
• Develop advanced solutions for software distribution and access, including automated and remote installation and management, network licensing and license metering.
• Investigate the availability and value of software management products.
• Partner with the Office of Budget and Finance to develop improved practices and identify specific business opportunities.

Communication
• Use appropriate channels, such as the campus web site, constituent group meetings, e-memos, support community events, and print advertising to:
  o Inform the campus community of the existence of site and other broad license agreements.
  o Raise awareness about the rights and responsibilities of software ownership and use.
  o Ensure that IT support providers can provide accurate and timely information.

Policy & Standards
• Develop guidelines for selecting and acquiring software products.
• Develop standards and/or guidelines for managing assets and complying with licenses.
- Publicize position statements and policies that promote the ethical and legal use of software.

**Required Involvement**

**Governance & Authority**
The Office of the Associate Vice Chancellor for Campus and Academic Technology.

**Required Departmental Involvement & Responsibilities**
- ITS for technical expertise in advising and support.
- Office of Budget and Finance for coordination of business service activities.
- Faculty and academic technology representatives and coordinators for guidance and identification/prioritization of software tools.
- Departmental support associates for guidance and identification/prioritization of software tools.
- Procurement Services and University Legal Counsel for review and authorization of contracts.

**Expected Costs**
The following infrastructure, operating, maintenance, and personnel items represent new costs. The specific products that are cited reflect solutions that are available today and provide a basis for cost estimates. Further analysis will be required to identify the best solution and to establish the actual cost of implementation and maintenance. These newly incurred costs would be partially offset by savings in budgeted software acquisition costs and unbudgeted staffing costs.

**Annual IT Infrastructure Investment**
Costs include hardware and software needed to deploy a large-scale software management system that provides: software distribution, cost recovery system, efficient license management, and monitors demand.
- Software management and distribution systems (e.g. e-Academy License Management System (ELMS)).
  - One-time setup and integration fee - $5000.
  - Annual license fee, including updates, $1 per FTE - $31,000.
  - Primary and backup hardware systems - $10,000 (replaced every 3 years).

**Operating and Maintenance**
The campus should provide funding to acquire essential software tools for faculty, especially for products that support teaching and learning. Since software costs are ongoing and occur annually, a fixed amount should be allocated to each full-time faculty member each year. Higher software costs for years in which hardware is replaced is mitigated by the inclusion of operating systems and related software in the new system's price. The use of these funds, while limited to software expenses only, could be amassed by several individuals to support the acquisition of licenses that are desired by more than one faculty member, program or department.
- Annual software allowance per full-time permanent instructional faculty - $400, which would equal $550,000 per year based on 1,375 eligible faculty members.

---

9 It was determined through faculty focus groups and individual interviews that approximately $400 would be needed on average for a full-time faculty member to acquire discipline-specific software tools to support teaching and learning activities. Many of these desired tools are unique and of interest to only a few, so economies of scale cannot apply. However, given the current fiscal environment it is not feasible to allocate $400 per faculty member. Rather, a figure of $45 is used to ensure that faculty at the very least have the full Microsoft Office suite (or subsidy of a comparable product).
Personnel
Personnel to design, develop, deploy, maintain, and enhance the license management system is estimated at 1.0 FTE or $60,000\textsuperscript{10} per year including salary, benefits, training, and operating expenses.

Personnel requirements to design, develop, deploy, maintain, and enhance the software management and distribution systems have not been established.

Personnel will be required to coordinate licensing activities; liaise with vendors; distribute software; communicate information to the campus; and provide accounting services. Leverage existing service units, such as the Procurement Service Center, Buffalo Chip, and ITS, which will minimize the personnel requirements.

Funding
Software is essential and increasingly mission-critical for all students, faculty and staff. A combination of institutional funding, student fees, and cost recovery should be identified to provide adequate software tools and to cover the associated administrative expenses. Course fees should be investigated to provide for unusual software expenses associated with specific curricula. Institutional funding would be the preferred means of covering these expenses.

Timing
An initial needs assessment and software inventory should be conducted for the campus in the fall of 2002, followed by the development of a plan to improve software licensing processes and procedures. “Quick win” opportunities should be identified at this time. An assessment of the financial impact of these recommendations should be conducted in AY 2002-03, with funding sources identified for FY 2003-04.

\textsuperscript{10}Salary $41,667/year plus benefits 26% at 100%, professional development and operating expenses $7,500/year.
4.5 Next Generation of Peoplesoft HR and SIS

Recommendation: Minimize impact of proposed Peoplesoft upgrade to the campus technical infrastructure.

An upgrade to the university’s Peoplesoft Human Resources system has been proposed for fiscal year 2003-2004 and is presently under evaluation. Depending upon implementation decisions, the campus should immediately begin consulting with members of the university’s Peoplesoft deployment team to measure possible technical impacts and implement measures to ensure a seamless transition to the new release. The impact of a possible replacement of the university’s Student Information System (SIS) is not addressed in this plan, as there is currently no plan to replace the system within the next four years.

Discussion of the Recommendation

Rationale
An upgrade of the university’s Peoplesoft Human Resource system to release 8.3 would introduce significant functional improvements by offering web-based transactional access. The campus technical infrastructure would be affected in the following areas:

- Campus network traffic – would be significantly increased due to reduced use of Citrix servers and associated data compression. (Citrix would continue to be used for the Financial System).
- Desktops – browser based access to HR system will require standard release levels of browser software. Panel navigation will require training for book-marking panel urls, etc.
- Data interfaces – some modification to campus system interfaces may be required to accommodate revised data interface formats and processes.
- Web-based authentication and authorization – the new release provides a capability for using an LDAP directory for authentication and role based authorization. Integration of these functions with the recently deployed enterprise directory service should be strongly considered.
- Portal interaction – the new release includes an optional functionality for self-update of employee information through a web interface and a portal channel interface. If selected, this option must be integrated with campus portal technical design and development planning considerations.

Specific Recommendations

- Determine technical impact and requirements for integrating Peoplesoft release 8.3 with campus technical infrastructure and planning.
- Develop and fund a Peoplesoft technical integration plan for the campus.

Implementation

- Create core technical team and process for defining project scope and requirements for integration with campus systems and processes.
- Participate in planning processes and provide consulting for Peoplesoft upgrade project.
- Analyze and evaluate alternative approaches to meet requirements for integration with campus systems and processes.
- Design and develop interfaces.
- Provide assistance and support for technical staff in campus departments.
**Communication**
Create a plan to communicate to the campus regarding technical impact of the new release and recommended solutions. Provide a feedback mechanism.

**Policy and Standards**
Develop and publish standard data formatting instructions for campus departmental technical staffs and coordinate issues related to security and common data feeds.

**Required Involvement**

**Governance and Authority**
The Office of the Associate Vice Chancellor of Academic and Campus Technology.

**Required Departmental Involvement and Responsibilities**
- ITS to provide project management, systems analysis and design, software development, training, technical standards, and operation and maintenance of system interfaces.
- University Management Systems (UMS) to provide interface support for these applications.
- Peoplesoft Development team to provide consulting and collaboration on technical issues.
- Campus departmental technical staffs to consult and collaborate on system interface issues.

**Estimated Costs**

**Personnel**
Personnel for technical impact analysis and design, development and implementation needs to be increased by approximately 1 full-time employee (FTE), over a period of one year, which will cost approximately $90,000 (including salaries, benefits, training, travel etc.) to be recovered through recharges.

**Funding**
Funding will likely include a combination of charge-back fees for auxiliary departments system interfaces and institutional funding for general fund departments and campus-wide interfaces. This funding model has been used for previous campus interface development efforts.

**Timing**
A Peoplesoft technical impact initiative for the campus can commence late in fiscal year 2002-2003, but depends upon timing of the upgrade project, which is not decided at this time.
4.6 Web-based Services Infrastructure Strategy

Recommendation: Provide a high-performance, centralized web infrastructure for hosting and managing campus web-based content and services.

CU-Boulder should provide a robust, highly available, fault tolerant, central infrastructure to serve present and future web-based operations and develop solutions for web content management for campus departments, students, faculty, and staff.

Discussion of the Recommendation

Current Situation
CU-Boulder’s web-based infrastructure has grown without attention to comprehensive planning and strategic goals. There is limited campus-wide coordination of development and hosting of web projects. ITS currently provides minimal hardware, software and staffing for hosting institutional, student, faculty, and staff web pages and some departmental web applications. However, a significant number of campus web-based applications and static pages are developed and hosted within individual departments on an ad hoc basis without oversight or coordination. With the proliferation of web content and web-enabled applications, the campus is facing policy-level and technology-related challenges to optimize web-based services. The campus has experienced web service outages in recent months due to limited infrastructure fail-over capability. Increased variety and complexity of content, such as animation, sound, and streaming video in addition to current text files and increasing demands for more advanced website functionality cannot be met by the current campus web infrastructure.

Rationale
A consistent, comprehensive campus web infrastructure is a prerequisite for further development and deployment of campus web-based applications. As the primary source for campus information, web services must be reliable, robust, and always available. As an institutional asset, campus web content should be managed and controlled in a manner that ensures the integrity of the content creation process. In addition to providing browser-based content administration tools, version control, and workflow capability, a good content management solution separates the development and deployment environments employing at a minimum, two physical servers – one for development where content is created and structured, and one for deployment, from which content is served. A central web infrastructure, utilizing content management and available campus-wide, would provide a secure and efficient operating environment for developing and supporting campus web-based applications. Adopting a web content management strategy and common security processes would improve consistency and currency of campus web-based information; reduce web development costs; enable the implementation of campus-wide security services utilizing the campus’ Enterprise Directory; and realize benefits from standard practices, shared costs, and increased quality of data.

Specific Recommendations Include

- Restructure the current central web-based infrastructure to improve performance, improve fail-over capability, improve manageability of content, and enhance security.
- Fund the development and maintenance of central web-based services to provide robust production level capabilities and staffing to meet necessary service levels for current and future campus needs.
• Fund and implement web content management hardware and software for a phased implementation of campus-wide access and distributed administration of central web-based content.
• Develop a program of operational excellence for supporting web-based services to meet campus departmental business needs, ensure customer satisfaction, and achieve the results required for mission-critical web sites.

**Steps**

**Implementation**

• Review and analyze components of the current web-based services infrastructure to determine approaches for rationalizing and stabilizing the current hardware and software platforms, addressing security issues and web content issues, implementing web site monitoring, adopting management tools, and developing and implementing policies and procedures.
• Develop a phased implementation plan and deploy a flexible, robust, comprehensive central web-based infrastructure, utilizing standard reference architectures, to provide web hosting for the campus. Adopt an operational excellence approach to meet the desired level of service and support.
• Develop a forecast of web-based access demand for a central infrastructure for the next three years including known and pending web application deployments, departmental web sites, opportunities for consolidation of web infrastructure, and growth in demand for higher bandwidth web services such as multi-media content.
• Analyze campus content components, investigate various content management alternatives, develop an implementation plan, and deploy a campus-wide web content management solution.

**Communication**

Create a plan to communicate to the campus regarding the deployment of campus-wide web-based services. Solicit feedback from campus departmental web administrators from early planning through implementation.

**Policy and Standards**

Establish and implement policy and technical standards for web-based services encompassing mandatory and recommended practices, technical services, and content management. Policies and standards should reflect differing business needs and privacy and security requirements presented by separate web spaces such as public, student, departmental, and intra-campus.

**Governance and Authority**

The Office of the Associate Vice Chancellor for Academic and Campus Technology.

**Required Departmental Involvement & Responsibility**

• ITS to design, implement, maintain, operate, and manage the central web-based services infrastructure.
• Web Communications to collaborate on web policy, best practices, selection, and deployment of web content management software and infrastructure design issues.
• Campus departments to collaborate on design, support requirements, web site monitoring and distributed content management.
• University Management Systems (UMS) to collaborate on design and content management issues.
• Committee on Electronic Communications to provide policy oversight.
• IT Council to provide guidance and programmatic direction.
Expected Costs

**Annual IT infrastructure Investment**

New costs

Infrastructure costs necessary to deploy a fully fault tolerant operating environment to ensure business continuity in the event of a disaster include: web server hardware and software, application server hardware and software, database hardware and software, network hardware and software and redundant power supplies. These costs are estimated to be $200,000 with annual costs estimated to be $40,000 per year.

Infrastructure costs necessary to create a production level central web service, provide the necessary content management capability and development platform include: web content management hardware and software, content development and staging hardware, and web site monitoring tools. These costs are estimated to be $250,000 with annual costs estimated to be $50,000 per year.

**Personnel**

New costs

Personnel for deploying, maintaining and supporting a production level central web service needs to be increased by two full-time employees (FTE), which will cost approximately $180,000 (including salaries, benefits, training, travel, etc).

**Funding**

Funding for creating a fully fault tolerant operating environment should be provided by general fund with re-allocation within ITS budget as necessary. Funding for web content management and central web production services will require a combination of general fund support for core services with recharge for specific departmental services as appropriate.

**Timing**

Development and deployment of a fault tolerant, fail-over campus web infrastructure should have high priority and begin early in 2002-2003. The development and deployment of web content management and central web production services should begin late in fiscal year 2002-2003.
4.7 Assistive Technology and Accessibility

Recommendation: Continue to provide access to assistive technology facilities and technology support for individuals with disabilities. Work to ensure the accessibility of all technology and information resources on campus.

Discussion of the Recommendation

Current Situation
Currently, students access assistive technology (AT) on campus at one of five satellite stations or at the central Assistive Technology Lab on the third floor of Willard. The AT Lab is operated and staffed by Disability Services (DS). Assistive technology satellite stations are jointly run by DS and ITS. Other labs on campus are minimally accessible (e.g., adjustable tables, operating system level accessibility tools, etc.). Support for the satellite stations is neither well coordinated nor provided by on-site ITS support staff or advisors, which often results in unnecessary downtime for the stations.

Disability Services and the AT lab provide some individualized assistance to students with disabilities, including a limited laptop loan program and some “help at home,” made possible by a special fund of money.

The Web Publishing Policy specifies “all electronic publications, to the extent feasible, must be made accessible to people with disabilities.” For several years, ITS and Disability Services have offered brown bag seminars on “Making Web Pages Accessible to People with Disabilities.” In 2001, the campus developed “Creating Accessible Web Pages,” a web site with resources and guidelines for campus web developers, and offered special workshops for IT staff that work with faculty. In addition, Web Communications is currently working with UMS to improve the accessibility of web registration. The new design of the CU-Boulder web site was developed to meet accessibility standards, and templates that meet the standards are available for web developers. As the new design is implemented, the percentage of accessible pages is increasing. However, much work remains to raise awareness among campus web developers and to improve the accessibility of campus information resources for people with disabilities.

Rationale
Through implementation of the recommendations below, the campus should take the next steps of integrating the satellite stations into the ITS support system and of integrating AT software into the labs on campus. The result would be significantly greater AT access for students with disabilities; improved repair and support of assistive technology on campus; and less duplication of effort by integrating AT into the existing ITS and ITS Support Center structure.

By implementing the recommendations below, the campus will ensure equitable access to its information and IT resources.

Specific Recommendations
CU-Boulder should continue to provide assistive technology facilities and support throughout the campus for individuals with disabilities both in the AT lab, as well as at existing satellite stations around campus. The AT Lab should work with ITS to develop and monitor standards for ensuring the accessibility of all labs. The campus should improve the support available to assistive technology satellite stations. The campus should continue to provide some individualized assistance to students with disabilities (e.g., laptop loans, etc.). The campus should expand
policies and develop communication plans to ensure the accessibility of campus information resources, such as web pages and web-based services.

Continue to fund and support the AT Lab and satellite stations (Disability Services [DS])
- Continue to provide dedicated space for student assistive technology stations in the AT Lab.
- Provide dedicated space for alternate formatting (e.g., brailling), preferably removed from the student workspace.
- Maintain the existing stand-alone adaptive stations in Norlin N310 and in Muenzinger and continue to assess usage statistics to determine need for these stations. Maintain three other satellite stations (Norlin Reference, Engineering, and Law).

Ensure accessibility of all labs (DS and ITS)
- Include AT software as part of the ITS loadset for ITS labs (e.g., screenreader, screen enlargement, and OCR/reading software for learning and visual disabilities).
- Continue the practice of adding at least one adjustable station in each ITS lab as labs are renovated.

Ensure that students have access to audio capabilities in all labs, through the long-term loan of headsets or short-term checkout of headsets in ITS labs with advisors.
- DS and ITS should work together to develop a procedure for accommodating students with disabilities in instructional facilities.
- Disability Services, the AT Lab, and ITS should work together to establish and communicate best practices for making departmental labs and classrooms accessible.
- DS and ITS should determine the best way to provide distributed scanning services to students with disabilities.
- DS and ITS should investigate and implement a method for making the IdentiKey prompt more user-friendly for vision-impaired users.

Improve support to satellite stations
- Integrate support of AT satellite stations into ITS 4-Tiered IT support model by:
  o Providing training to the ITS Service Center and Bug Buster advisors so they can provide broad support for existing adaptive satellite stations.
  o Integrating assistive technology support into ITS workflow system.
  o Making the AT Lab a Tier 4, core expert partner to handle escalated assistive technology cases.

Continue individualized assistance
- Continue and enhance the AT Lab loan of laptops with adaptive software to students with disabilities as needed.
- Explore the possibility of providing “help-at-home,” and work with other campus support services such as ResNet and the ITS Service Center to coordinate student support in residence halls or other locations.

Ensure accessibility of campus information resources
- Coordinate and expand efforts to provide training and resources on creating accessible web pages.
- Include accessibility in the criteria for evaluating upgrades to online student services and academic resources, such as WebCT, the campus portal, SIS, and PeopleSoft.
- Initiate the development and implementation of an expanded web accessibility policy by preparing a Briefing for the Vice Chancellor for Student Affairs (as recommended by the Office of Diversity and Equity).
- Address resource needs (staff, training, and communication) as part of the briefing.
Steps

Implementation

- Obtain, test, and pilot adaptive software and keyserver technology in ITS lab loadsets.
- Develop a model for improving audio capabilities in ITS labs.
- Establish best practices for ITS and departmental labs.
- Monitor usage of satellite stations.
- Research models for distributed scanning services for students with disabilities.
- Develop a training program for ITS Advisors and help desk and implement.
- Develop a service level agreement between ITS and the AT Lab.

Development of the Web Accessibility Briefing

- Research applicable laws and accessibility policies at other universities.
- Assess the accessibility of campus web-based information resources
- Prepare a proposal for the CU-Boulder that includes:
  - Issues and opportunities.
  - Special needs for online student services and academic resources.
  - Definition of standards.
  - Resource needs: staff, training, and communication.
  - Proposed model for coordination with the UMS.
  - A proposed implementation plan.
  - Timeline and priorities for implementation.

Required Involvement

Governance & Authority
Office of the Associate Vice Chancellor for Academic and Campus Technology.

Required Departmental Involvement & Responsibilities

- Disability Services
  - Provide AT training for ITS Service Center.
  - Continue to work on AT Lab, Satellite stations, laptop loan program, and “help-at-home” possibilities.
  - Work with ITS on lab accessibility best practices, program for widespread AT software in ITS labs, audio accessibility in ITS labs, exploring distributed scanning services, and developing a procedure for accessibility accommodations.

- ITS
  - Work with DS on lab accessibility best practices, program for widespread AT software in ITS labs, audio accessibility in ITS labs, exploring distributed scanning services, and developing a procedure for accessibility accommodations.
  - Work to integrate the AT lab into ITS workflow system as a Tier 4 Core Expert in the field of IT accessibility, including an SLA between the groups.

- Office of Diversity and Equity
  - Provide leadership, coordination, and possibly funding for the development and communication of guidelines, policy, and training opportunities to ensure the accessibility of information and IT resources across campus, including web-based student services and academic resources.

- University Communications
  - In conjunction with the Office of Diversity and Equity and the Office of the Associate Vice Chancellor for Academic and Campus Technology, develop and
communicate guidelines, policy, and training opportunities to ensure the accessibility of information and information technology resources.

- Instructional Computing Working Group (ICWG) for discussions about ITS student-fee funded labs.

**Expected Costs**

**Annual IT Infrastructure Investment**
Establishing AT software in ITS labs program
KeyServer software for ITS labs - $18,250 (new cost)
KeyServer hardware - $7,000 (new cost)
AT software (10 licenses of each) - $12,000 (new cost)
Total one time costs - $37,250

**Operating and Maintenance**
Annual maintenance cost of KeyServer software - $3,300 (new cost)
Annual cost of replacement cycle for satellite stations - $1,500 (existing)
Annual cost of headphone loan program - $500 (new cost)

**Personnel**
- 0.25-0.50 FTE for integration of AT software into ITS loadsets (new cost)
- 0.10–0.20 FTE AT-Lab costs for upgrading and servicing 5 Satellite stations (existing)

**Funding**
Funding for the continued operation and the renewal and replacement of satellite labs should come from ICWG funds as in previous years. The campus needs to look into alternate sources of funding for integration of AT software into ITS labs. Possible sources include ICWG as well as Disability Services or Office of Diversity and Equity.

Funding for the distributed AT software and headphone loan programs should be obtained from ICWG due to their availability in open student facilities.

Disability Services currently funds support for Satellite Stations and should continue to provide that support.

Funding for the .25 - .50 FTE for personnel for integration of AT software possibly could be absorbed by ITS.

The Web Accessibility Briefing will investigate further funding requirements.

**Timing**
- Begin integrating greater AT support into the campus IT support system with the goal of having Tier 3 AT support provided by ITS and Tier 4 AT support provided by DS by fall 2003.
- Develop a procedure for accommodating accessibility needs in ITS facilities by spring semester 2003.
- Develop and implement campus policies regarding information and information technology accessibility by fall of 2003.
- Begin work on widespread AT software availability in ITS computing facilities with a goal of a pilot program by spring semester 2003 and widespread use by fall semester 2003.
- Develop a plan for distributed scanning services for students by fall 2003 with an implementation goal of fall 2004.
- The Web Accessibility Briefing will be developed in fall 2002.
4.8 File Systems

**Recommendation:** Provide a robust, highly available campus-wide file storage, access, management, backup and retrieval system.

**Discussion of the Recommendation**

**Current Situation**
A wide variety of file storage systems exist on campus. Very limited storage, typically 5 – 20 MB, is available on centrally-provided servers for student, faculty, and staff web pages. Space is also available on central systems for departmental uses, though it is constrained by available capacity. Other central servers are available for limited multimedia applications and centrally provided email.

Computing lab workstations have no persistent storage available natively. Students in particular are highly mobile, using a variety of platforms both on- and off-campus. To have access to their electronic materials from anywhere, students must rely on removable media or email, neither of which can easily accommodate large quantities of data or facilitate sharing. Complex tools are required for all constituents to move files from local desktop or lab systems to central servers. Group collaboration can be challenging, with the need to understand file ownership and permissions and often relies upon insecure sharing of a group account. Backups of central systems are performed to recover from catastrophic failure but retrieving individual files is performed in an on-demand, fee-based manner and is awkward and slow.

Many departments have private servers but must invest considerable resources in both hardware and personnel to deliver security and availability. Other departments, due to lack of financial resources or sufficient technology proficiency, have no access to even basic file sharing and fallback on email and even floppy diskette transfer to exchange data.

**Rationale**
Supporting coursework, creative endeavors, and collaboration requires adequate data storage, typically far in excess of what is now routinely available. Capacity that is considered modest on an inexpensive desktop computer is still considered extravagant when provided centrally. Collaborative projects among and between students and faculty demand storage availability and tools to manage ownership, permissions and file transfer and to ensure version integrity is maintained between edit cycles. The lifecycle of storage must extend beyond semester boundaries as students accumulate coursework and faculty build portfolios. Highly mobile constituents should be able to use a public access kiosk, a computing lab workstation, or their own laptop or desktop workstation to gain easy access to their files.

Departments have both similar and different needs. Individuals need adequate capacity to store administrative data, though their capacity requirements are typically less than in the academic area. Like faculty and students, they need to collaborate electronically with colleagues using tools that facilitate file transfer as well as sharing functions such as ownership and permissions. Departmental needs differ in that they may also require substantial capacity for databases and archival of scanned text or workflow processing. Security of data may be a serious consideration for departments that have responsibility for secure or critical data.

No online system is effectively maintained unless backup procedures take into consideration needs for recovering from catastrophic loss as well as more routine unintended file deletion. Data of high importance should be backed up both on-site for easy retrieval and also stored in a remote location geographically separated from the primary storage facility.
Efficiencies may be realized when needs for storage across campus are considered in a comprehensive manner. Though storage needs and uses may be different, a network accessible file system infrastructure could provide high capacity and availability for typical applications such as web pages, databases, multimedia, and administrative data. However, certain segments of the campus community, such as Libraries with their impending massive digital library collections, may be outside the scope of a widespread storage solution.

**Specific Recommendations Include**

- Develop and deploy an institutional file system (IFS\textsuperscript{11}) providing significant storage space to all students, faculty, and departments\textsuperscript{12}; space will be accessible through designated central campus servers. The IFS should be compliant with campus authentication and authorization strategies.
- Implement platform-neutral\textsuperscript{13} methodology to enable users on all supported campus platforms to:
  - Easily transfer files between the desktop and IFS.
  - Specify individuals and groups who should have access.
- Ultimately implement a platform-independent\textsuperscript{14} web-based system to:
  - Transfer and manage files and ownership.
  - Enable project collaboration by controlling versions.
- Investigate the feasibility of providing centralized, user-controlled backup and retrieval services for the IFS. Consider extending the service to departmental servers.
- Leverage the knowledge gained in developing a campus-wide storage architecture to explore solutions for large scale initiatives such as Libraries’ digital collections.

**Steps**

**Implementation**

- Determine requirements for adequate storage space and features for students, faculty, and departments; requirements may be discipline- or departmental-specific.
- Acquire appropriate storage system and server infrastructure, including backup subsystems, to provide storage access to campus-supported platforms\textsuperscript{15} using campus standards-based authentication integrated with the Enterprise Directory.
- Further investigate web-based storage management tools to enable platform-independent shared access to files.
- Investigate solutions for institutional backup and retrieval systems that integrate with an institutional file system. Evaluate the feasibility of providing such services beyond the central IFS.
- Investigate web-based solutions to enable platform-independent versioning and content management.

**Communication**

- Partner with campus IT providers and support personnel to help them leverage a centrally provided IFS to better meet their constituents’ needs.
- Use appropriate channels such as campus web presence, constituent group meetings, ememos, and print advertising to communicate availability of services.

---

\textsuperscript{11} IFS – Institutional File System.
\textsuperscript{12} Fee-based for departments.
\textsuperscript{13} Platform-neutral: same basic feature set available from supported computing platforms, though interface and advanced features may vary slightly from one to another.
\textsuperscript{14} Platform-independent: same user interface on any of the supported computing platforms.
\textsuperscript{15} Campus-supported platforms currently include Windows 98, NT, 2000; Macintosh OS 9 and X; Solaris; and soon will include FreeBSD and redhat linux.
Policy & Standards

- Develop guidelines and best practices for efficient and effective storage and sharing of files.
- Develop best practices for the management and backup of campus file servers.

Required Involvement

Governance & Authority
The Office of the Associate Vice Chancellor for Campus and Academic Technology.

Required Departmental Involvement & Responsibilities

- IT Council to provide guidance and programmatic direction.
- ITS to develop and promote best practices in cooperation with departmental file server providers.
- ITS to design, maintain, operate and manage the central IFS.
- ITS to partner with faculty and academic technology representatives and coordinators to develop tools and methods for file sharing.
- ITS and Student leadership to assess needs and develop training and usage strategies.

Expected Costs

Annual IT Infrastructure Investment
Costs include hardware and software needed to deploy a fault tolerant operating environment, including the central IFS, basic backup subsystems, redundant power environment, and software. Additional costs will be incurred to provide redundancy of file arrays, network switches, network file server; and further costs will be incurred for an automated backup/retrieval system.

One-time costs:
- Implement the basic infrastructure of storage arrays and platform-neutral file servers to create a central IFS. Include a basic backup subsystem and configure with capacity to provide disk capacity of 100 MB/individual for students (assume 26,000 FTE) and 100 MB/individual for faculty/instructors (assume 2000 FTE) - $330,000 plus $100,000 for basic backup capability.
- Provide disk capacity for departmental use with costs fully recovered through fee for service - $100,000 for 1,000 GB (1 TB).
- Expand disk capacity as demand warrants - $100,000 for 1,000 GB (1 TB).
- Enhance infrastructure by adding additional redundancy of fiber switches and network file servers - $300,000.
- Develop and implement a web-based file access solution with versioning and content management – costs cannot be estimated at this time.

Operating and Maintenance
On-going costs:
Renewal and replacement should be budgeted at 25%/year (4 year replacement cycle). Hardware/software maintenance is budgeted at 10%/year and small capital improvements are budgeted at 10%/year.
- Disk capacity for departments (costs recovered through fees) - $45,000/year.
Cost savings:
Departments that choose to use centralized file systems instead of providing their own server could realize annual savings of $7,000 – 20,000/year currently expended on hardware and software acquisition, renewal and replacement, and maintenance. Personnel savings of 0.2 FTE per server could also be realized.

**Personnel**
- Design and implementation of basic infrastructure – 0.5 FTE for two months. Existing within ITS.
- Design and implementation of automated backup and retrieval system – 0.5 FTE for four months. Existing within ITS.
- Investigation of web-based versioning and content management systems – 0.5 FTE for two months. Existing within ITS.

**Funding**
Basic infrastructure:
- Use a one-time reallocation of student computing fee to pay for the basic infrastructure serving students and faculty - $16.50/student (assume 26,000 students).
- Continuing reallocation of student fee to fund on-going costs - $3.75/semester/student.

Departmental file services:
- Perform cost analysis, provide on at-cost basis. Expect fees of approximately $120/year/200 MB.

**Timing**
A basic institutional file system with 100 MB of storage for all students should be deployed for spring Semester 2003. Capacity for faculty early adopters should be part of the initial deployment for spring Semester 2003. As usage grows, additional capacity for faculty and student use and collaboration should be added along with enhanced redundancy. A pilot service to provide file services for departments should be implemented in CY 2003 and expanded in scope as the service is developed. Web versioning and content management should be explored in AY 2002-2003 with target implementation of fall Semester 2003.
4.9 Application Standards and Best Practices

Recommendation: Provide application development guidelines, best practices, and technical review process for campus administrative systems initiatives.

Develop baseline campus technical standards for the purchase and/or “in-house” development of administrative computer applications. Develop, publish, and keep current “best practices” for the purchase and/or development and integration of campus applications with core campus technical architecture and maintenance and support of deployed applications. Establish a centralized review process to ensure adherence of campus application initiatives with campus best practices and technical guidelines. Create a web-based application certification process for publishing and hosting web applications through the campus’ institutional web sites.

Discussion of the Recommendation

Current Situation
The development and implementation of campus administrative systems and web-based applications is being done in an uncoordinated, inconsistent manner without benefit of technical oversight to ensure compliance with the campus technical infrastructure or well established best practices for software development. Because there is no unifying technical development oversight and coordination, campus departments may not utilize a systems development methodology to define and understand requirements before acquiring or developing applications. Departments may rely solely on advice from software vendors for purchasing software or departmental staff for in-house development to address complex technical issues without campus assistance. Without guidelines, issues such as integration with central and campus systems, authentication and authorization, directory services integration, database requirements, data conversion, software licensing, privacy, and legal liability may not be adequately addressed. Software applications developed and implemented in this environment cost more to implement, maintain, and support than software that has been developed using standard development methodology and completed systems often fail to meet campus’ technical requirements.

Rationale
Campus application developers and technical staff can benefit from the use of common standardized technical approaches, guidelines, and best practices for application development. Development costs can be reduced, applications can better interoperate and integrate with the campus infrastructure, data quality, and security can be improved and common development techniques can be shared across campus. Implementation, presently underway by the campus, of an Enterprise Directory services infrastructure and recent campus security initiatives provide an important technical foundation that should be leveraged to unify future campus application development efforts. The deployment of a web-based portal infrastructure is under consideration and if implemented will require that standard development techniques be used to certify that web-application or content to be presented or published, through the portal, meet technical requirements.
Specific Recommendations Include

- Develop and publish a set of technical guidelines, best practices, and policies to ensure that adequate systems development methodologies are employed in the acquisition or development of campus administrative applications.
- Develop and publish a set of technical guidelines, best practices and policies for the utilization of campus-wide directory services, authentication and authorization, database standards and data administration to ensure that campus technical development and integration requirements can be met by departmental administrative applications.
- Develop and implement a technical review process to encourage compliance with guidelines, best practices and policies for administrative application acquisition and/or development.

Steps

Implementation

- Create a campus-wide core technical team and process for defining and maintaining an administrative application development methodology, technical guidelines, best practices and policy recommendations.
- Create and fund a plan for the implementation of application development platform and tool standards.
- Create and fund an application integration position within ITS to provide campus-wide integration and coordination between departmental applications and campus technical infrastructure.
- Establish and fund a campus-wide administrative application review process.

Communication

Create and fund a plan to communicate to the campus regarding technical guidelines, best practices, policies and processes.

Policy and Standards

- Create a policy to ensure that administrative systems and applications acquired or developed meet departmental functional requirements and comply with campus technical infrastructure requirements.
- Establish technical standards for application development and integration.

Required Involvement

Governance and Authority

The Office of the Associate Vice Chancellor for Academic and Campus Technology and the IT Council. Policies and standards will be brought before the IT Council and the voting members will be responsible for reviewing proposed standards.

Required Departmental Involvement and Responsibility

- Campus departments as IT providers to provide technical collaboration and consulting in defining and developing guidelines and to adopt resulting guidelines, processes and standards.
- ITS to provide technical leadership, collaboration and consulting in the development and maintenance of guidelines, policies, processes and standards.
Expected Costs

Annual IT Infrastructure Investment (new)
Infrastructure costs include acquisition and deployment of campus-wide standard application development platforms and tools. These costs are estimated to be $120,000 with annual costs estimated to be $20,000.

Personnel (new)
Personnel for project management, departmental liaison, application review process administration and application platform administration needs to increase by 1 full-time employee (FTE), which will cost approximately $90,000 annually.

Funding
This should be provided as a core campus service funded by institutional funding for acquiring, deploying, and supporting standard application platforms and tools, and creating and administering applications standards and a review process.

Timing
The initiative should begin early in fiscal year 2002-2003.
4.10 Four-Tier Support Model

Recommendation: Provide best-in-class IT support to the campus community through the Four-Tier Support Model.

The Four Tier Support Model is an effective model for providing IT support to the CU-Boulder campus and in the next four years we should continue to 1) move support even closer to the customer and 2) strengthen the internal infrastructure within the Four Tier Support Model.

Discussion of the Recommendation

Current Situation
The elements of the Four-Tier Support Model: communication, training, self help, distributed, centralized, and core experts, are deployed and have been adopted by the campus at large as the appropriate structure through which IT Support is delivered. The distributed or second tier of the Four-Tier Support Model comprises in-house IT support staff in each campus department and provides a vital mechanism for communication and service integration between ITS and all units on campus. Although deployed, the quality and quantity of IT support delivered through the elements of the model can be improved through refinement of communication and by moving the delivery of support as close as is practical to the customer.

Rationale
As the campus grows and becomes increasingly dependent upon IT resources, so also grows the demand for fast, efficient and robust IT support. In order to meet this demand with best-in-class IT support, the delivery of that support must be easy to find, easy to use, and must leverage the entire support community of ITS and departmental staff.

Specific Recommendations for Item 1) Include

- Develop Educational Technology Facilities Support (ETFS) for classrooms, labs, team rooms and assistive technology stations.
- Leverage the success of the Tier 2 program by further developing liaison relationships within departments for educational technology facilities and web resources.
- Continue to move support closer to the end-user by dedicating Desktop Support resources to the schools and colleges.
- Develop IT support teams within the schools and colleges consisting of Distributed Academic Technology Coordinators, Desktop Support Technicians, and Educational Technology Facility Support Technicians. These teams will work alongside the existing Tier 2 resources in each area.
- Expand and improve Tier 1 self help to be a more effective resource for ITS and our customers through a dedicated Tier 1 web support position, a natural language searchable knowledgebase, Frequently Asked Questions for all products and services, and the addition of a dedicated knowledge management position.
- Establish a fee-based Server Administration Service for non-UNIX (Windows and Apple) platforms.
- Increase and improve communication both internal and external to the support model.
Specific Recommendations for Item 2) Include

- Review Clarify as a workflow tool, ensure renewal and replacement costs for a workflow tool, and manage the expectations of what any workflow tool can provide to customers both internal and external to ITS.
- Improve reporting and trend analysis on data collected through the support model.
- Advertise and promote training that already exists and new training opportunities as they are developed. This includes creating a Faculty/Staff Trainer position within ITS to provide a delivery mechanism to the faculty and staff, to improve existing training materials, and to develop new training curriculums.

Steps

Implementation

- Recommendation 1) will require: Combine the resources of the existing Classroom Support, Site Support and Lab Advising programs and redistribute these resources into the schools and colleges to provide Educational Technology Facilities Support. Continue to build relationships with departments by establishing Tier 2 entities for educational technology facilities, web resources and hiring a Telecommunications Liaison Coordinator. Fund, hire and/or purchase a Tier 1 web resources manager, a web content management tool, a knowledgebase manager, and a natural language searchable knowledgebase. Establish an auxiliary or add to an existing auxiliary to provide server administration services on a self-funded basis.
- Recommendation 2) will require: Establish funding for the renewal and replacement of the workflow tool and then reevaluate the workflow products available and the option of writing a custom application. Improve data collection opportunities, provide trend analysis, and distribute this information throughout the support community. Fund and hire a faculty and staff trainer and more heavily promote new and existing training opportunities. Fund and hire a position to support the use of database applications by the faculty in their research and in their curriculums.

Required Involvement

Governance & Authority
ITS is the owner for both recommendations in this initiative.

Required Departmental Involvement & Responsibilities

- ITS to provide leadership, direction, and communication for all elements of the Four-Tier Support Model.
- Schools, Colleges, and Departments to provide guidance on their IT support needs, input to the IT support teams serving their customers, supervision of Tier 2 personnel, funding as a partner on appropriate initiatives, and feedback on the support process to ensure that Four-Tier Support Model is achieving the greatest efficiency possible.

Expected Costs

Annual IT Infrastructure Investment

- Workflow tool replacement (existing)- $350,000
- Natural language searchable knowledgebase (new) - $75,000
- Web Content Management tool (new)- $35,000

Operating and Maintenance

- Workflow tool renewal (existing)- $70,000
• Natural language searchable knowledgebase (new) - $15,000
• Web Content Management (new) - $7,000
Operating and Training funds for five new personnel (new) - $30,000

**Personnel**
- Web Resources Manager (new) – Programmer Analyst I - $52,000
- Faculty and Staff Trainer (new) – IT Professional I - $52,000
- Database Application Support (new) – IT Professional III - $62,000
- Knowledgebase Manager (new) – IT Professional I - $52,000
- Communications Liaison Coordinator (new) – General Professional III - $48,000

**Funding**
Funding will include a combination of 1) the redistribution of existing ITS resources; 2) contributions on a one-to-one ratio by schools/colleges and ITS to the deployment of the Desktop Support Technicians; 3) development of for fee services such as server administration support; 4) an internal ITS recharge mechanism for establishing a fund for the renewal and replacement costs of the workflow tool; and 5) requesting continuing funds for purchasing a knowledgebase, purchasing a web content management tool and for staff positions that are not reallocated from existing resources.

**Timing**
Enhancements to the Four-Tier Support Model are in progress and will continue to be pursued through the life of the IT Strategic Plan.