BEST PRACTICES, IRM

Title: Business & Finance Computer Rolldown Process   **#**   9

Source: University of Memphis   **Co Area:**

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2004.html

Abstract: With over 400 computers to track and assign to staff, the Division of Business and Finance at The University of Memphis faced a daunting task when attempting to develop a plan to ensure that staff members have a computer system that meets job requirements. To help with this, the office of Business & Finance Technology (BFT) developed a computer rolldown process that includes a user needs assessment, the definition of computer configurations for each requirement level, and assigning user positions appropriately.

BFT has unveiled a Web site to enable users to search for information about the systems involved in the rolldown. This Web application uses an Access database, an ODBC connection, Crystal Reports, JavaScript, and a Web browser. Searches can be performed either by department or by rolldown number. These searches provide users with an easy way to track workstations by assigned user, serial number, department code, processor speed, and much more.

This project ensures that every member of the Division has adequate equipment to do his/her job effectively. A significant amount of money has been saved in the process of purchasing and assigning computers where they will benefit the Division. This Web site can be accessed at http://bf.memphis.edu/bftech/rolldown/roll.php.

Title: Information Technology Web-Based Ordering Tracking System   **#**   15

Source: University of Memphis   **Co Area:**

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2004.html

Abstract: The University of Memphis' Information Technology Division (ITD), Department of Client Support Services, assumed campus-wide responsibility for the procurement, distribution, and tracking of all information technology related purchases paid for by student technology access fees (TAF). With over 2500 equipment purchases annually, the IT Division at The University of Memphis faced a daunting task to assure timely purchases, delivery, and installation of goods. These multi-million dollar annual expenditures for hardware and software are subjected to an annual audit and must be traceable from purchase to declaration of salvage. The Information Technology Division developed a web-based equipment order tracking system which has resulted in improved client service and which compliments the campus' fixed asset and billing systems.

BEST PRACTICES, IRM

Title: Implementing Business Continuity on a Shoestring   **#** 129

Source: University of North Carolina   *Co Area:*

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2005.html

Abstract: The University of North Carolina at Wilmington is in the eye of many storms or so it would seem. Since 1996, Bertha, Fran, Bonnie, Dennis, Floyd, Kyle, and Charley have passed within 60 nautical miles and the main campus of UNCW which lies less than seven miles from the coast. In this environment you really don't want all your datacenter eggs in one basket. The Business Affairs Division has worked proactively to provide warm backup site for their systems, within a budget using off the shelf technology, to provide better data redundancy and system continuity.

The most important factors in building this system were place and space. We needed a place, somewhere geographically separate, affordable, with limited physical access, sufficient cooling, power, and high speed network connectivity to locate some servers as well as needing affordable, sufficient, and network available disk space to store all the data and applications. We also needed processing power and the ability to effectively have a system masquerade as another on the network. Finally, we needed the ability to copy data and to schedule when the copies would occur. This all had to occur, within our yearly server budget of $25K.

Title: Identity and Access Management   **#** 160

Source: Oklahoma State University   *Co Area:*

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2003.html

Abstract: Managing identities and authorities is a major component to an information technology infrastructure. Knowing who some is and what authorities they have are vital to the system use and security. Keeping the information in sync within all the systems can be a time consuming and very labor intensive operation. Computing & Information Services at Oklahoma State University developed a universal directory of core identity and access information. The Universal Directory becomes the hub for identity and access updates, which then passes the information to systems managed by CIS. By implementing this infrastructure, CIS will improve the time to provide access system, update the information across all systems simultaneously and reduce the overhead in maintaining identities.

BEST PRACTICES, IRM

Title: Implementing a Project Management Office **#** 161

Source: Oklahoma State University *Co Area:*

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2003.html

Abstract: As information technology projects became more cross-functional in nature, Oklahoma State University's Computing & Information Services (CIS) looked to managing projects from end to end in a consistent manner. Each area in CIS was managing their part of the project, but communication and coordination across the areas did not always go well. To help improve communication, coordination and successful project outcomes, CIS implemented a Project Management Office (PMO). CIS looks to the PMO to provide project management expertise on critical projects, cross-functional projects or single area projects. The PMO has developed a mission, goals, short-term objectives and long term objectives, which tie into the CIS goals and objectives. The PMO focuses on managing the project using a consistent methodology. To improve on the project management methodology, the PMO evaluates each project to outline lessons learned for future methodology modifications. The information from these projects along with other project management reference material is housed in a repository, which is available for departmental use. Also, to improve project management techniques, a training plan for project managers has been developed along with curriculum for project sponsors and project team members.

By managing projects in a consistent manner, the PMO is improving scheduling, communication, and successful outcomes from these projects.

BEST PRACTICES, IRM

Title: In-Service Training Program   **#**   172

Source: University of Arkansas   *Co Area:* Registrar's Office

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2003.html

Abstract: In-Service Training is a web application that offers staff of the University of Arkansas Cooperative Extension Service classes that advance skills and meet continuing education requirements. A student can review all courses offered; enroll in available classes; drop approved or pending classes. Once approved by the supervisor, a class is automatically placed on the student's GroupWise calendar. Instructors can review the names of students who have enrolled in their courses. They can also send emails to their students and submit class attendance reports.

Supervisors can approve or disapprove course requests and see the schedules of all students who work under their immediate supervision.

The program administrator can update course offerings by
* Correcting class listings in the database
* Removing a class from the database
* Adding a class to the database

The administrator can also generate reports for
* All or individual student schedules
* All or individual instructor schedules
* District participation

Special administrative privileges include
* Adding a student directly to a class, even if the class is closed
* Removing a student from a class
* Approving or disapproving of a pending class request

BEST PRACTICES, IRM

Title: Implementation of TMA Enterprise and Interface to PeopleSoft   **#**   186

Source: University of Southern Mississippi   **Co Area:**

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2003.html

Abstract: In 2002, the University of Southern Mississippi implemented TMA Enterprise (computerized maintenance management software) and created an interface to the PeopleSoft general ledger package. This interface eliminated the manual processing of Physical Plant, Central Stores, Housing Maintenance, and Science Stores charges.

Before the interface, chargeable work orders were printed from TMA and the data was manually entered into PeopleSoft. Duplicate data entry presented an opportunity for errors and required a reconciliation of the information in PeopleSoft and TMA. Another enhancement provided by the interface is that Stores charges, previously billed separately, are now billed directly on the work order through the interface. This allows Physical Plant customers to see all of the charges for a work order in one place. Prior to the interface, customers received a bill from Stores for materials and a bill from Physical Plant for labor and contractual services. Tremendous efficiency has been realized with the advent of this interface.

The TMA system also provides a much higher level of customer service. It allows customers to enter their work requests on-line. Once the work request is received, an email response is sent with a work order number that allows them to enter to monitor the progress of the work. Customers can query requests via the web to search on criteria for work performed. Additionally, a customer service evaluation is sent on an incremental basis to monitor customer satisfaction.

This interface, that required a collaborative effort among several departments, has improved efficiency and enhanced customer service for the entire campus. Customers now have on-line access to charges and the amount of staff time and effort to provide accurate billing has been greatly reduced.

BEST PRACTICES, IRM

Title: InTouch Kiosk System **#** 237

Source: Sinclair Community College *Co Area:*

Addl Info: http://www.educause.edu/995/1274

Abstract: The InTouch Kiosk System can be described as a one-stop shopping center for Sinclair information and academic advising services. At any of thirteen locations on the Sinclair campus, a student can make a quick stop at a touch-screen kiosk to print his/her class schedule and/or transcript, search a database of scholarships, look for a part-time (off campus) job, find an open section of ENG 113, check out the price of a used text book for BIO 211, and consult with an expert system about Sinclair's degree programs, e.g., Allied Health. Each month, the InTouch system handles about 22,000 transactions.

When Sinclair first initiated this project in the summer of 1990, touch-screen kiosks were unknown in higher education. However, the idea of a touch-screen kiosk for delivery of campus information is not what makes this project unique. The truly innovative aspect of this application is the integration of expert systems for academic advising into a comprehensive information delivery system that includes database access and multimedia components.

The kiosk project, in fact, began as an Artificial Intelligence (AI) initiative funded in part by the State of Ohio for the purpose of transferring AI technology from military to civilian use. Sinclair elected to use part of the AI grant to develop an actual expert system, primarily to give faculty some hands-on experience that would broaden their understanding of artificial intelligence technology. As the advising expert systems evolved, the project team began to explore touch screen kiosks as a means of fielding the expert systems. Working closely with the College's partner, TRG, Inc., Sinclair has integrated its AI components into the TRG "InTouch" kiosk software. Although AI is now a relatively small component of the InTouch kiosk system, it is one of the most useful parts and certainly the most unique.

See http://www.sinclair.edu/departments/helpdesk/ServicesSupported/InTouchKiosks/index.cfm for more info.

Title: The Knowledge Base: Computing Help 24 Hours, Seven Days a Week **#** 240

Source: Indiana University *Co Area:*

Addl Info: http://www.educause.edu/999/1245

Abstract: This computing-use expert system uses technology to help support the increasing demand for technology support at Indiana University. The Knowledge Base (KB) draws from around 5,000 documents and answers over 40,000 questions each week, using a Web-based interface that allows questions in keyword or plain English forms. Deployed at all eight IU campuses, the system has become the primary tool for end-user support. It also serves as a resource to other higher education institutions, who can use the database for information that is not specific to IU, and has been customized into "domains" established for departments and other service providers who can provide special-interest information for their customers. The project is noteworthy for its effective aggregation of a wealth of information pieces, its ability to disseminate documentation, and the breaking down of help desk boundaries-without increased staff resources. Although developed as an internal tool, it has already been emulated by several other universities.

More - http://www.educause.edu/LibraryDetailPage/666?ID=EDU0033

BEST PRACTICES, IRM

Title: Selective Mass Messaging System   **#**   241

Source: University of California Irvine   *Co Area:*

Addl Info: http://www.educause.edu/999/1245

Abstract: The latest release of UC Irvine's e-mail message system uses the power of the Web to move internal communication to a new level of sophistication and simplicity. No longer a service provided by the Distribution and Document Management staff, the new system made the campus message system (ZotMail) part of a communication infrastructure through which messages can be sent to defined groups of employees 24 hours a day, seven days a week, from anywhere in the world - and recipients can control which messages they receive. The transmission authorization system is based on an organizational taxonomy, and recipients can see which area sent the message. Unsolicited messages have been virtually eliminated; more frequent and focused messages have improved campus communications; the decentralized subscription process has eased administration for both senders and recipients. Noteworthy are the streamlined management and control process, the excellent combination of technology and policy which the program represents, and the graceful solution to a significant problem area of insatiable technology need.

https://www.ddm.uci.edu/zotmail/

BEST PRACTICES, IRM

Title: Best Practice guide for email use   **#**   266

Source: University of Bristol, England   **Co Area:**

Addl Info: http://www.bristol.ac.uk/is/learning/documentation/email-g3/email-g3.html

Abstract: This website should be reviewed to see if FAU's e-mail site could be improved.
Summary
Introduction
Sending mail
   Mail security
   Size of messages and attachments
   Format of attachments
   Creating HTML files
   URLs in mail messages
   Mail headers
   Addresses and mailing lists
   Mailing to very large groups
Administering mailboxes
   General
   Junk mail
   When you're away
   Having someone else read your mail
   Shared mailboxes
References

Title: Information Systems Best Practices   **#**   283

Source: Harvard University   **Co Area:**

Addl Info: http://vpf-web.harvard.edu/rmas/best_practices.html

Abstract: Bests Practices provided by Risk Management and Audit Services, covering -

Software Licensing
Password Management
User Management
Antivirus Management
Change Control
Computer and Network Security Best Practices
Credit Card Transactions Best Practices

BEST PRACTICES, IRM

Title: Information Technology Best Practices   **#**   309

Source: University of Georgia System   **Co Area:**

Addl Info: Taken Off Line - Contact Institution

Abstract: Approximately 30 Information Technology related Best Practices for review.

Old URL - http://www.usg.edu/bestpractices/current/index.phtml?area=infotech

Title: Back Up Your Data   **#**   312

Source: American University   **Co Area:** Human Resources

Addl Info: http://www.american.edu/technology/sites/helpdesk/content.cfm?id=709

Abstract: Upon doing a search, it was discovered that FAU's IRM had a good file on backing up data at
http://www.ecs.fau.edu/Training/downloads/Backupyourfiles.pdf - probably better than above - but IF the faculty/staff are not made aware of
such a resource, more data than necessary will be lost.

Perhaps with the assistance of Human Resources, this type of information could be brought to the forefront. Backing up data is an not a high
priority task - BUT - after a crash it becomes the only priority.

Title: Best practices: Pointers to Recommendations and Tips   **#**   314

Source: Microsoft   **Co Area:**

Addl Info: http://technet2.microsoft.com/windowsserver/en/library/ (Original URL no longer valid)

Abstract: Microsoft TechNet
75+ Technology related Best Practices. Examples -

* Auditing Security Events Best practices
* Best practices for disaster recovery
* Best practices for selecting and configuring hardware
* Network Connections Best Practices
* Stored User Name and Password Best practices
* VPN best practices

BEST PRACTICES, IRM

Title: Best Practices for product support recommendations and tips on managing security   **#** 315

Source: Microsoft   ***Co Area:***

Addl Info: http://technet.microsoft.com/en-us/library/bb742420.aspx

Abstract: Microsoft Windows 2000 Adv'd Server Documentation
http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/sag_SEconceptsBP.htm?id=758

From the above site, see the following 6 links:
Best practices for access control
Best practices for auditing
Best practices for Certificate Services
Best practices for Encrypting File System
Best practices for security configuration and analysis
Best practices for managing security templates

Title: Best Practices for Desktop Computer Use   **#** 340

Source: Cal State - Fullerton   ***Co Area:*** Human Resources

Addl Info: http://www.fullerton.edu/it/news/Publications/itdownload/archive/May02/content.htm

Abstract: Scroll about 2/3 of the way down to come to this Best Practice. This could be given out at New Employee Orientation.

It is a checklist of how the university expects you to be using the desktop computer provided through the President's Technology infrastructure Initiative.

It covers -
Computer Operations
Energy / Monitor Management
Computer Security

BEST PRACTICES, IRM

Title: IT Best Practices   **#**   414

Source: University of Iowa   *Co Area:*

Addl Info: http://cio.uiowa.edu/policy/bestpractices.shtml

Abstract: Many university websites have best practices related to IRM or IT and very few are covered in this data base. However the above site is an excellent example of an IT Best Practice site.

A "Best Practice" is a resource promoted by management as a recommendation. Best practices are developed by subject matter experts either locally or through external groups, vendors, or a combination. Best practices may develop into standards as they mature.

* Email Attachments
* Exchange
* Laptop Computers
* Mass Email
* Password Management
* Safe Computing
* Security Best Practices
* SPAM
* Work Station Protection

IT Policy Feedback Form

Title: Distance Education Best Practices Manual   **#**   451

Source: University of Phoenix - Illinois Valley CC Web Site   *Co Area:* Distance Learning

Addl Info: http://www.ivcc.edu/malcolm/distance_education_best_practice.htm

Abstract: Many higher education websites have information on Distance Learning Best Practices - this appears to be one of the better ones.

BEST PRACTICES, IRM

Title: Privacy Policy   **#**   452

Source: Kaskaskia College   **Co Area:**

Addl Info: http://www.kaskaskia.edu/privacypolicy.asp

Abstract: The following statement explains our policy regarding the personal information we collect about you.

  1. Statement of intent
  2. Information on visitors
  3. What is a cookie?
  4. Submitting personal information
  5. Access to your personal information
  6. Password Policy
  7. Users 16 and under
  8. How to find and control your cookies
  9. How do you know which sites use cookies?
  10. How to see your cookie code

BEST PRACTICES, IRM

Title: SUNY Best Practices Search Facility   **#**   475

Source: State University of New York   **Co Area:**

Addl Info: http://www.suny.edu/BestPractices/Best.Practices.2004.01.27.pdf

Abstract: As part of the Task Force on Efficiency and Effectiveness, campus presidents were asked to provide initiative they believe they carry out better than any other campus, along with those innovative ideas that have saved or avoided spending resources. The "Best Practices" reported in this document have resulted in significant savings throughout SUNY and, when shared with other campuses, have the potential to realize even greater savings within the system.

Page 30 of the above PDF Document

Personal Cell phone Contracts
Student Employee at Help Desk
Telecommuting for Employees
Computer Based College Orientation
 Financed Purchase of PC's
Thin Client Computing
E-Print Reports
Scanned Documentation
Automated Student Tracking
E-mail Communication with Students
Installing Latest Technology
Hand-held Inventory Scanner
Integrated Computer Access Control

Title: Phishing-related Best Practices   **#**   496

Source: Columbia State Community College   **Co Area:**

Addl Info: http://www.columbiastate.edu/it/Media/trendmicro_whitepaper_phishing.pdf

Abstract: Phishing is slowly becoming a household term, with a new scam arriving in users' inboxes as frequently as once per week. Phishing has become so widespread, in fact, that even many consumers know what it is!

The Internet community is not completely helpless against Phishing attacks. This section outlines several logical guidelines and Phishing-related best practices that could help prevent users of all types from being victimized by Phishing scams.

Covers Personal and Home Networks and Small and Medium Businesses (SMB) to Enterprise Networks

---

BEST PRACTICES, IRM

Title: Security Awareness, Training and Education   **#**   513

Source: University of Georgia   *Co Area:*

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2006.html

Abstract: Horror stories of breaches in security abound, whether the organization is in higher education, government or the private sector. The University of Georgia is certainly not immune to these problems and, in response to growing security concerns, the Enterprise Information Technology Services (EITS) staff has implemented a proactive security awareness program to inform staff of the potential risks and countermeasures to protect campus information.

The SANS (SysAdmin, Audit, Network, Security) Institute's Security Awareness Training and Certificate Program is offered online for all EITS staff and may soon be available to the University's administrative and academic units. The long-range goal is to include the entire University System of Georgia in this opportunity. Through real-life case studies, this commercial, off-the-shelf program illustrates the do's and don'ts of basic security awareness. Quiz questions are integrated throughout the program to reinforce key concepts. At the end of the training, a passing score on a 50-question final examination rewards the user with a printable SANS Awareness Certificate of Completion, which is valid for one year.

Title: How to tame the e-mail beast   **#**   525

Source: CIO Magazine - CNN Website   *Co Area:* Human Resources

Addl Info: http://archives.cnn.com/2001/TECH/internet/10/18/email.beast.idg/index.html

Abstract: Attachments - Allegiance has a relatively stringent approach to enforcing its corporate e-mail usage policy -- employees must agree to the policy's terms and conditions each and every time they log on to the e-mail system. The policy includes a prominent directive: Don't open unexpected attachments.

Start with a usage policy - Your first line of defense against e-mail troubles is a solid e-mail usage policy, regularly communicated and consistently enforced. Unfortunately, no single e-mail policy works for all companies. At Paul, Hastings, Janofsky & Walker, a law firm headquartered in Los Angeles with more than 1,900 employees, staffers must sign a technology usage agreement upon joining the firm. CIO Mary Odson also circulates an update or review of the agreement every six months.

Training employees on e-mail policies is standard procedure for many companies, but training that stops there is inadequate. Employees also need instruction in e-mail etiquette, including how to recognize spam, scams and urban legends.

BEST PRACTICES, IRM

Title: Campus Computing and the Environment   **#**   536

Source: University of Guelph   **Co Area:** Physical Plant

Addl Info: http://www.isc.uoguelph.ca/documents/060301GreenComputingReport-Draft3.doc

Abstract: In response to the release of the study Environmental Impact of Computer Information Technology in an Institutional Setting: A Case Study at the University of Guelph the ISC struck a Green Computing Task Group to review policies, guidelines and practices at the University of Guelph with respect to the purchase, use and disposal of computers, in order to make recommendations that would mitigate the environmental impacts of computing on campus. Computers are defined as desktop units which typically include; central processing unit, monitor, keyboard, mouse and external speakers; and laptop and notepad computers which include all of the above components in a single unit.

Specific Objectives:
* identify green computing best practices at other universities and in other sectors
* benchmark the University of Guelph against these best practices
* examine the need for and nature of computing procurement guidelines
* identify energy conservation strategies and practices
* identify equipment disposal procedures
* recommend a campus awareness program

Title: Computing Best Practices: Troubleshooting!   **#**   544

Source: University of Manitoba   **Co Area:**

Addl Info: http://umanitoba.ca/faculties/science/computing/bestpractices/

Abstract: The following are some of the things you can do when you encounter errors, system crashes or other computer problems. The list below contains steps that are recommended good practice to follow for general computer usage. Now some of these items may seem like very basic steps to you, but you would be surprised to see how many people still do not follow them.

Topics briefly covered -
   * When in Doubt Reboot
   * Check Peripherals and Cables
   * Make a Note of Error Messages
   * System Maintenance
   * Use the Help Provided
   * Read the Manual
   * Run Windows Update
   * Read Instructions Carefully
   * Keep your Anti-virus software updated
   * 10 Tips for PC Troubleshooting

BEST PRACTICES, IRM

Title: Your guide for protection your data and computer   **#**   548

Source: University of Toronto   **Co Area:**

Addl Info: http://cns.utoronto.ca/UTORprotect/documents/UTORProtect_Best_Practices.pdf

Abstract: Information protection and computer security have become increasingly important issues to many computer users. Computer viruses have become more sophisticated and as more and more users leave their computers connected to the Internet 24x7, attacks by hackers have increased dramatically.

If you are using your computer to conduct research or to complete assignments or for business, then it is important that you take the necessary precautions to protect the data and information that is stored on your computer. The University expects that any institutional data stored on computers, whether on campus or at you place of residence, must be protected.

The University is increasingly taking a pro-active approach to data protection. For example, an institutional license for anti-virus software makes this software available at no cost to all students, faculty and staff. This should reduce instances of infections that generate a lot of unnecessary traffic on our networks as well as protect data and information from being inadvertently divulged to unauthorized individuals. Another initiative is a service that enables departments to backup network servers.

As part of the UTORProtect Program initiated by Computing & Networking Services, this Best Practices document was developed in order to assist all users associated with the University to protect their computers and the data and information stored on computers.

This document is intended to assist students, faculty and staff to determine how best to protect their computers. It is not intended to address technical issues nor is it a detailed "how to" or "do it yourself" technical reference document.

Title: Best Practices Statement - Instant Messaging Security   **#**   600

Source: State of Arkansas   **Co Area:**

Addl Info: http://www.techarch.state.ar.us/domains/security/best_practices/IM_best_practice.pdf

Abstract: Purpose
Instant messaging is an alternate way to people to communicate with each other using their personal computers, but IM can be a conduit for malicious software to infect users' machines. While IM has benefits, it should be utilized in a controlled manner to protect state resources.

Scope
This best practices statement is recommended for all state agencies, boards, commissions and institutions of higher education.

BEST PRACTICES, IRM

Title: Recognition Awards   **#** 608

Source: National Association of State Chief Information Officers   *Co Area:*

Addl Info: http://www.nascio.org/awards/index.cfm

Abstract: NASCIO represents state chief information officers and information resource executives and managers from the 50 states, six U. S. territories, and the District of Columbia. State members are senior officials from any of the three branches of state government who have executive-level and statewide responsibility for information resource management. Representatives from federal, municipal, and international governments and state officials who are involved in information resource management but do not have chief responsibility for that function participate in the organization as associate members. Private-sector firms and non-profit organizations may join as corporate members.

Title: Security Tips and Best Practices   **#** 647

Source: University of Massachusetts   *Co Area:*

Addl Info: http://www.massachusetts.edu/SecurityAwareness/securityawareness.html

Abstract: The following links are considered "Best Practices" for securing computers and networks. Here you will find information on policies and guidelines data, computer and network security, virus alerts and hoaxes and computer security awareness. Your thoughts and ideas on improving this website and promoting information security are welcome.

Secrets to the Best Passwords
Educause Effective Practices and Solutions
A Users Guide to Security Threats on the Desktop
Denial of Service Attacks
Beginner's Guides Home Network
Security - from CERT for home networks . . . for home computers
The Simplest Security: A Guide To Better Password Practices
Protecting Yourself from Password File Attacks
Email Bombing and Spamming
Spoofed/Forged Email Educause
Effective Practices and Solutions
Virus Primer
Software Piracy Information - Business Software Alliance

BEST PRACTICES, IRM

Title: Higher Education Best Practices - Screen Capture and Recording Software **#**   651

Source: TechSmith   **Co Area:**

Addl Info: http://www.techsmith.com/community/education/highedcasestudies.asp

Abstract: TechSmith is the world's leading provider of screen capture and recording software. People are using TechSmith products to capture content from their screen in ways that help them communicate more clearly, create engaging presentations for diverse audiences, and analyze product usability and customer experience.

Higher Education Best Practices - Administration and Staff

Training Videos Eliminate Need for Massive Manpower
Mary Longcore of Michigan State University's HealthTeam creates Flash videos to ease training load.

TechSmith's Morae Plays Key Role in Huge Success of Mizzou's New Award-Winning Undergraduate Online Admissions Website
Case study - MU found Morae to be the ideal way to integrate usability testing into the IE Lab and into their design and development processes for Web sites, software applications and grant-based research projects.

Small Flash Files Provide Online Learning Solution
Thomas Hennigan creates highly effective Flash tutorials at Lewis-Clark State College so small even dial-up users love them.

SnagIt Screen Capture Saves Technologists Time on Support Documentation
A Minnesota State University department adopts SnagIt after recommendation by online learning specialist.

Technology Instructions for Faculty Made Easy with Help Videos
Every time a new Blackboard feature is added at the University of Miami, a video is created to train staff on its use.

There is also a list for Faculty

BEST PRACTICES, IRM

Title: Keeping Clemson Secure; A Best Practices Guide   **#**   754

Source: Clemson University   **Co Area:**

Addl Info: http://www.clemson.edu/ccit/support_services/how_to/solution_guides/BestPractices.html

Abstract: Security is a part of our every day thinking in this day and age. Clemson University takes security seriously and wants our users to be vigilant and practice due diligence when it comes to security. It is important that our users understand what is expected of them in securing Clemson's resources as well as what concerns they should have to avoid falling victim to a security incident. This guide serves as a best practices guide to aid the user in following good security practices to help keep Clemson a safe and secure environment.

Covers -
   Adhere to Clemson Computing Policies
   Protect your Identity
   Safeguard your workstation
   Be alert

To report a security incident, please fill out the Incident Report Form - http://dcit.clemson.edu/support/security/report.php

---

Title: Information Technology Unit Managerial Competencies: The Four Pillars   **#**   795

Source: George Mason University   **Co Area:** Human Resources

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2007.html

Abstract: The "Information Technology Unit (ITU) Managerial Competencies: The Four Pillars" was developed to establish and define the expectations for all managers within the department. "The Four Pillars" provides staff with clear descriptions of behaviors that an effective manager should incorporate in his or her interactions with direct reports and with superiors. Managers, through self assessment or with a supervisor, can chart a personal development path to improve on competencies that need strengthen. Leadership retreats sponsored by the ITU for all managers can be directed to competencies that need overall focus and prioritization.

The ITU's Four Pillars are designed to help its managers acquire the knowledge, skills and abilities that will make them competent in their managerial roles. Supervisors make a commitment to negotiate an agreement with their manager to develop the needed competencies and to provide opportunities for managers to practice these skills.

Furthermore, ITU managers at all levels are expected to be effective leaders, particularly with respect to leading change. The mission of the ITU is to advance the University's strategic goals, support learning, enable scholarly endeavors, and improve institutional management. Clearly the fulfillment of this mission requires leaders who can identify the need for change, design and implement change strategies, and assist staff and customers in dealing with change.

The four "pillars"—Knowing the organization, Leading and managing people, Managing resources, and Communicating effectively—form the basis of the managerial competencies the ITU expects at all levels of the organization.

BEST PRACTICES, IRM

Title: Automated Security Self-Evaluation Tools (ASSETs)   **#**   814

Source: University of Georgia   *Co Area:*

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2007.html

Abstract: The University of Georgia's Internal Auditing Division and the Office of Information Security, utilizing existing internal staff, set out to complete the task of assessing 19 identified high-risk, highly visible and greatest target-of-opportunity operations on the University campus. In order to identify and manage at-risk IT systems effectively, a protocol was developed which placed the responsibility on the units themselves to perform and report self-evaluations: the Automated Security Self-Evaluation (ASSETs) program.

UGA ASSETs provides a comprehensive set of online, intuitive, extensible and automated tools for college and department security liaisons. These tools include self-assessment, security, compliance reporting and security planning for the unit's own assets, as well as self-help and "shared responsibility" for information and information systems security.

Title: Access Technologists Higher Education Network   **#**   839

Source: Access Technologists Higher Education Network   *Co Area:*

Addl Info: http://www.athenpro.org/

Abstract: ATHEN was formed to meet a critical need for a professional identity and build a collective understanding of what it means to work in the field of Access Technology in Higher Education. While other organizations exist that work on parallel tracks in disability services, the founding membership felt that a targeted organization was needed to fulfill the collective needs of the membership. A secondary driving force is the creation of professional development activities for Access Technologists that mirror similar career tracks in other areas of IT management and service delivery.

The primary goals of ATHEN are:

   * Acquiring, sharing, and dissemination of best practices in Access Technologies (AT), including:
      1. AT training materials
      2. Core-Curriculum
      3. Promote the establishment of Degree Programs
   * The establishment of a professional identity for those who practice AT in Higher Education.
   * The development of Professional Standards of Practice for AT in Higher Education.

BEST PRACTICES, IRM

Title: Collection of 31 Best Practices for Cyber-Security Awareness   **#**   851

Source: Microsoft   *Co Area:*

Addl Info: http://msmvps.com/blogs/harrywaldron/archive/2007/11/01/isc-collection-of-31-best-practices-for-cyber-security-awareness.aspx

Abstract: Microsoft's Most Valuable Professions offer 31 suggestions concerning -
1. Establishing a User Awareness Training Program
2. Best Practices
3. Hardware/Software Lockdown
4. Safe Internet Use
5. Privacy and Protection of Intellectual Property

Also see Cyber Security Awareness Month - Summary and Links - http://isc.sans.org/diary.html?storyid=3597

Title: Environmental best practices in ICT in Higher Education report   **#**   944

Source: Computing for Sustainability   *Co Area:*

Addl Info: http://computingforsustainability.wordpress.com/2009/01/27/environmental-best-practices-in-ict-in-higher-education-report/

Abstract: Short story: return of the data centres (but with a green tinge).

The chapter is structured around taking action. Data centres are seen as an important area with rapidly expanding data storage requirements. These, though , have a "hidden environmental footprint" with "rapidly growing energy consumption".   They give three scenarios.

Blogs about: Computing For Sustainability - http://wordpress.com/tag/computing-for-sustainability/
Also see http://computingforsustainability.wordpress.com/2009/01/27/balancing-benefits-and-invisible-overheads-in-ict-in-higher-education-report/

Title: Google's Best practices against hacking   **#**   956

Source: Google Webmaster Central Blog   *Co Area:*

Addl Info: http://googlewebmastercentral.blogspot.com/2009/02/best-practices-against-hacking.html

Abstract: These days, the majority of websites are built around applications to provide good services to their users. In particular, are widely used to create, edit and administrate content. Due to the interactive nature of these systems, where the input of users is fundamental, it's important to think about security in order to avoid exploits by malicious third parties and to ensure the best user experience.

Some types of hacking attempts and how to prevent them

BEST PRACTICES,   IRM

Title: Fostering Institutional Change and Collaboration through the Implementation of a Knowledge Management Infrastructure   **#**   970

Source: Tallahassee Community College   *Co Area:*

Addl Info: http://www.sacubo.org/sacubo_resources/best_practices/2009.html

Abstract: Before early 2007, TCC didn't have a unified online environment through which students could manage important information about college life. They had to remember three passwords to access course grades and curriculum requirements; financial aid status; and registration forms using a third-party database system called EagleNet. Students required a fourth password to use a Web-based course-management system. The IT department had to manually administer these passwords for 15,000 students.
Faculty and staff members faced similar problems trying to find information stored among data silos and directories on the college's network drives. There was no single place to publish information or go to for administrative forms, nor a way to easily automate workflows for those forms.

The Information Technology department designed three portals to house information for outside entities, the District Board of Trustees, the faculty and most importantly students. At the same time an IT team was formed to begin the process of building a robust business intelligence solution to allow all authenticated users the ability to approach and mine the information to
support decisions across the organization.

The portals have had many benefits. The DBOT portal was extremely important when decisions about tuition increases came in the spring of 2007. The board members were able to use models on the portal workshop site to calculate possible state budget cuts, enrollment growth, and tuition increases in real time. This model illustrated the impact of each of those adjustments on the
future budget year. The tool provided to be a powerful enough experience to cause the DBOT to have an unscheduled vote on tuition.

Title: Systems Security   **#**   992

Source: University of Tennessee   *Co Area:*

Addl Info: http://security.tennessee.edu/policies.shtml

Abstract: Several Best Practices and policies related to technology security. Also see similar site from University of Northern Iowa at http://www.uni.edu/its/security/bestpractices.html.

Title: Best practices for computer security   **#**   993

Source: Indiana University   *Co Area:*

Addl Info: http://kb.iu.edu/data/akln.html

Abstract: This document details how you can secure your personal computer accounts and the data stored on them .Also see http://informationsecurity.iu.edu/articles/

BEST PRACTICES, IRM

Title: IT Security Best Practices   **#**   998

Source: Wayne State University   **Co Area:** Inspector General

Addl Info: http://internalaudit.wayne.edu/security-practices.php

Abstract: This is a site under the Office of Internal Audit. The following is a list of best practices that were identified to develop, identify, promulgate, and encourage the adoption of commonly accepted, good security practices. They represent 10 of the highest priority and most frequently recommended security practices as a place to start for today's operational systems. These practices address dimensions of information security such as policy, process, people, and technology, all of which are necessary for deployment of a successful security process. This initial set of practices is targeted toward executive leadership in industry. When adopted, these practices catalyze a risk-management-based approach to ensuring the survivability and security of critical information assets.

General Management
System & Network Management
Policy
Authentication & Authorization
Risk Management
Monitor & Audit
Security Architecture & Design
Physical Security
User Issues
Continuity Planning & Disaster Recovery

Title: National Center for Higher Education Management Systems (NCHEMS)   **#**   1013

Source: National Center for Higher Education Management Systems (NCHEMS)   **Co Area:**

Addl Info: http://www.nchems.org/

Abstract: The National Center for Higher Education Management Systems (NCHEMS) is a private nonprofit (501)(c)(3) organization whose mission is to improve strategic decision making in higher education for states and institutions in the United States and abroad.

Through its more than thirty years of service to higher education, NCHEMS has been committed to bridging the gap between research and practice by placing the latest concepts and tools in the hands of higher education policy makers and administrators. Since its founding, NCHEMS has received widespread acclaim for developing practical responses to the strategic issues facing leaders of higher education institutions and agencies. With project support from multiple foundations, NCHEMS develops information and policy tools targeted at policy makers and institutional leaders that can help them set strategic directions and evaluate their effectiveness. NCHEMS also delivers research-based expertise, practical experience, information, and a range of management tools that can help institutions and higher education systems and states improve both their efficiency and their effectiveness. A particular hallmark of what we do is identifying and analyzing data drawn from multiple sources to help solve specific policy and strategic problems.

BEST PRACTICES, IRM

Title: eForms: Process Re-engineering, Paperwork Reduction and Environmentalism **#** 1037

Source: Cincinnati State Technical and Community College **Co Area:**

Addl Info: http://www.cacubo.org/pdf/2009/10_Cincinnati%20State_eForms%20Process%20ReEngineering.pdf

Abstract: In order to improve College business processes; generate savings in staff time, supplies and storage; and reduce environmental waste, the College's IT department developed a web-based electronic forms application. Called eForms, the application was built using Microsoft .NET and a Microsoft SQL Server database.

An eForm can be developed by any employee, after a little training. eForms replace existing paper forms. Among system features are electronic routing and approval, the ability to attach documents, the automatic aggregation of data in spreadsheet form, the ability to make fields required or optional, and an option for customized programming. To ensure form integrity, the system has an archiving capability.