<table>
<thead>
<tr>
<th>Title</th>
<th>Source</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEST PRACTICES, Office of Information Technology</td>
<td>Educause</td>
<td>237</td>
</tr>
<tr>
<td>Title: Educause</td>
<td>Source: Educause</td>
<td></td>
</tr>
<tr>
<td>Addl Info: <a href="http://www.educause.edu/">http://www.educause.edu/</a></td>
<td>Co Area:</td>
<td></td>
</tr>
<tr>
<td>Abstract: Do a search for Best Practices.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EDUCAUSE helps those who lead, manage, and use information technology to shape strategic IT decisions at every level within higher education.

<table>
<thead>
<tr>
<th>Title</th>
<th>Source</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Systems Best Practices</td>
<td>Harvard University</td>
<td>283</td>
</tr>
<tr>
<td>Title: Information Systems Best Practices</td>
<td>Source: Harvard University</td>
<td></td>
</tr>
<tr>
<td>Addl Info: <a href="http://vpf-web.harvard.edu/rmas/best_practices.html">http://vpf-web.harvard.edu/rmas/best_practices.html</a></td>
<td>Co Area:</td>
<td></td>
</tr>
<tr>
<td>Abstract: Bests Practices provided by Risk Management and Audit Services, covering -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Licensing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Control</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Source</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best practices from Microsoft</td>
<td>Microsoft TechNet</td>
<td>314</td>
</tr>
<tr>
<td>Title: Best practices from Microsoft</td>
<td>Source: Microsoft TechNet</td>
<td></td>
</tr>
<tr>
<td>Addl Info: <a href="http://technet.microsoft.com/en-us/ms376608.aspx">http://technet.microsoft.com/en-us/ms376608.aspx</a></td>
<td>Co Area:</td>
<td></td>
</tr>
<tr>
<td>Abstract: Do a search on Best Practices</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Many university websites have best practices related to IRM or IT and very few are covered in this database. 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: How to tame the e-mail beast
Source: CIO Magazine - CNN Website
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.
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
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.
# Best Practices Statement - Instant Messaging Security

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

**Source:** State of Arkansas

**Addl Info:** [http://www.dis.arkansas.gov/policiesStandards/Pages/BestPractices.aspx](http://www.dis.arkansas.gov/policiesStandards/Pages/BestPractices.aspx)

**Abstract:** The following is a list of best practices relating to technology in the State of Arkansas for your reference. A best practice is a technique, method, process, activity, or incentive that is believed to be effective at delivering a particular outcome or a technique or methodology that, through experience and research, leads to a desired or optimum result.

- A Model Internet Appropriate Use Policy
- Best Practices - K-12 Password Management
- Best Practices for Accessibility
- Best Practices for Managing State IT Projects
- Electronic Records Management Guidelines
- Instant Messaging
- Internet Appropriate Use Guidelines
- Machine Readable Privacy Policy Guidelines
- Use of Non-Governmental Equipment
- Wireless Security

---

# Recognition Awards

**Title:** Recognition Awards

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


**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.
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
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
Title: Higher Education Best Practices - Screen Capture and Recording Software
Source: TechSmith
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
Title: Keeping Clemson Secure; A Best Practices Guide
Source: Clemson University
Addl Info: http://www.clemson.edu/ccit/help_support/safe_computing/resources/best_practices.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

Title: Access Technologists Higher Education Network
Source: Access Technologists Higher Education Network
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.
**Title:** Collection of 31 Best Practices for Cyber-Security Awareness

**Source:** Microsoft


**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

---

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

**Source:** Computing for Sustainability


**Abstract:**
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.


---

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

**Source:** Google Webmaster Central Blog


**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
Fostering Institutional Change and Collaboration through the Implementation of a Knowledge Management Infrastructure

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.

Welcome to the University of Tennessee's resource for information technology security. The Information Security Office (ISO) is charged with the responsibility of network and systems security at the University of Tennessee.

The ISO works with members of the UT community, including system administrators, students, staff and faculty, to protect the UT network and connected hosts. The ISO cooperates with administrators at other sites, as well as law enforcement entities, in response to security incidents.

Several Best Practices and policies related to technology security.
Best practices for computer security

Indiana University

http://kb.iu.edu/data/akin.html

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

IT Security Best Practices

Wayne State University

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

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
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.

eForms: Process Re-engineering, Paperwork Reduction and Environmentalism

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.

For additional information, contact Financial Affairs