COMPUTER SECURITY AUDIT REPORT

Board of Regents' Information Systems: Reviewing Computer Security at Various Universities

A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
April 2005

05 IT 101

Legislative Post Audit Committee
Legislative Division of Post Audit

THE LEGISLATIVE POST Audit Committee and its audit agency, the Legislative Division of Post Audit, are the audit arm of Kansas government. The programs and activities of State government now cost about $11 billion a year. As legislators and administrators try increasingly to allocate tax dollars effectively and make government work more efficiently, they need information to evaluate the work of governmental agencies. The audit work performed by Legislative Post Audit helps provide that information.

We conduct our audit work in accordance with applicable government auditing standards set forth by the U.S. Government Accountability Office. These standards pertain to the auditor's professional qualifications, the quality of the audit work, and the characteristics of professional and meaningful reports. The standards also have been endorsed by the American Institute of Certified Public Accountants and adopted by the Legislative Post Audit Committee.

The Legislative Post Audit Committee is a bipartisan committee comprising five senators and five representatives. Of the Senate members, three are appointed by the President of the Senate and two are appointed by the Senate Minority Leader. Of the Representatives, three are appointed by the Speaker of the House and two are appointed by the Minority Leader.

Audits are performed at the direction of the Legislative Post Audit Committee. Legislators or committees should make their requests for performance audits through the Chairman or any other member of the Committee. Copies of all completed performance audits are available from the Division's office.

LEGISLATIVE POST AUDIT COMMITTEE

Representative John Edmonds, Chair
Representative Tom Burroughs
Representative Peggy Mast
Representative Bill McCreary
Representative Tom Sawyer

Senator Les Donovan, Vice-Chair
Senator Anthony Hensley
Senator Nick Jordan
Senator Derek Schmidt
Senator Chris Steineger

LEGISLATIVE DIVISION OF POST AUDIT

800 SW Jackson
Suite 1200
Topeka, Kansas 66612-2212
Telephone (785) 296-3792
FAX (785) 296-4482
E-mail: LPA@lpa.state.ks.us
Website:
http://kslegislature.org/postaudit
Barbara J. Hinton, Legislative Post Auditor

The Legislative Division of Post Audit supports full access to the services of State government for all citizens. Upon request, Legislative Post Audit can provide its audit reports in large print, audio, or other appropriate alternative format to accommodate persons with visual impairments. Persons with hearing or speech disabilities may reach us through the Kansas Relay Center at 1-800-766-3777. Our office hours are 8:00 a.m. to 5:00 p.m., Monday through Friday.

LEGISLATURE OF KANSAS

LEGISLATIVE DIVISION OF POST AUDIT

800 SOUTHWEST JACKSON STREET, SUITE 1200
TOPEKA, KANSAS 66612-2212
TELEPHONE (785) 296-3792
FAX (785) 296-4482
E-MAIL: lpa@lpa.state.ks.us

April 21, 2005

To: Members, Legislative Post Audit Committee

Representative John Edmonds, Chair	Senator Les Donovan, Vice-Chair
Representative Tom Burroughs	Senator Anthony Hensley
Representative Peggy Mast	Senator Nick Jordan
Representative Bill McCreary	Senator Derek Schmidt
Representative Tom Sawyer	Senator Chris Steineger

This report contains the findings, conclusions, and recommendations from our completed performance audit, *Board of Regents' Information Systems: Reviewing Computer Security at Various Universities*.

The report includes several recommendations for the three universities we looked at: Emporia State University, Kansas State University, and the University of Kansas. We would be happy to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other State officials.

In conjunction with this report, separate, confidential reports were prepared for each of the universities we reviewed. Those reports will be distributed and discussed in executive session during the April 25th meeting of the Committee.

Barbara J. Hinton
Legislative Post Auditor

READER'S GUIDE

Get the Big Picture

Read these Sections and Features:

1. **Executive Summary** - an overview of the questions we asked and the answers we found.

2. **Conclusion** and **Recommendations -** are referenced in the Executive Summary and appear in a box after each question in the report.

3. **Agency Response** - also referenced in the Executive Summary and is the last Appendix.

Helpful Tools for Getting to the Detail

- In most cases, an "**At a Glance**" description of the agency or department appears within the first few pages of the main report.
- **Side Headings** point out key issues and findings.
- **Charts/Tables** may be found throughout the report, and help provide a picture of what we found.
- **Narrative text boxes** can highlight interesting information, or provide detailed examples of problems we found.
- **Appendices** may include additional supporting documentation, along with the audit **Scope Statement** and **Agency Response(s)**.

Legislative Division of Post Audit
800 SW Jackson Street, Suite 1200, Topeka, KS 66612-2212
Phone: 785-296-3792 E-Mail: lpa@lpa.state.ks.us
Web: www.kslegislature.org/postaudit

EXECUTIVE SUMMARY

LEGISLATIVE DIVISION OF POST AUDIT

Overview of Computer Security in a University Environment

.....page 3

Universities present one of the most complex environments to secure within State government. They're large institutions with many computers, they have several distinctly different groups of users who have their own needs, many of the people associated with them aren't employees, and they have very decentralized information technology operations. Finally, universities have a long and deeply ingrained tradition of academic freedom and the free and open exchange of ideas, concepts that aren't always seen as compatible with computer security.

Because of the openness and the large number of computers, universities have been favorite targets for hackers, spammers, and others. As a result, universities regularly are in the headlines for significant security incidents. Maintaining adequate computer security while accomplishing the goals of a university is a difficult balance to achieve.

Question 1: How Well Do Universities Manage the Security of Their Information Systems?

.....page 7

In many areas, security practices described by university officials seemed adequate, but hadn't been put into official written policies. *We reviewed information security at Emporia State, K-State, and KU. The bulk of our work involved evaluating universities' security policies against a list of 54 best practices. For more than a third of these policy areas, the practices the universities described were adequate but hadn't been developed or adopted as official written policies. The three areas where unwritten policies were most common were access controls (passwords), operations, and physical security.*

The lack of written policies increases the risk that intended procedures won't be followed. Computer security covers a broad range of subject matter, most of which is technical. When computer security policies aren't written, people tend to make up their own ways of doing things, or don't do anything at all. It takes only one "hole" in an organization's computer security for its data to be compromised.

We also noted that the policy-setting process at all three universities was very time-consuming, and could result in "watered-down" security policies. Policy development should involve input from the users affected by the policy, but it appeared to us this concept had been taken too far. Draft policies have to be reviewed or approved by a number of committees, and it can take a policy a year or more to get through the process.

K-State has a procedure that can mitigate such delays. Officials sometimes create an interim policy that's in effect while the draft policy is going through the standard policy-setting process. This approach offers protection while the proposed policy winds its way through the process.

We found instances of inadequate or nonexistent security policies at all three universities. *For example, we found that the universities didn't all have written incident response plans. Such plans spell out what staff are supposed to do in response to different types of incidents. and are important in mitigating the chaos that can occur during security incidents. Also, the universities didn't all have adequate policies to ensure that security was considered throughout the development of new computer applications. When security is added at the end of a project, it tends to be more expensive and less effective.* .....page 10

Some of the problems we identified can't be discussed in any detail in a public report without putting the universities at greater risk. Therefore, we prepared a confidential report for each university that also will be presented in executive session to the Legislative Post Audit Committee.

All three universities need to elevate the role of their IT security officer. *A security officer should report directly either to a chief executive or to the Chief Information Officer. This is necessary because security officers need to be free to voice their security concerns with officials in a position to take action across the organization. In addition, the security officer needs to sit high enough in the organization to be perceived as having authority.* .....page 10

We noted problems with one or both of these areas at all three universities, as follows:

- *Emporia State doesn't have a dedicated security officer.*
- *K-State's security officer has less authority and more narrow responsibilities than desirable.*
- *The security officer at KU has appropriate authority, but is placed too low in the organization.*

The overall security function is strongest at the larger universities. *The universities have been subject to a number of fairly significant computer attacks in recent years. Security policies can prevent or help minimize the harm of such attacks. Over the last few years, KU and K-State have begun taking a more proactive approach to computer security by establishing policies and procedures and establishing a security structure.* .....page 13

At KU, a security officer and four staff members have been dedicated to security. At K-State, security efforts are led by the Chief Information Officer, a network manager, and the security officer. Both universities have taken steps to expand the reach of the central security function into the academic departments and administrative units.

At Emporia State, although the Chief Information Officer ultimately is responsible for security, this position has had significant turnover during the past decade, resulting in a lack of direction and momentum in developing a security structure.

Each university protects itself from viruses coming from the residence halls, but Emporia State needs to do more to help protect its students from viruses. *Residence halls on university campuses provide challenges for system network administrators. The university has no control over the types of computers students bring, or what software is on their computers This environment makes the residence halls susceptible to widespread virus infections.*

Both KU and K-State had severe computer virus outbreaks in residence halls last year that affected the universities' computer networks. Both subsequently developed and provided students with anti-virus programs to protect their computers, and report that virus outbreaks have been vastly reduced.

Emporia State has placed the residence halls on isolated networks, and placed a firewall between the residence halls and the rest of the university. This action keeps student computers from infecting the university network. However, the university has taken few steps to ensure that student computers have current anti-virus software, or that appropriate patches have been applied to their software.

Security awareness training needs to be beefed-up at Emporia State. *User awareness of security issues is a key element in maintaining the integrity of computer systems. Regular users generally are considered to be the most significant security risk in any organization. Therefore, it's imperative to educate employees about computer security and the important role they have in the process. Although Emporia State has placed security awareness information on its IT website, it does little else to make staff and students aware of IT security issues. Both KU and K-State have instituted security awareness training programs for their staff and students.*

This audit was conducted by Allan Foster and Molly Coplen. If you need any additional information about the audit's findings, please contact Mr. Foster at the Division's offices. Our address is: Legislative Division of Post Audit, 800 SW Jackson Street, Suite 1200, Topeka, Kansas 66612. You also may call us at (785) 296-3792, or contact us via the Internet at LPA@lpa.state.

Board of Regents' Information Systems: Reviewing Computer Security at Various Universities

This is the fifth in a series of specialized compliance and control audits designed to focus on an important area of agency operations that generally hasn't been reviewed: the technical aspects of operating information systems. At the direction of the Legislative Post Audit Committee, this audit focused on the management of information systems at several Regents' universities.

In fiscal year 2004, the Regents' universities spent about $65 million on their information systems (this figure excludes salary information). In all, about 650 full-time-equivalent staff develop, maintain, support, and control the information systems for the universities.

In the last two years, several high-profile computer intrusions at Regents' institutions have resulted in sensitive student and staff data being put at risk. The universities are at various stages of re-engineering their information systems, developing and implementing new applications, instituting wireless access, and expanding accessability from the Internet. However, there's currently little outside oversight of whether the risks associated with current or planned operations are being adequately managed.

This audit addresses the following question:

How well do universities manage the security of their information systems?

To answer this question, we reviewed information system standards and best practices, interviewed University officials, reviewed and evaluated policies and other documentation, and tested selected computer controls used by the universities in managing their computer systems. We looked at three universities: Emporia State University, Kansas State University, and the University of Kansas.

The criteria we used in reviewing the universities' management efforts were compiled primarily from the Federal Information Systems Controls Audit Manual (FISCAM), published by the U.S. General Accountability Office.

A copy of the scope statement for this audit approved by the Legislative Post Audit Committee is included in Appendix A. Because publicly identifying certain control weakness could compromise universities' security, we have written separate, confidential reports for each university that contain information too sensitive to be presented in this public report.

In conducting this audit, we followed all applicable government auditing standards. Our findings begin on page seven after a brief overview of computer security issues at universities.

Universities Are Complex Environments That Are Difficult to Secure For Many Reasons

They provide a number of unique challenges to security, including:

- There are a large number of users and a correspondingly large number of computers.
- A lot of students are eager to explore university resources, not always in constructive or mature ways.
- Faculty members work on projects with peers from other universities across the country and internationally.
- People associated with the university, but not officially employed, need computer access.
- Information technology tends to be very decentralized, with departments having a high degree of independence.
- Universities have goals of including, not excluding, people.

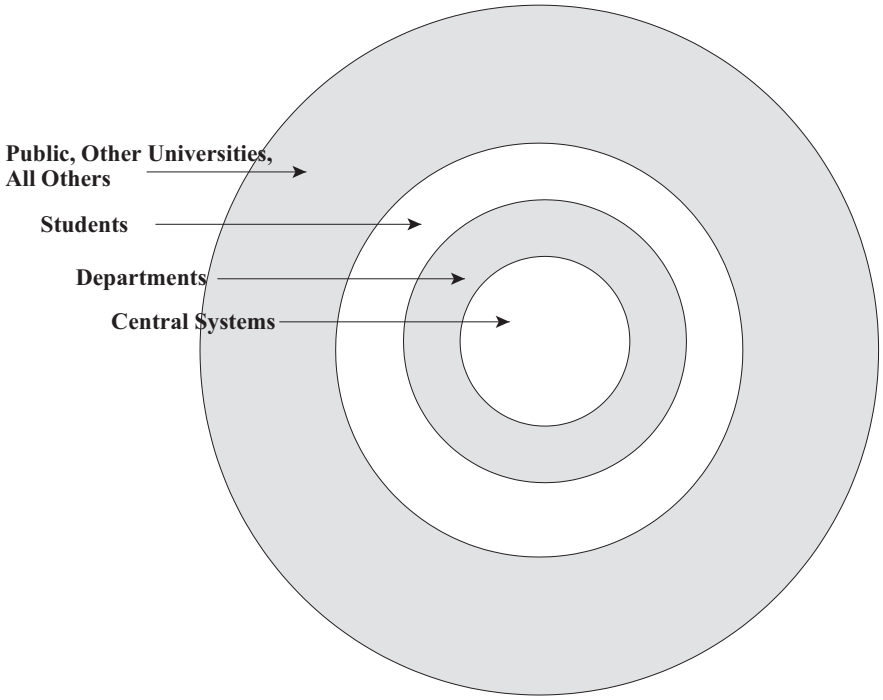
Finally, universities have a long and deeply ingrained tradition of academic freedom and the free and open exchange of ideas, concepts that are sometimes seen as not compatible with security. As a result, faculty can be very resistant to "security" because of the fear that it may interfere with their ability to communicate with students and peers inside and outside the university. And, in keeping with academic freedom, faculty are used to a great deal of independence from central authority. The universities we dealt with all said they strive to be open and welcoming environments.

Universities have many different types of confidential or sensitive data, and many groups of people who need to access both public and confidential data. *Figure OV-1* on the next page shows an abstract diagram of the groups that use information systems at a typical university. Important administrative applications, such as student records, classroom management tools, personnel and payroll, accounting, and communications are the core central systems. These tend to be centralized, often confidential or sensitive, and managed by the central IT staff. This staff typically also manages a variety of services such as a "help desk", computer training, security awareness, student labs, and local-area-networks for some departments.

The next ring represents the departments. Their systems are very decentralized, with each department maintaining its own systems. The central IT departments and officials have little direct control over these systems, which typically include computers housing research project data, student computer labs, local-area-networks belonging to larger departments or schools, student health information, etc. Then third ring consists of students, residential and otherwise, who have their own computers. Finally, the outer ring represents people outside the university who need access, such as faculty from other universities working on joint projects and the public.

Figure OV-1

University IT Constituent Groups



University databases hold a miscellaneous assortment of data. In addition to accounting, human resource, and student academic records, they also contain data related to student health centers, parking, athletics, fund raising, physical plant systems, continuing education programs, and alumni, to name only a few.

Because of the openness and the large number of computers, universities have been favorite targets for hackers, spammers, and others. As a result, universities regularly are in the headlines for significant security incidents, as described in the profile to the right.

Maintaining adequate computer security while accomplishing the goals of a university is a difficult balance to achieve. In the past, many universities haven't achieved that balance. However, the growing number of significant security events demands a better response.

Recent Security Incidents in Higher Education

Computerworld recently reported that of 501 colleges and universities surveyed last fall by The Chronicle of Higher Education, Inc., 41% of the respondents said hackers had succeeded in penetrating their systems. Fully 53% reported denial-of-service attacks, and 14% reported unauthorized access to student data.

George Mason University discovered in January 2005 that computer hackers captured the names, Social Security numbers, photographs and other information of more than 30,000 students and staff. The hackers used software with a remote probing tool and password-cracking tools. The computer the information was stolen from wasn't protected by a firewall, a tool designed to prevent unauthorized access.

University of Northern Colorado reported in January 2005 that a computer hard drive containing personal information (Social Security and bank account numbers, names, and other information) for 30,000 people was reported missing. University officials said they don't know if the drive was misplaced or stolen, but campus police have launched a criminal investigation.

University of California, San Diego had three security breaches within 18 months. In mid-November 2004, a hacker breached two computers with Social Security numbers and names of about 3,500 students and alumni. Earlier, hackers breached security at the San Diego Supercomputer Center and at the University's Business and Financial Services Department, gaining access to four computers storing Social Security and driver license numbers for 380,000 UCSD students, alumni, faculty, employees and applicants. In December 2003, information for more than 178,000 students, alumni and employees was exposed when hackers broke into a computer system.

University of California, Berkeley reported in October 2004 that unknown hackers had gained access to a database containing confidential information on 1.4 million recipients and providers participating in a California Department of Social Services program. The information was data a researcher had collected on elderly people and individuals who provided in-home care to seniors.

University of Colorado reported 1,000 continuing education students had their personal information compromised by a joy-rider who broke into the system without actually taking identifying information.

University of California, Los Angeles disclosed in June 2004 that a laptop containing personal Information on 145,000 blood donors was missing.

University of Missouri, Kansas City reported in January 2004 that a hacker cracked into its security system, compromising about 17,000 student, staff and faculty passwords for the university email system. The Internet system was shut down and users were forced to change their passwords, because UMKC employs a single-sign-on system designed to make it easier for users to reach the systems with a single username and password.

Georgia Institute of Technology reported in March 2003 that a server containing credit card information on more than 57,000 patrons of the Institute's arts and theater program was breached.

University of Texas reported in March 2003 that personal information for 37,000 students and staffers had been stolen from a database. The University reported it spent $167,000 responding to the security breach and warning people of possible identity theft.

Wichita State University reported in February 2005 that someone had accessed three of its servers. The servers held data on as many as 8,000 students, faculty, and former students.

Kansas State University reported in February 2005 that someone had successfully launched a denial of service attack and its Internet was down for 1.5-2 hours

Information Technology Represents A Significant Expense for Universities

In this audit, we reviewed three of the Regents' institutions, Emporia State University, Kansas State University, and the University of Kansas. In Fiscal Year 2004, the three institutions combined had a total budget of more than $1.1 billion, and spent $33 million on central information technology systems. In addition, individual departments, research institutes, and others had computer systems not accounted for in this figure. For the central IT function alone:

- The University of Kansas (excluding the Medical Center) spent $14 million, and had a staff of 193 FTE.
- Kansas State University spent $14 million, and had a staff of 171 FTE.
- Emporia State University spent $3 million, and had a staff of 34.5 FTE.

KU is completing a multi-year project to move all of its central administrative systems from a mainframe system to a server-based system. Emporia State and Kansas State are working on similar projects.

How Well Do Universities Manage the Security of Their Information Systems?

ANSWER IN BRIEF:	*In many areas, security practices described by university officials seemed adequate, but they hadn't been adopted as official written policies. We found instances of inadequate or nonexistent security policies at all three universities we reviewed. We also found that all three universities need to elevate the role of their IT Security Officer. The Universities protected themselves from viruses coming from the residence halls, but Emporia State needs to do more to help protect students in its residence halls from viruses. KU and K-State provide security awareness training to staff and students, but more needs to be done at Emporia State.*

In Many Areas, Security Practices Described by University Officials Seemed Adequate, But Hadn't Been Put Into Official Written Policies

The bulk of our work in this audit involved evaluating universities' security policies against a list of 54 best practices. *Figure I-1* on the next page lists these best practices, and highlights the areas where each university reported following a practice that appeared to be adequate, but didn't have a written security policy.

As the figure shows, the three areas where unwritten policies were most common were access controls (passwords), operations, and physical security.

Lack of written policies exposes the universities to increased risk that intended procedures won't be followed. Written policies are the way that upper-level managers communicate their intent on significant issues. Ordinarily, written policies are the result of a studied decision-making process involving representatives of important groups within the organization.

Unwritten policies or practices, on the other hand, tend to develop in the absence of written policies and arise through much less robust means. They have neither the weight of written policy nor the reach. In diverse organizations, it's nearly impossible for a "practice" to become or remain consistent across the organization because it depends on word of mouth and memory. Lastly, enforcing a "practice" is extremely difficult.

In computer security, the risks of not having codified practices are tremendous. Security covers a broad range of subject matter, most of which is technical. If security policies aren't written down, people tend to make up their own ways of doing things, or don't do anything at all. It takes only one "hole" in an organization's computer security for its data to be compromised.

Figure I-1

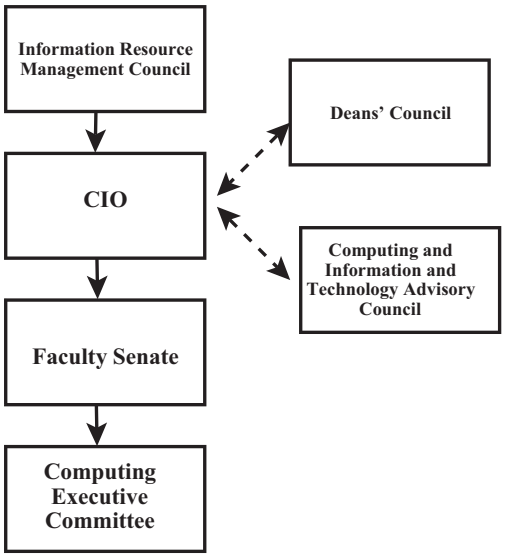
Areas With Adequate Practices Reported, But No Written Policies *(shaded)*

Shaded cells reflect areas where an adequate practice has been reported, but has not been adopted as a written policy.
Unshaded cells reflect areas where there is an adequate written policy OR where a policy or practice is inadequate or nonexistent.

	Best Practice	KU	K-State	Emporia
Access Controls	Addresses how much access they allow vendors	■	■	
	Each person should have a unique UserIDs			■
	Specifies requirements for passwords			
	Users are limited to the least amount of privileges and access they need.	■		■
	Requires screen saver passwords to be enabled			■
	Specifies rules to remote access of network		■	
	Requires default passwords on computer equipment to be changed	■	■	■
	Requires all trust relationships with other computer systems be approved	■		
	When employees are terminated, the policy requires an exit interview all keys be collected and all computer access disabled		■	
Data Controls	Data owners establish access rights to their data sets	■		■
	Access to files with confidential information and data sharing between applications should be authorized by the data owner.	■		■
	Agency data is classified according to its sensitivity			■
	Prohibits confidential data from being transmitted unencrypted over wireless phone, modem or wireless LAN			■
	Prohibits confidential data from being transmitted unencrypted over the internet			
	Requires confidential data stored on a portable computer to be encrypted.			■
General Controls	General policy statement and scope			■
	Specifies responsibilities of agency directors, data owners, users, security officers			■
	All resources are to be used to conduct state business except as authorized by agency; Agency has appropriate use policy			
	Restricts copying of proprietary software in violation of the license agreement			
	The message on the screen meets legal requirements			
	Prohibits the use of unlicensed software			
	Has an enforcement clause for violations of the security policy			
Incident Response	Specifies how to report incidents		■	■
	Specifies responsibilities of security staff in investigating incidents			
	Requires unauthorized access attempts to be investigated.		■	■
	If an unauthorized access attempt is successful, requires corrective action be taken to correct the vulnerability.		■	■
Operations	Requires agency to have a continuity plan			
	Requires audit trails to be maintained to track security administrator activity and to detect security violations.	■		
	Specifies what events to log	■		
	List of things to log meets requirements on page 11 of guidelines	■		
	Requires periodic review of logs	■		
	Requires the use of anti-virus software which is updated regularly	■		■
	Requires data to be backed up regularly and stored securely	■	■	■
	Doesn't allow modems to be enabled on computers hooked to the network			
	Doesn't allow the use of modems other than those installed by agency computer staff			■
	Requires servers, databases, and workstations to be current on security patches	■		
	Requires a system of configuration management for servers, workstations and firewalls	■	■	
Physical Security	Requires switches and other network hardware to be protected.			■
	Requires servers to be locked in rooms	■		■
	Requires wiring closets to be locked			■
	Requires secure storage for laptops	■	■	■
	Requires office doors to be locked after hours	■	■	■
	UPS required to be used on critical equipment	■	■	■
System Development	Security plan required for all projects under development			
	Specifies what a system security plan should include			
	When systems are changed, documentation should address impact of change on security system.	■		
	Each phase of system development should address security and audit controls.			
	Requires testing be done in separate environment from production.	■	■	■
Security Management	Requires security awareness training for users	■		
	Requires risk assessment to be done periodically.	■		
	Requires periodic auditing or monitoring of security		■	
	If the agency uses an intrusion detection system, the policy requires a policy on how the system will be used.	■	■	
	Requires periodic use of vulnerability checking software.	■		
	The organization have a firewall policy (ISO 17799.9.4.6)	■		

Source: LPA Analysis

Figure I-2
K-State's IT Policy-Setting Process



Source: Kansas State University
Solid line indicates approval required, dashed line indicates review and comment required

The policy-setting process at all three sample universities is very time-consuming, and can result in "watered-down" security policies. Policy development should involve input from the groups of users affected by the policy. In State agencies, there's often a security committee or an information technology committee made up of representatives of the different areas of the agency to aid in developing policies. The security officer or chief information officer takes the proposed policy to that committee, which provides needed input. When the policy is accepted, the committee sends the policy to the Secretary for his or her approval.

At the universities we reviewed, this concept has been taken to the extreme:

- before a policy can be ratified, it must receive the comments, and may have to receive the approval, of many different committees, as shown in *Figure I-2* for K-State.
- draft policies may be modified at each step to meet the concerns of the different committees, which can create problems. For example, KU's first draft for its new password policy was very strong. But several months later, after it had gone part way through the review process, that policy had been watered down to such an extent that it no longer meets minimum best practices. It still hasn't made it through the process.
- the process can be very time-consuming. One university estimated it could take a year to get through the review and approval process. At Emporia State, the last comprehensive security policy never made it through the process.

University officials pointed out that the process is very useful in educating users and achieving buy-in for the policies. K-State has adopted a procedure that can mitigate the delays caused by the university's policy review and approval process. For important policies, K-State officials sometimes create an interim policy that's in effect while the draft policy is going through the standard policy-setting process.

We Found Instances of Inadequate Or Nonexistent Security Policies At All Three Sample Universities

A major part of this audit involved evaluating the universities' security policies. We found a number of problems at each university, some of which were significant. Few of those problems can be discussed in any detail in a public report without putting the universities at greater risk. Therefore, the confidential report for each university lists specific best practices where the schools' security policies were inadequate to provide the necessary protection, or where no policies had been established.

This public report briefly and generically highlights problems we saw in each area of best practice. No problems were listed in *Figure I-3* on the pages 11-12 unless they were found at more than one university.

All Three Universities Need to Elevate the Role Of Their IT Security Officer

A security officer should report directly either to a chief executive (in universities, this might be the Provost), or to the Chief Information Officer. This is necessary because security officers need to be free to voice their security concerns with officials in a position to act and effect change across the organization. In addition, in monitoring security, helping set and enforce policy, and reacting to security incidents, the security officer needs to sit high enough in the organization to be perceived as having authority

We found problems with one or both of these areas at all three universities.

- **Emporia State doesn't have a dedicated security officer**. Instead, the Associate Vice President for Technology and Computing Services (essentially the chief information officer) has the main responsibility for security, and the wide-area network manager handles many of the security duties. In effect, Emporia State has no security officer–both these individuals have many other responsibilities.

- **K-State's security officer has less authority and more narrow responsibilities than desirable**. The security officer reports to the Chief Information Officer through his manager. The risk here is twofold: the security officer may not be able to freely voice his concerns, and he sits too low in the organization to effect the amount of control needed for the job.

  In addition, the security officer doesn't play a large role in security monitoring. Those duties are largely carried out by network staff.

Figure I-3 Common Problems in Security Policies	
Access Control	Passwords are the primary means of access control. We found at least some deficiencies in each university's password policies.
	Password-protected screen savers are important controls that can help prevent someone from sitting down at an empty desk and accessing the network. The universities didn't always enforce their use across campus.
	The universities generally had adequate systems to ensure that computer accounts for employees who left the university were disabled. However, those systems didn't always work as well as they should. We found accounts of past employees at each university that hadn't been disabled. One university depended on access to critical applications being immediately disabled, but had kept nearly 100 past employees' network accounts active for several months.
Data Controls	Over the last few years, there have been rapidly increasing problems across the country with the loss of confidential data. It's vitally important that an organization be aware of what data need to be protected. This requires a formal effort to classify all data by its confidentiality and sensitivity, so that proper controls can be designed to protect the data and ensure that everyone is clear on how to handle different types of data. Because of federal regulations, universities are being required to classify several types of data such as student records and health care data, but haven't always classified other data. In other cases, staff responsible for the servers containing the data may have good knowledge of classifications, but aren't sure how it is handled after it leaves their custody.
	Whenever confidential data are transmitted over the internet there is risk. While data are being sent from one place to another, there are many opportunities for people to see it or copy it without users at the sending or receiving end knowing anything has happened. To prevent this, best practices call for the data to be encrypted while in transit. That way, anyone who intercepts it can't read it. The universities don't all require such data to be encrypted. One university policy requires data to be encrypted in transit if it's economically feasible.
General	Network banners warn off unauthorized users and notify authorized users that their communications are subject to monitoring. Banners need to be strengthened and more widely used to increase universities' ability to identify and prosecute wrongdoing.

Incidence Response	Incident response plans lay out what security staff are to do in response to different types of security incidents. Without plans, valuable time can be wasted and important evidence may be destroyed. The universities didn't all have written plans.
Operations	One important operational control is having business continuity plans or disaster-recovery plans. Such plans are extremely important in the event of emergencies or disasters. None of the universities had up-to-date plans.
	Another important aspect of operations is accountability. In the event of a security incident, it's important to be able to track what actions people took. Audit or security logs on servers and workstations provide these records, and are the only way to tell what users did. However, they generally don't come "enabled" on computers—the user has to turn them on. Policies are necessary to specify what types of actions need to be logged, and how they are to be reviewed. We found few policies at the universities on logging, and where logging was used, we found inconsistent practices.
System Development	A prevalent problem in information technology is that new applications often are designed without security, which ends up being tacked on at the end of the project. This results in software that isn't as secure as it should be, and increases costs. Best practices call for security to be considered at all stages of development, for security plans to be developed for applications, and for user documentation to be updated to reflect the impact on security when an existing application has been modified. We found problems in nearly all these areas at the universities. In some cases, development staff told us they think about security throughout a project, but don't document it. In other cases security is handled well in administrative systems, but central IT staff have little control over how departmental projects are done. At one university, systems are checked at the end of the project by the security officer. While this is a good control, it is too late in the process.
Security Management	Firewalls provide essential protection at the border of networks and at strategic places in a university's network. We found problems with where firewalls were placed or how they were used.
	Vulnerability-checking software is a useful way to make security monitoring more efficient and effective. It wasn't being used to maximum capacity in some universities.

Source: LPA Analysis of university security policies and practices

While these staff are well-qualified, it puts them in the situation of monitoring themselves.

- **The security officer at KU has appropriate authority, but is placed too low in the organization**. As at K-State, the security officer at KU reports to the Chief Information Officer through his immediate manager. We think this can create the perception that he is the security officer only for the data center, not for the entire university, and others may challenge his authority.

  The Chief Information Officer told us she essentially shares the CIO duties with the security officer's manager, so she thinks the security officer does report to a high enough level. While this argument has some merit, it depends too much on personalities to resolve the potential issues. A different Chief Information Officer might not share those responsibilities.

The Overall Security Function Is Strongest at The Larger Universities

As described in the Overview, the universities have been subject to a number of fairly significant computer attacks in recent years. Although even the best security policies can't prevent all such attacks, they can help minimize the harm such attacks can cause.

KU and K-State have begun taking a more proactive approach to managing computer security in the last few years. They've established policies and procedures in many areas, and have established a "security structure" throughout the university.

At KU, a security officer and four staff members have been dedicated to security. KU also has a Security Council composed of the four IT leadership positions, the security officer, an assistant director for networking, and the policy and planning coordinator. The Chief Information Officer briefs the University's Provost monthly, as well as whenever there's a security incident.

KU Has Been Proactive in Reacting to Its Serious Security Incidents

KU has probably had more high-profile security incidents than any other State agency--three within the past two years. In January 2003, staff discovered that hackers had compromised the server containing information on 1,450 international students at the University, including their passport information. In April 2004 hackers compromised a server at the Watkins Health Center containing medical information on past patients. Finally, in November 2004 hackers again compromised a server, this time a server at the Life Span Institute at Parsons State Hospital, which contained confidential employee data, and confidential medical data. In each of these incidents, confidential data were either lost, or potentially lost. In each case the university took action to warn all people whose personal data was potentially lost.

Since 2002, KU has undertaken an extensive effort to improve its computer security. It has put together a fairly robust security function headed by a well-qualified security officer. Officials from KU and K-State developed a thorough risk and vulnerability assessment document, and KU is using it as a planning document to identify security policies it is lacking. KU also used the document to make an organized plan to work towards becoming certified under the Code of Practice for Information Security Management, a widely accepted set of standards for security. Finally, after each serious security incident, KU officials conducted "lessons learned" meetings to figure out how to improve their security management. KU security and policy staff have made several presentations on this topic to other organizations so others can learn from their mistakes.

At K-State, security efforts are lead by the Chief Information Officer, the networking manager, and a security officer. The 20-member Security Incident Response Team, created initially to respond to security incidents, has been charged with security planning, procedure development, security research, security audit, and incident response. Its includes individuals with expertise in security from every college and administrative area, and its members are assigned to this area for a minimum of three-tenths time from their various units on campus. All policy related to information technology is routed through the Information Resource Management Council.

The security structure at Emporia State is by far the weakest. While ultimately the Chief Information Officer is responsible for security, this position has had significant turnover over the past decade, resulting in a lack of direction and momentum in developing a security structure. The network manager has taken on some of the tasks of a security officer, but he isn't in a position to have authority over other areas. The lack of a continuous Chief Information Officer to set a vison and push for specific actions likely has contributed to security policies being held up in the Computer Advisory Committee and the Faculty Senate, both of which must approve the policies.

Both KU and K-State have taken steps to expand the reach of the central security function into the academic departments and administrative units. Information technology at universities tends to be very diversified, making security more difficult.

KU and K-State have both created teams made up of technical staff representing each department. These staff are provided training in various areas of security, such as security awareness and incident response. This gives the security officer a trained point-of-contact in each department. These department contacts monitor IT security in their unit, communicate security issues to their constituents, ensure that the devices on the network comply with security policy, and help respond to security incidents.

Each University Protects Itself from Viruses Coming from the Residence Halls, But Emporia State Needs To Do More To Help Protect Its Students from Viruses

Residence halls on university campus provide challenges for system network administrators. The university has no control over the types of computers students bring, or what software is on their computers This environment makes the residence halls susceptible to widespread virus infections.

Both KU and K-State had severe computer virus outbreaks in residence halls last year that affected the universities' computer networks. Both subsequently developed and provided students with anti-virus programs to protect their computers, and report that there have been no outbreaks this year.

KU purchased a campus-wide license for anti-virus software that provides the software free-of-charge to the students. The University requires students to have the software on their computers before they can log onto the network in the residence halls. In addition, KU has a system that checks students' computers for current anti-virus updates and security patches—if the computers aren't current, students can't log onto the network.

KSU also purchased a campus-wide license for anti-virus software to cover student computers. It then launched Operation PC in Fall 2004, where each student was required to have IT staff remove software viruses and apply security patches, install the managed version of an anti-virus product, and register their computer before the student was allowed to connect into the University's network. University officials reported updating 3,000 computers in three days. This process will be repeated at the beginning of each Fall semester

Emporia State needs to do more to prevent student computers from becoming infected with viruses. Emporia State has placed the residence halls on isolated networks, and placed a firewall between the residence halls and the rest of the university. This action keeps student computers from infecting the university network. However, it has taken few steps to ensure that student computers have current anti-virus software, or that appropriate patches have been applied to their software. As a result, student computers are susceptible to viruses, trojan horses, and worms when they hook into the network in the residence halls, and viruses can spread freely throughout the residence halls.

Security Awareness Training Needs To Be Beefed-Up at Emporia State University

User awareness of security issues is a key element in maintaining the integrity of computer systems. Regular users generally are considered to be the most significant security risk in any organization. Therefore, it's imperative to educate employees about security and the important role they have in the process.

For example, anti-virus software is always a step behind the viruses themselves, and in the interim before the software is updated and downloaded onto individual computers, a user who has learned not to open a document from an unknown sender, or one with an ".exe" tag, is the first line of defense.

Although Emporia State has placed security awareness information on its IT website, it does little else to make staff and students aware of IT security issues. By contrast, KU has initiated a mandatory university-wide program to help local IT staff better

understand security issues and become better trained at dealing with them. It also makes presentations to departments and faculty groups on campus.

And both KU and K-State reach out to students: KU publishes technology tips in the student newspaper, and the K-State IT Assistance Center publishes a weekly newsletter that contains basic security tips such as how to protect yourself from attacks, and the importance of applying security patches.

CONCLUSION

In many ways, universities present the most challenging environment for security in State government. Unlike most agencies, their business model demands openness in their networks, and they have a large number of different kinds of users with very diverse needs. All these needs can be met and still maintain a secure environment, but to do so takes skill and good communication on the part of the security function, and clear support from upper-level management. Progress in securing these complex environments is being made to varying degrees at each of the three universities we reviewed, but all seem to be missing some of the basics.

With computer security, written policies are essential. Because of the level of risk and the technical nature of the subject, it is vitally important that everybody know the "rules," that people do things consistently, and that users know their roles. In addition, because security is sometimes inconvenient for people, they need to know that upper-level management supports strong security measures. The only way to accomplish all these things is through written policies and procedures. "Unwritten rules" don't work in large and diverse organizations. We found some good practices at all three universities, and the University of Kansas is in the middle of a large effort to identify and adopt needed security policies. However, as the figure on page eight shows, all three have a long way to go in this area. For the needed policies to be adopted successfully, the universities must address their unwieldy policy-setting processes. For all the needed policies to get through the universities' current approval processes would probably take years. They need to find some way to enable all the important groups of users to have input into the policies, and get them approved in a timely manner.

Finally, the universities need to upgrade the level of the security function and the security officer role. That function is important in monitoring the effectiveness of the policies, and keeping the process dynamic.

The following recommendations pertain to findings presented in this public report. The confidential reports contain additional recommendations for security weaknesses we found at specific universities.

RECOMMENDATIONS

1. To ensure that the universities manage the security of their systems effectively, they should do the following:
   a. develop written policies to implement current adequate, but unwritten, practices identified in this report
   b. develop written policies in the areas identified generally in this report—and detailed in the confidential reports—as lacking adequate practices
   c. streamline their processes for approving written security policies, so that policies that meet the standards of best practices can be adopted on a timely basis.

2. To ensure that the information security function has the organizational independence and authority it needs to be effective, the universities should do the following:
   a. at KU, the security officer should report directly to the Chief Information Officer
   b. at K-State, the duties of the security officer should be reconfigured to include more involvement in monitoring security. In addition, the security officer should report to the Chief Information Officer.
   c. at Emporia State, a security officer position should be established. That position should report to the Chief Information Officer.

3. To ensure that information security is handled more consistently throughout their campuses, the universities should:
   a. increase security training for technical staff, both centrally and in the departments
   b. expand communication between the central staff and the departments regarding basic controls and procedures for responding to incidents.

4. To ensure that users are better protected and better educated to serve as the first line of defense in computer security, the universities should do the following:
   a. make users more aware of security issues and how to protect themselves. This could be done through articles in the school newspapers, email notices, web-sites, and so on.
   b. require every system connecting into the university networks to have the current software patches and the most current virus-protection software.

Appendix A

SCOPE STATEMENT

Regents Information Systems:
Reviewing Computer Security at Various Universities

In fiscal year 2003, the Regents' institutions spent about $50 million on their core information systems; this figure does not include the salaries for the unclassified staff who make up more than half the total IT staff. In all, about 620 FTE staff develop, maintain, support, and control the central information systems for the universities. The universities are at various stages of re-engineering their information systems, developing and implementing new applications, instituting wireless access, and expanding accessability from the Internet.

During the last few years, concerns have been expressed about the lack of monitoring of State computer systems. Each year State agencies become more dependent on their computer systems and on the data those systems contain to make decisions and fulfill their missions. More and more, computing is moving out of the data center and into the hands of staff who use the data to make decisions. Computers and computer networks also are being used to communicate with the public, provide services, and conduct business.

These are positive developments that can result in increased efficiency and effectiveness and better service. However, significant risks are associated with these advances in technology that agencies should be addressing and managing. In fact, over the last two years there have been several high-profile computer intrusions at Regents' institutions that resulted in sensitive student and staff data being stolen. At present there is little oversight of agencies' computer operations to monitor whether these risks are being adequately managed.

To help address these risks, the Legislative Post Audit Committee approved an ongoing series of information system audits to be done as an adjunct to the Division's compliance and control audits. This audit looks at universities' information systems, and will address the following questions:

1. How well do universities manage the security of their information systems? To answer this question, we will choose a sample of three universities and review each universities' system of managing its information system security, with emphasis on how the security functions are structured and managed, and on security policies and procedures.

2. How well do the universities carry out their security policies? This question will follow from the previous question, but will look in greater detail at how certain policies are carried out. The emphasis in this question will be on those areas we judge to be the most important or present the highest risk, such as how they respond to security incidents. Based on the results of question one, we will choose one or more universities to review for this question.

We anticipate releasing each question in a separate report.

Estimated time to Complete: 12-14 weeks for each question.

Appendix B

Agency Responses

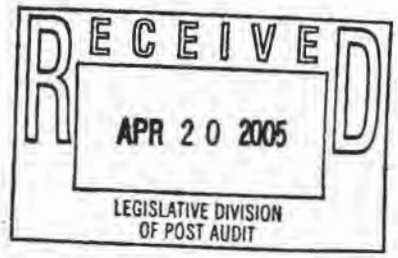
On April 13-14, 2005, we provided copies of the draft audit report to the Board of Regents, the University of Kansas, Kansas State University, and Emporia State University. Their responses are included in this appendix.

KANSAS BOARD OF REGENTS

1000 SW JACKSON • SUITE 520 • TOPEKA, KS 66612-1368

TELEPHONE – 785-296-3421
FAX – 785-296-0983
www.kansasregents.org

April 20, 2005



Barb Hinton, Legislative Post Auditor
Legislative Division of Post Audit
800 S.W. Jackson St., Suite 1200
Topeka, KS 66612-2212

Dear Ms. Hinton:

Thank you for providing the Kansas Board of Regents with the opportunity to respond to the Legislative Division of Post Audit IT Security audit of the University of Kansas, Kansas State University, and Emporia State University. This audit is particularly timely because it comes on the heels of the Board's effort to sharpen its focus upon and elevate the profile of IT Security issues within the State university system.

Over the last year, the State universities have been working through a revitalized Regents Information Technology Council (RITC) to develop a Regents IT security framework and self-assessment tool initiative pursuant to ITEC Policy 4310.

Under this policy, Board of Regents staff has been engaged with the universities to establish an IT security self-assessment framework and tool. Results derived from the application of this tool will be reported to the Board annually. RITC is incorporating both the ISO 17799 standard and Educause "Effective Practices for IT Security" guidelines into this framework and tool. This approach has been reviewed and endorsed by the Educause/Internet2 Security Task Force.

IT and data security is something that our office and campuses take very seriously. The development of a Regents IT Security framework and self-assessment tool constitutes only a part of what we hope to accomplish in this area as a result of RITC's re-invigoration. These issues are critically important to us and we believe that your agency's audit report will serve as a valuable roadmap as we work to address issues in this area. We look forward to working with the universities as they respond to your helpful recommendations.

Again, we thank you for the time and effort that your staff put into this audit process. We also appreciate the professionalism reflected in your work and the attitude of your staff. We will continue to look for ways to better address IT security on our campuses, and we look forward to working with you on this and other topics as they may arise.

Sincerely,

Reginald L. Robinson
President and CEO

cc: Chancellor Robert Hemenway, KU
President Jon Wefald, KSU
President Kay Schallenkamp, ESU
Brad Williams, KBOR
David Schmidt, Chairperson, RITC
Denise Moore, Executive CITO

The University of Kansas

RECEIVED
APR 20 2005
LEGISLATIVE DIVISION
OF POST AUDIT

Office of the Vice Provost
for Information Services

April 20, 2005

To: Allan Foster, Legislative Post Audit

From: Marilu Goodyear, Vice Provost for Information Services

Re: University of Kansas Responses to the Legislative Post Audit Computer Security Audit Report – **Public Report**

Attached are responses from the University of Kansas to recommendations in the *Computer Security Audit Report,* April 18, 2005, performed by the Legislative Division of Post Audit. We appreciated the opportunity to review our current policies and practices and share information on the challenges of maintaining a secure computing environment in institutions of higher education. As noted in a recent publication[1] from EDUCAUSE[2]:

> Certain aspects of higher education make direct transposition of business or government security procedures a challenge. The unique mission of higher education and its role in developing individuals is one distinctive feature. Another is an operational environment characterized by a transient student population, a residential environment, and the research enterprise. These attributes create security challenges. Institutions grapple with balancing security and higher education's core principles.
>
> Computer and network security is necessary but must be implemented with sensitivity to higher education's unique environment. Discussion among academic, technical, and security communities will allow higher education to find the appropriate balance between historic principles and current computer and network security needs.

Finally, we would like to note that KU is in the process of reviewing and developing campus security-related policies and best practices. Our assessment framework is based on the ISO 17799 standard and the EDUCAUSE/Internet2 best practice guide. This approach has been reviewed and endorsed by the Educause/Internet2 Security Task Force and has been adopted by the Regents Universities for security planning and assessment. KU's initial policy and best practice development should be complete within the next year.

---

[1] Oblinger, Diane, Computer and Network Security and Higher Education's Core Values, EDUCAUSE Center for Academic Research (ECAR), *Research Bulletin*, vol. 2003, issue 6, March 18, 2003.

[2] EDUCAUSE is the national higher education IT professional association whose mission is to advance higher education by promoting the intelligent use of information technology. The current membership comprises more than 1,900 colleges, universities, and educational organizations, including 200 corporations, with 15,000 active members. http://www.educause.edu

Strong Hall • 1450 Jayhawk Blvd., Rm. 223 • Lawrence, KS 66045-7535 • (785) 864-4999 • Fax: (785) 864-0360

	Legislative Post Audit Report: Public Section	4/20/2005
	Report Recommendation	**University of Kansas Response**
1	To ensure that the universities manage the security of their systems effectively, they should do the following:	--------
1a	develop written policies to implement current adequate, but unwritten, practices identified in this report	Compliant written policy is under development and will reference the appropriate state and federal regulations the University is subject to.
1b	develop written policies in the areas identified generally in this report -- and detailed in the confidential reports -- as lacking adequate practices	Under development with specific deadlines as noted in the Confidental Report
1c	streamline their processes for approving written security policies, so that policies that meet the standards of best practices can be adopted on a timely basis	The University is close to completing our suite of information technology policies; we believe that keeping these policies current will be more efficient in the future. While we recognize the current process may appear cumbersome, applications in a research campus environment are complex and require extensive consultation with system administrators and users. The University has a clear line of authority for policy approval.
2	To ensure that the information security function has the organizational independence and authority it needs to be effective, the universities should do the following:	--------
2a	at KU, the security officer should report directly to the Chief Information Officer	The Security Policy outlines the IT Security Officer's authority on campus. The IT Security Officer, who reports to the Associate Vice Provost, has direct access to the Provost and the Vice Provost/CIO. The IT Security Officer job description will be modified to make this clear. The IT Security Officer communicates an average of 4-5 times daily with the Vice Provost Office.
3	To ensure that information security is handled more consistently throughout their campuses, the universities should:	--------
3a	increase security training for technical staff, both centrally and in the departments	KU's Security Policy currently requires that designated departmental staff become certified to be a technical liaison by successfully completing the appropriate training offered by the IT Security Office. In addition, a new Field Security Officer program, which includes more in-depth training, has been implemented.

3b	expand communications between the central staff and the departments regarding basic controls and procedures for responding to incidents	Our policy is that all technical staff must report security incidents through the central Help Desk to ensure a consistent response. This procedure is taught in the technical liaison and security awareness training programs (see Response to 3a).
4	To ensure that users are better protected and better educated to serve as the first line of defense in computer security, the universities should do the following:	
4a	make users more aware of security issues and how to protect themselves. This could be done through articles in the school newspapers, email notices, web-sites, and so on.	A robust security awareness program has been implemented.
4b	require every system connecting into university networks to have current software patches and the most current virus-protecting software.	KU employs a defense-in-depth strategy, and these two recommendations (patching and virus protection), are encouraged for all systems that access the network. This is already required for computers in ResNet and, when technically feasible, for our critical systems.

RECEIVED
APR 20 2005
LEGISLATIVE DIVISION
OF POST AUDIT

K-STATE
Kansas State University
Vice Provost for Academic Services and Technology
Dean of Continuing Education
108 Anderson Hall
Manhattan, KS 66506 -0113
785-532-6520
Fax: 785-532-6507
Email: beth@k-state.edu

April 18, 2005

Re: Response to the Board of Regents Information System: Computer Security Audit

From: Kansas State University
Elizabeth A. Unger
Vice Provost for Academic Services and Technology
Dean of Continuing Education

The Legislative Post Audit Review team that accomplished the information technology security audit at Kansas State University did a very professional job.

The University essentially concurs with the four recommendations found at the end of the document.

Response to recommendation 1: The University has already begun to codify the informal procedures and practices and needed policies are already underway. To address the issue of streamlining the policy approval process, it has been decided that all proposed policy submitted to IRMC will immediately become interim policy while it undergoes formal review.

Response to recommendation 2: The University will move the reporting structure for the University Security Officer to the position of a direct report to the Vice Provost for Academic Services and Technology and Dean of Continuing Education (VPAST/DCE) – essentially the CIO. There is only one person devoted full time to security that person interacts daily with the Chair of the University Information Security Council and the VPAST/DCE on a daily basis.

Response to recommendation 3: Security education and awareness training for both staff and users is essential and efforts to increase the current efforts are already being considered. Budget for these efforts is very limited and personnel to accomplish these tasks are also over committed. Having said that, three major educational efforts have been approved since receipt of the draft report; the SIRT will be provided with two formal training opportunities each year, the departmental security representatives will be provided with 3-5 workshops each year and the campus police department has agreed to have two officers trained in computer forensics to assist the University Information Security Council and the VPAST in policy formation, user education and incident response.

Response to recommendation 4: An evaluation of current weekly newsletters and home page security information effectiveness will be undertaken Discussion of various 'marketing" techniques to achieve these goals for the Fall, when our population changes by 4000-5000 new people, is underway. The university is in the second year of a two year phased project to "managed computing". This should be completed by July 1, 2006 and addresses 4b.

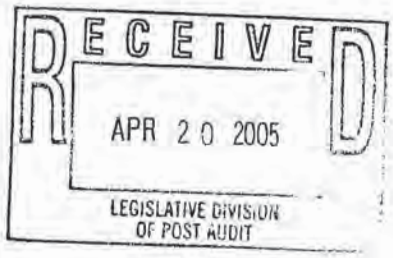
We wish to express our thanks to LPA for providing this assistance to the university.

EMPORIA STATE UNIVERSITY™

1200 Commercial St
Emporia, Kansas
66801-5087

620-341-5333
620-341-5553 fax
www.emporia.edu

OFFICE OF THE PRESIDENT
Campus Box 4001



April 20, 2005

Ms. Barbara J. Hinton, Legislative Post Auditor
Division of Legislative Post Audit
800 Southwest Jackson Street, Suite 1200
Topeka, KS 66612-2212

Dear Ms. Hinton,

Thank you for the opportunity to respond to the Legislative Post Audit's report "Board of Regents Information Systems: Reviewing computer security at various universities," specifically Emporia State University.

We appreciate the time that Auditors spent in reviewing our security practices and policies on the Emporia campus. As they pointed out in their report "universities have a long and deeply ingrained tradition of academic freedom and the free and open expression and exchange of ideas". There is, in other words, a healthy tension that exists on most university campuses between, on the one hand, the need to protect our information assets while at the same time meet the expectations of our faculty and students for the free flow of information. What we all seek is the appropriate balance between security and access. We also recognize our significant responsibility to protect the personal and confidential information that is maintained within our information systems.

By and large, we are in agreement with both the findings and the recommendations of the auditors.

To that end, we have already begun to adopt the recommendations:

Policies and procedures – we are drafting interim security policies and procedures that will be adopted and promulgated until each one is fully vetted and adopted through the University process;

Information Security Officer – we have identified funding, have drafted a job description and are conducting a nation-wide search for an appropriate information technology security professional. We hope to have an individual on staff in the summer;

Required patches and anti-virus software definitions on all computers and servers attached to the University's network – this is an issue that is complicated by the decentralized nature of many of our servers and the requirements of many commercial software products. However, we will make every effort to secure our server resources;

An Equal Opportunity Employer

Student Viruses –Robust anti-virus software is available to all of our students without cost. Additional efforts will be made to communicate with our students and to verify that their computers are protected from viruses.

Security training for technical staff – The focus of technical staff development over the coming year will be on security and related issues;

Security awareness training – The campus wide education program focusing on security related issues will be enhanced.

Thank you, once again, for providing an opportunity to respond to the security audit. Please thank the auditors, Molly Coplen and Allan Foster, for their excellent, thorough, professional, and helpful work.

Regards,

Kay Schallenkamp
President