COMPUTER SECURITY AUDIT REPORT

Regents' Information Systems: Following Up On Computer-Security Issues At Various Universities

A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
February 2009

09CC01

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 $13 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 Virgil Peck Jr., Chair
Representative Tom Burroughs
Representative John Grange
Representative Peggy Mast
Representative Tom Sawyer

Senator Terry Bruce, Vice-Chair
Senator Anthony Hensley
Senator Derek Schmidt
Senator Chris Steineger
Senator Dwyane Umbarger

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.ks.gov
Website: http://kslegislature.org/postaudit
Barbara J. Hinton, Legislative Post Auditor

DO YOU HAVE AN IDEA FOR IMPROVED GOVERNMENT EFFICIENCY OR COST SAVINGS?

The Legislative Post Audit Committee and the Legislative Division of Post Audit have launched an initiative to identify ways to help make State government more efficient. If you have an idea to share with us, send it to ideas@lpa.state.ks.us, or write to us at the address above.

You won't receive an individual response, but all ideas will be reviewed, and Legislative Post Audit will pass along the best ones to the Legislative Post Audit Committee.

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.ks.gov

February 2, 2009

To: Members, Legislative Post Audit Committee

Representative Virgil Peck Jr., Chair	Senator Terry Bruce, Vice-Chair
Representative Tom Burroughs	Senator Anthony Hensley
Representative John Grange	Senator Derek Schmidt
Representative Peggy Mast	Senator Chris Steineger
Representative Tom Sawyer	Senator Dwayne Umbarger

This report contains the findings, conclusions, and recommendations from our completed performance audit, *Regents' Information Systems: Following Up On Computer-Security Issues At Various Universities*.

The report includes several recommendations for Kansas State University, Emporia State University, the University of Kansas, the Legislative Post Audit Committee, and the Joint Committee on Information Technology. 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.

Barbara J. Hinton
Legislative Post Auditor

READER'S GUIDE

The Big Picture

Executive Summary	Provides an overview of the questions we asked and the answers we found
Conclusions and Recommendations	Located at the end of the report sections, and referenced in the Executive Summary
Agency Response	Included as the last Appendix in the report
List of Figures	Lists all figures used in the report and their location (as shown at the end of the Executive Summary)

The Details

"At-a-Glance Box"	Used to describe key aspects of the audited agency; generally appears in the first few pages of the main report
Side Headings	Point out key issues and findings
Charts, Tables, and Graphs	Visually help tell the story of what we found
Narrative Text Boxes	Highlight interesting information or provide detailed examples

This audit was conducted by Allan Foster. Scott Frank was the audit manager. If you need any additional information about the audit's findings, please contact Allan Foster at the Division's offices.

Legislative Division of Post Audit
800 SW Jackson Street, Suite 1200
Topeka, Kansas 66612

(785) 296-3792
E-mail: LPA@lpa.ks.gov
Web: www.kslegislature.org/postaudit

Table of Contents

Have the Regents' institutions adequately addressed the security recommendations from our 2005 computer-security audit?

Our 2005 Computer Security Audit of Three Regents' Universities Included a Large Number of Recommendations. ..... page 3

Overall, the Three Universities Have Fully Implemented Very Few of the Policy Recommendations From the 2005 Report. ..... page 5

The Three Universities Have Fully Implemented Most of the Non-Policy Recommendations From the 2005 Report. ..... page 8

Conclusion. ..... page 9-10
Recommendations for executive action ..... page 10
Recommendations for legislative action ..... page 11

List of Figures

Figure 1-1: Universities' Responses to 2005 Policy Recommendations ..... page 6-7
Figure 1-2: Universities' Responses to Non-Policy Recommendations ..... page 9

List of Appendices

Appendix A: Scope Statement ..... page 13
Appendix B: Agency Responses ..... page 15

Regents' Information Systems: Following Up On Computer-Security Issues At Various Universities

In fiscal year 2007, the Regents' institutions spent about $75 million on their core information systems. This figure does not include salary costs. In all, about 665 FTE staff develop, maintain, support, and control the information systems for the universities and the Board of Regents.

Our 2005 computer security audit of three Regents' institutions—Kansas State University, Emporia State University, and the University of Kansas—found a number of issues with those institutions' management and application of computer security. There were no written policies in many security areas, and in many instances there were no or inadequate policies in such areas as confidential data encryption, disaster recovery plans, and security planning for new computer systems.

To help address the risks that are related to the advances and expansion of technology in State government, the Legislative Post Audit Committee approved an ongoing series of computer security audits to be done as an adjunct to the Division's compliance and control audits. This audit follows up on the findings from our 2005 audit of universities' information systems.

This audit answers the following question:

Have the Regents' institutions adequately addressed the security recommendations from our 2005 computer-security audit?

To answer this question, we asked each of the three universities to list what they had done in response to each recommendation from the 2005 audit report, and to provide copies of all new policies written as a part of those efforts. We compared the policies the universities provided against the recommendations, and also tested several areas to see if what the universities actually were doing in those areas was adequate and followed policies. To review the non-policy recommendations we did some additional interviews and compared the universities' responses against the recommendations.

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 the public report.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our findings begin on page 3.

Have the Regents' Institutions Adequately Addressed the Security Recommendations From Our 2005 Computer-Security Audit?

ANSWER IN BRIEF: *Our 2005 computer-security audit of Kansas State University, Emporia State University, and the University of Kansas included a large number of recommendations, most of which were related to missing or inadequate security policies. We also made a number of non-policy recommendations concerning areas such as increasing the authority of the security officer position and the efficiency of the policy-setting process. In this audit, we found that the three universities have fully implemented very few of the policy recommendations from the 2005 report. While Emporia State University did the best, fully complying with 28 of 41 recommendations, Kansas State University complied with only 7 of 33, and the University of Kansas complied with only 5 of 33. We conducted further testing on six of the policy areas at the universities to evaluate their actual practices, and found significant access control problems at one university and a few other minor problems at the other universities. Finally, we found that the universities have implemented most of the non-policy recommendations from the 2005 audit report. These and other findings are discussed in more detail in the sections that follow.*

Our 2005 Computer Security Audit of Three Regents' Universities Included a Large Number of Recommendations

The 2005 computer security audit of Kansas State University, Emporia State University, and the University of Kansas was an in-depth assessment of the three universities' security management, policies, and activities. In conducting that audit, we selected 54 security best practices to review from the following policy areas:

- Access Controls—Protect information technology resources against unauthorized access. Among other things, these policies define the requirements for passwords, restrict what data users can access, and ensure terminated employees' access is disabled.
- Data Controls—Protect data integrity, including policies for classifying data according to sensitivity, and protecting confidential data as it moves within the organization and across the Internet.
- General Controls—Control the overall information technology environment in which systems and applications exist. They include such things as defining the appropriate use of computer equipment, and protecting copyrights.
- Incident Response—These policies are essential to minimize confusion and maximize the effectiveness of the response by specifying how staff should respond to security incidents.
- Operations—Ensure that the operational environment is secure by specifying how servers and other equipment should be configured, requiring that they are kept up-to-date with the most recent patches, and tracking the network activities of administrators.

- Physical Security—Protect the security of the physical environment in which information technology resources reside. These policies include keeping servers and network equipment in locked rooms, and physically securing laptops.

- System Development—Ensure that the development and modification of computer systems and applications are done with security in mind. These policies include requiring that security be considered throughout every stage of a development project, and maintaining documentation of security features.

- Security Management—Define an organization's program for managing security as a cycle of activity, including risk assessment, policy formation, promoting awareness, and monitoring security effectiveness.

For each best practice, we reviewed the universities' policies and procedures, and interviewed their officials to learn about their practices. We also tested several important areas in more depth to see if the actions actually taken by staff were adequate to meet best practices.

In addition to policy areas, the 2005 audit also looked at several non-policy areas at each university. The non-policy areas included issues such as how the universities organized their IT functions and infrastructure, how they managed security, how they developed and approved security policies, and how they promoted security awareness on the campus.

We found the following problems at the three universities:

- **The universities had relatively few written policies.** In many areas, the security practices they described were adequate, but they hadn't been adopted as official written policies. Without written policies, there is little consistency across the organization because practices depend on word of mouth or memory. In addition, it's difficult to enforce unwritten practices.

- **All three universities were missing or had adopted inadequate security policies or practices in a number of other areas.** For example, we found password problems at each of the universities, some of the universities didn't require confidential data to be protected while in transit, and some didn't have incident response procedures.

- **The policy approval process at all three universities was extremely cumbersome.** That made it difficult for the institutions to develop and approve security policies.

- **All three universities needed to elevate the role of their security officer**. They needed to do that either by adding to their responsibilities and authority, or by having their security officers report to someone higher in the organization.

Because of the sensitive nature of many of our findings, we issued several reports for our 2005 audit—a public report that covered the broad findings all three universities, and separate confidential reports

for each university that addressed the specific findings that were too sensitive to include in the public report.

Between the public and confidential reports, we made a total of 123 policy recommendations and 38 non-policy recommendations for the three universities to correct the issues we found. In their responses to the audit, all three universities generally agreed with the recommendations.

Overall, the Three Universities Have Fully Implemented Very Few of the Policy Recommendations From the 2005 Report

We had officials from each university provide us with explanations for what they had done in response to each of the 2005 recommendations, and support those explanations with copies of the applicable policies and procedures. We evaluated those responses and the supporting documents, assigning each to one of the following categories:

- Written Policy—The university had adopted a written policy that adequately addressed the recommendation.
- Draft Policy—The university had developed a written policy that adequately addressed the recommendation, but it hadn't yet been officially approved.
- Inadequate Policy—The university had adopted a written policy, but it didn't fully address the recommendation.
- No Policy—The university hadn't developed any written policy to address the recommendation.

As a final note, we decided to not follow up on a number of policy recommendations from our previous audit. Some recommendations were so closely related to other recommendations that they could be combined. Other recommendations referred to technology that was either outdated (e.g., phone modems) or was no longer in use at the universities. In sum, we followed up on a total of 107 recommended policy areas at the three universities. Our results are summarized in ***Figure 1-1*** on the following pages.

The left-hand side of the table shows the best practices included in the 2005 report, by category. The right-hand side of the table shows a summary of each university's response to their recommendations in each category. Because we only made recommendations for those best practices a university had problems with, the totals on the right often differ from the number of best practices shown on the left.

Figure 1-1
Universities' Responses to 2005 Policy Recommendations

Best Practice		Response	KU	K-State	Emporia
Access Controls	Addresses how much access they allow vendors	Written Policy	1	4	6
	Each person should have a unique UserIDs	Draft Policy	2	1	0
	Specifies requirements for passwords	Inadeq Policy	1	1	1
	Users are limited to the least amount of privileges and access they need	No Policy	3	2	1
	Requires screen saver passwords to be enabled	**Total**	**7**	**8**	**8**
	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	Written Policy	0	0	4
	Agency data is classified according to its sensitivity	Draft Policy	5	4	0
	Prohibits confidential data from being transmitted unencrypted over wireless phone, modem or wireless LAN	Inadeq Policy	0	0	0
	Prohibits confidential data from being transmitted unencrypted over the Internet	No Policy	0	0	1
	Requires confidential data stored on a portable computer to be encrypted	**Total**	**5**	**4**	**5**
General Controls	Specifies responsibilities of agency directors, data owners, users, security officers	Written Policy	0	0	1
	All resources are to be used to conduct state business except as authorized by agency; Agency has appropriate use policy	Draft Policy	0	0	0
	Restricts copying of proprietary software in violation of the license agreement	Inadeq Policy	0	0	1
	The message on the screen meets legal requirements	No Policy	1	1	0
	Prohibits the use of unlicensed software	**Total**	**1**	**1**	**2**
	Has an enforcement clause for violations of the security policy				
Incident Response	Specifies how to report incidents	Written Policy	0	3	3
	Specifies responsibilities of security staff in investigating incidents	Draft Policy	0	1	0
	Requires unauthorized access attempts to be investigated	Inadeq Policy	0	0	0
	If an unauthorized access attempt is successful, requires corrective action be taken to correct the vulnerability	No Policy	0	0	1
		Total	**0**	**4**	**4**

Figure 1-1
Universities' Responses to 2005 Policy Recommendations

Best Practice		Response	KU	K-State	Emporia
Operations	Requires agency to have a continuity plan	Written Policy	2	0	6
	Requires audit trails to be maintained to track security administrator activity and to detect security violations	Draft Policy	1	1	0
		Inadeq Policy	0	0	1
	Specifies what events to log	No Policy	4	5	2
	Requires periodic review of logs	**Total**	**7**	**6**	**9**
	Requires the use of anti-virus software which is updated regularly				
	Requires data to be backed up regularly and stored securely				
	Requires wireless access points to be approved by IT officials				
	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	Written Policy	0	0	3
	Requires servers to be locked in rooms	Draft Policy	1	0	0
	Requires secure storage for laptops	Inadeq Policy	0	0	0
	Requires office doors to be locked after hours	No Policy	4	3	2
	UPS required to be used on critical equipment	**Total**	**5**	**3**	**5**
System Development	Security plan required for all projects under development	Written Policy	0	0	2
	When systems are changed, documentation should address impact of change on security system	Draft Policy	0	0	0
		Inadeq Policy	0	0	1
	Each phase of system development should address security and audit controls	No Policy	4	4	1
		Total	**4**	**4**	**4**
	Requires testing be done in separate environment from production				
Security Management	Requires security awareness training for users	Written Policy	2	0	3
	Requires risk assessment to be done periodically	Draft Policy	2	0	0
	Requires periodic auditing or monitoring of security	Inadeq Policy	0	0	0
	Requires periodic use of vulnerability checking software	No Policy	0	3	1
	The organization have a firewall policy	**Total**	**4**	**3**	**4**
Overall Totals		Written Policy	5	7	28
		Draft Policy	11	7	0
		Inadeq Policy	1	1	4
		No Policy	16	18	9
		Total	**33**	**33**	**41**

Source: LPA analysis of universities' written policies and and procedures.

As the bottom section of the figure shows, the universities have fully implemented very few of the policy recommendations, although the responses varied among the three institutions:

- **Emporia State University has fully implemented 28 of 41 recommendations.** While this is the best compliance rate of the three universities, it is only two-thirds of the recommendations.
- **Kansas State University has fully implemented only 7 of 33 recommendations** and has another 7 recommendations in draft form.
- **The University of Kansas has fully implemented only 5 of 33 recommendations** and has another 11 recommendations in draft form.

We conducted further testing on six policies in the categories of access controls, operations, physical security, and security management based on what represented the highest areas of risk. In these reviews we looked at the universities' actual practices, such as how their servers were configured, or how their network equipment was protected. We compared what we found to the universities' policies and to best practice. Overall, we found few issues but we did note a couple of problems:

- There were significant problems with access controls at one university, and minor problems at the other two.
- There were minor problems with physical security at one university.

For security reasons we can't discuss these problems further in this public report, but more details are included in the specific universities' confidential reports.

The Three Universities Have Fully Implemented Most of the Non-Policy Recommendations From the 2005 Report

In addition to policy recommendations, the 2005 audit contained a number of recommendations that weren't policy related. For example we made recommendations about such things as the security officers' duties, staff and user training, and communication between the IT and departmental staff. As was the case with the policy recommendations, we didn't follow up on a couple of the non-policy recommendations because they were very expensive and didn't appear to be worth their cost in the current economic climate.

Our results are summarized in ***Figure 1-2*** on the next page.

Figure 1-2
Universities' Responses to Non-Policy Recommendations

Non-Policy Recommendation	Did the University Address This Adequately? (a)		
	KSU	ESU	KU
Establish or strenghten the security officer position	Yes	Yes	Yes
Streamline the policy approval process to make it more timely	Yes	Yes	Yes
Expand communications between central and departmental IT staff	Yes	Yes	Yes
Increase security training for central and departmental technical staff	Yes	**No**	**No**
Make users more aware of security issues	Yes	Yes	Yes
Confidential recommendation #1 (b)	Yes	NA	Yes
Confidential recommendation #2 (b)	**No**	**No**	NA
Confidential recommendation #3 (b)	NA	Yes	NA

(a) The universities didn't all receive the same recommendations. An entry of "NA" indicates that the recommendation didn't apply to the university.

(b) Because of the sensitivity of these recommendations, and the fact that not all of the unviersities have addressed them, they have been redacted from this public report. The specific recommendations can be found in each university's confidential report.

Source: LPA Analysis

As the figure above shows, there were only a couple of non-policy recommendations that weren't implemented by all three universities:

- One was a recommendation that the universities increase the security training for central and departmental IT staff. Both Emporia State University and the University of Kansas provided adequate training for their central IT staff, but not for their departmental IT staff. Training is important for departmental staff because they must handle security in their departments and respond to security incidents.

- The other non-policy recommendation that wasn't implemented was too sensitive to describe in this public report. It will be discussed in the universities' confidential reports.

Conclusion:

An organization's network and data must be secure at all times, and that security generally results from a well-designed, dynamic system of security management. Policies are the foundation of such a system, and are especially important in complex environments like universities. Because it isn't realistic to expect all IT staff to have a deep understanding of all aspects of security, the best way to ensure that staff know the right thing to do in all situations is to have a comprehensive set of security policies for people to refer to when necessary.

Despite their importance, the findings of this follow-up audit show that the three universities generally have done a poor job implementing the policy recommendations from the 2005 audit. While it may be difficult to develop and approve policies in a university setting because of the need to develop consensus among numerous constituencies, the universities have had three years to address these policy recommendations. Further, these recommendations all relate to standard best practices that aren't controversial, and that should be relatively easy to get approved. For example, it shouldn't be difficult to develop and approve policies that require data backups be stored securely, or that information security be monitored regularly. Whatever the reasons for not addressing these recommendations in the past, the universities should take care of them now.

Recommendations for Executive Action:

1. To ensure that universities effectively manage the security of their systems, they should develop and approve written security policies for all the policy recommendations from the 2005 audit that they haven't yet been fully addressed, including policies that currently are in draft form. (These policy areas are detailed in each university's confidential report.)

    a. The universities should submit written progress reports to the Legislative Division of Post Audit on May 1, 2009, September 1, 2009, and January 1, 2010. The reports should include a list of each policy recommendation from the university's confidential report, and the actions taken to address them. The Division will make those progress reports available to the Legislative Post Audit Committee, the Joint Committee on Information Technology, and any other appropriate legislative committees in such a way as to protect the confidential information included in them.

    b. The final implementation of all policies should be accomplished by January 1, 2010. In the event that not all policies have been addressed by that date, the universities should explain why, and should continue to submit progress reports on May 1, September 1, and January 1 of each year until all the policy areas have been fully addressed.

2. To ensure that all IT staff have the security knowledge needed to maintain security throughout the university, the University of Kansas and Emporia State University should provide on-going security training for <u>departmental</u> IT staff.

Recommendations for Legislative Action:	1.	To monitor the universities' compliance with the recommendations of this follow-up report, the Legislative Post Audit Committee and the Joint Committee on Information Technology should review the progress reports submitted by the universities, and after January 2010 should invite representatives from the three universities to report on their compliance at a Committee meeting.

APPENDIX A

Scope Statement

This appendix contains the scope statement for this follow-up audit of Kansas State University, Emporia State University, and the University of Kansas. This audit was conducted as part of the ongoing system security audit work authorized by the Legislative Post Audit Committee.

Regents' Information Systems:
Following Up on Computer Security Issues at Various Universities

In fiscal year 2007, the Regents' institutions spent about $75 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 information technology staff. In all, about 665 FTE staff develop, maintain, support, and control the information systems for the universities and the Board of Regents.

Our 2005 computer security audit of three Regents' institutions—Kansas State University, Emporia State University, and the University of Kansas—found a number of issues with those institutions' management and application of computer security. There were no written policies in many security areas, and in many instances there were no or inadequate policies in such areas as confidential data encryption, disaster recovery plans, and security planning for new computer systems.

To help address the risks that are related to the advances and expansion of technology in State government, the Legislative Post Audit Committee approved an ongoing series of computer security audits to be done as an adjunct to the Division's compliance and control audits. This audit follows up on the findings from our 2005 audit of universities' information systems, and will address the following question:

1. **Have the Regents' institutions adequately addressed the security recommendations from our 2005 computer security audit?** To answer this question, we will interview officials from the three universities we examined in the 2005 audit (Kansas State University, Emporia State University, and the University of Kansas), review and evaluate their policies and other documentation, and test selected computer controls as needed to determine what steps they've have taken to address our recommendations and whether those steps are adequate. We will conduct additional work as necessary.

Estimated Resources: 1 staff (10-12 weeks)

APPENDIX B

Agency Responses

On January 6, 2009 we provided copies of the complete draft audit report to the following agencies:

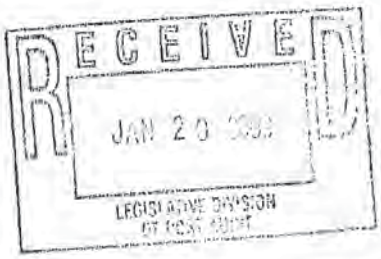
- the Board of Regents
- Kansas State University
- Emporia State University
- the University of Kansas

These agencies generally concurred with the report's findings, conclusions, and recommendations. The responses from the universities are included in this appendix. The President of the Board of Regents decided not to respond to the audit because we didn't make any recommendations to the Board.

In the responses to the confidential reports, both Kansas State and Emporia State had issues with a recommendation on access control. Emporia State asked for additional time to implement the recommendation, and Kansas State disagreed with the recommendation.

K-STATE
Kansas State University
Office of the President
110 Anderson Hall
Manhattan, KS 66506-0112
785-532-6221
Fax: 785-532-7639

January 16, 2009



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

Dear ~~Ms. Hinton:~~ Barbara,

Thank you for providing Kansas State University with the opportunity to respond to the follow-up performance audit, *Regents' Information Systems: Following Up on Computer Security Issues at Various Universities.* This letter serves as K-State's response to the public portion of the audit report, outlining actions we have taken or plan to take to implement the recommendations.

Recommendation 1: Develop and approve written security policies for all the policy recommendations from the 2005 audit that they have not yet fully addressed, including policies that currently are in draft form.

K-State is committed to completing written security policies addressing all the policy recommendations from the 2005 audit. An action plan has been created and additional staff resources allocated to develop the recommended policies and meet the reporting and compliance dates outlined in the audit reports. Specific plans for each recommendation are outlined in K-State's response to the confidential portion of the audit report. Of the policies in draft form at the time of the audit report, one has been formally approved so it is no longer a draft and the other is in the final stages of the approval process – it should be formally approved within the month.

Recommendation 2: Provide on-going security training for departmental IT staff.

Although Kansas State University is not mentioned in this recommendation, we recognize the importance of continuing to enhance IT security training and awareness for all faculty, staff, and students. Consequently, K-State recently hired on a temporary basis a cyber-security analyst with experience in state government and law enforcement to expand existing IT security training and awareness programs and develop new ones.

The security of our information and technology resources is a high priority at K-State, exemplified by the appointment of Chief Information Security Officer and allocation of additional staff on the IT security team. Thank you for the assistance this audit provides in identifying areas that need attention to strengthen our security posture. Please express our appreciation to Allan Foster for his professionalism during the audit process. It was a pleasure to work with him, as it was in 2005 during the initial security audit.

Sincerely,

Jon Wefald

Dr. Jon Wefald
President

dh

cc: Dr. Duane Nellis, Provost and Senior Vice President
Dr. Bruce Shubert, Vice President for Administration and Finance
Ms. Lynn Carlin, Interim Vice Provost for IT Services
Dr. James Lyall, Associate Vice Provost for IT Services

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

January 21, 2009

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

Dear Ms. Hinton,

I write this letter to assure you that I fully support ESU's response to the Legislative Division of Post Audit's report "Regents' Information Systems: Following Up on Computer-Security Issues At Various Universities." I have met with Michael Erickson for a complete review of the findings and our response, and I concur with each of the items in his response as well as the time frame within which we can make the needed changes.

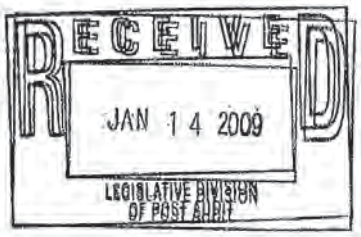
I assure you that the results of this follow up are a high priority for ESU. Data security is a critical priority for ESU as it should be for every institution of Higher Education. Should you wish to discuss any of the items in our response, I and Mr. Erickson would be happy to sit down with you or any member of the audit team to discuss the issues.

Sincerely,

Michael R. Lane
President

cc: Dr. Tes Mehring, Provost & Vice President for Academic Affairs and Student Life
cc: Mr. Michael Erickson, Associate Vice President, Technology and Computing Services and Chief Information Officer
cc: President Reginald Robinson, Kansas Board of Regents
cc: Ms. Donna Shank, Chair, Kansas Board of Regents

EMPORIA STATE UNIVERSITY™
1200 Commercial St.
Emporia, KS 66801-5087
USA
620-341-1200
www.emporia.edu



January 14, 2009

Barbara Hinton, Legislative Post Auditor
Legislative Division of 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 Division of Post Audit's report *"Regents' Information Systems: Following Up on Computer-Security Issues At Various Universities".*

We appreciate the time the Legislative Post Audit team spent in reviewing Emporia State University's progress in responding to recommendations from the 2005 computer-security audit. We acknowledge the results of their efforts and agree, for the most part, in their assessment of the areas in which our institution did not adequately address the recommendations made. However, we also feel it is important to note that significant progress has been made in both the policy and non-policy areas of information technology security at ESU.

During the past 3 years, Emporia State University has made significant strides in improving the security surrounding information technology. We have successfully created and implemented nearly 30 new policies addressing a breadth of issues which – as noted in the original report – can be 'difficult' to accomplish. In addition to the implementation of policy, ESU addressed a number of non-policy related recommendations – including the re-allocation of personnel resources to create the position of Information Security Officer, in increasing communication to faculty, staff, and students regarding the importance of IT security, as well as other areas. Finally, ESU has implemented many security standards, procedures, and best practices as part of an overall IT security management strategy.

As a result of this report and as a part of the continuing effort to improve our overall approach to IT security at ESU, we offer the following responses and proposed actions to address each of the report's recommendations:

Recommendation 1:
ESU will develop new policies or revise existing policies as needed to address each of the policy recommendations from the 2005 audit that have not been fully addressed. Specific responses to each of the policies appropriate to ESU can be found in our response to the confidential report.

a. We will submit written progress reports to the Legislative Division of Post Audit as requested.
b. We will move quickly to put draft policies in place and pursue full implementation as quickly as possible.

Recommendation 2
ESU will develop on-going security training appropriate for departmental IT staff, identify the appropriate audience for such training, and carry out training session(s) for all identified staff prior to the end of this calendar year.

These efforts will be directed by our Information Security Officer and overseen by myself as Chief Information Officer in an effort to meet and exceed the recommendations of this audit report. We have reviewed each of the issues and our responses with President Lane and have his full support in addressing the concerns identified.

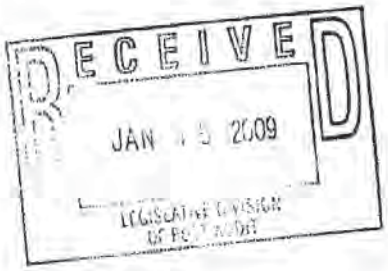
Thank you, once again, for providing an opportunity to respond to this report on the follow-up audit. In addition, we would like to thank Allan Foster for his efforts and professionalism as a part of this process.

Sincerely,

Michael D. Erickson
Associate Vice President, Technology and Computing Services
Chief Information Officer

cc: Dr. Michael R. Lane, President
cc: Dr. Tes Mehring, Provost & Vice President for Academic Affairs and Student Life

KU THE UNIVERSITY OF KANSAS



January 15, 2009

Barbara Hinton, Legislative Post Auditor
Legislative Division of Post Audit
800 SW Jackson St, Suite 1200
Topeka, KS 66612-2212

Dear Ms. Hinton:

I am pleased to provide the University of Kansas' response to the *Regents' Information Systems: Following Up on Computer Security Issues at Various Universities* dated January 6, 2009.

The University manages its security infrastructure using a risk management approach, recognizing the imperative to mitigate risks through technology intervention and change in practices. As noted by the findings, many of the technical, physical and administrative controls currently implemented reflect high risk and high impact areas to the University, such as those that fall under HIPAA and PCI regulations.

KU has continued to make progress toward building an optimally secure information security environment. The outcomes of central IT reorganization and sustained attention to security include current campus wide initiatives towards standardization of hardware, software, tools and KU IT staff expertise. These initiatives include the implementation of consistent, effective information management and information infrastructure procedures and policies.

KU has a highly decentralized environment and academic culture. These characteristics of the institution factored into policy making and implementation of new practices in order to produce meaningful and sustainable security outcomes. Toward this end, the University is actively engaging the campus through education, standardization, and the deployment of effective administrative procedural and policy controls. This strategy is evidenced by the draft information management policies that were reviewed during the review process.

We anticipate the finalization of pending draft policies and the implementation relevant technical initiatives during 2009.

Regards,

Denise Stephens
Vice Provost for Information Services and CIO
For Robert Hemenway
Chancellor for the University of Kansas

Enclosures

Cc: Robert Hemenway

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

KU THE UNIVERSITY OF KANSAS
Office of the Chancellor

January 16, 2009

Barbara Hinton
Legislative Division of Post Audit
800 SW Jackson Street, Suite 1200
Topeka, KS 66612-2212

Dear Ms. Hinton:

I meant for this letter to accompany KU's letter of January 15, 2009, which responded to the audit of Regents Information Systems.

I wanted you and your staff to know how serious I am personally about the audit. We clearly need to monitor this highly technical subject, and I wanted you to know that we appreciate the careful audit you performed. We will make sure that the suggestions of your staff will be taken literally and carefully reviewed.

If you have any questions that I should address, I will be happy to do so.

Sincerely,

Robert E. Hemenway
Chancellor

REH:glc

Office of the Chancellor
Strong Hall | 1450 Jayhawk Blvd., Room 230 | Lawrence, KS 66045-7535 | (785) 864-3131 | Fax (785) 864-4120 | www.ku.edu