Procedure for Regents Institutions' Annual Security Self-Assessment

Last Modified: September 2, 2005

Background

State of Kansas Information Technology Policy 4310, the "State of Kansas Information Technology Security Self-Assessment" (http://da.state.ks.us/itec/Documents/ITECITPolicy4310.htm), went into effect in July 2004 and requires all state agencies to perform an annual security self-assessment. The purpose of this policy is to "annually determine the status of information systems security through a self-administered assessment." This policy states that the Regents institutions are to report to the Kansas Board of Regents, so this document specifies procedures for performing and reporting the self-assessment to assist Regents institutions with complying with the policy. This is similar to ITEC Security Council's (ITSEC) "Procedures for Security Self-Assessment" used by non-Regents state agencies (http://da.state.ks.us/itec/itsec/Procedures.htm).

The ITSEC used the National Institute of Standards and Technology's (NIST) security self-assessment as a guideline and customized it for Kansas government (http://da.state.ks.us/ITEC/ITSEC/Security_SelfAssessment.doc). However, like the federal NIST self-assessment, the Kansas self-assessment survey is geared toward provision of government services and is not a good fit for institutions of higher education that have a substantially different mission and clientele. Consequently, the Regents Information Technology Council (RITC) developed an IT security framework (hereafter called the "Regents IT Security Framework") that combines the ISO 17799 international standard with the "Effective Practices and Solutions in Security" guide (http://educause.edu/EffectiveSecurityPracticesGuide/1246) produced by the EDUCAUSE and Internet2 joint Computer and Network Security Task Force. This framework contains:

- Comprehensive list of security tasks that institutions should address in their campus security plans ("Security Worksheet" worksheet)
- A method to assess progress and prioritize these tasks ("Progress" columns in the "Security Worksheet" worksheet)
- Ability to add institutional-specific tasks ("Institutional Details" worksheet)
- A method for assessing risk ("Risk Assessment" worksheet)
- A self-assessment tool for higher education developed by the EDUCAUSE/Internet2 Computer and Network Security Task Force ("Annual Assessment Tool" and "Annual Assessment Score" worksheets). **This self-assessment tool is the basis for the annual self-assessment report required by ITEC Policy 4310.**

The Regents IT Security Framework, Annual Security Self-Assessment Report form, and procedures for the annual report are available on the Kansas Board of Regents web site at http://www.kansasregents.org/board/committees/computer.html

Procedures for Regents Institution Annual Security Self-Assessment

- All Kansas Regents institutions must complete the "Annual Assessment Tool" and "Annual Assessment Score" worksheets in the Regents IT Security Framework.
- The specific scores from the self-assessment tool will not be reported to the Board of Regents office. Rather, the results will be generalized in narrative form for the final report using the confidential form titled "Regents Institution Annual Security Self-Assessment Report" (see http://www.kansasregents.org/board/committees/computer.html

  Likewise, for security reasons specific details of security technologies used should not be reported.

- All entities must submit the completed "Regents Institution Annual Security Self-Assessment Report" form (http://www.kansasregents.org/board/committees/computer.html) to the Board of Regents via e-mail to bwilliams@ksbor.org by October 1 of each year.
- The time period for activities covered by the self-assessment report is the last full fiscal year (July 1 to June 30) prior to the October 1 reporting date.
- Entities are encouraged to use the "Security Worksheet" and "Risk Assessment" worksheets in the Regents IT Security Framework to provide information for filling out the annual assessment tool
- All entity reports and completed self-assessment tools will be considered confidential under the Open Records Act
- All entity reports shall be stored securely in the Board of Regents office.
- The Board of Regents Director of Information Technology and RITC will produce an executive summary report for the President/CEO of the Board of Regents based on the entity reports.
- The executive summary report shall have no information identifiable by entity.
- The executive summary report will identify which entities submitted a self-assessment report and which did not.