RITC Security Incident Policy and Procedure, Approved 4/2005

Individual campuses are responsible for assessing the nature and severity of all security incidents on their campuses. The following steps are built into all the local campus security incident reporting procedures.

1) If it is determined to be a major incident, the IT incident is escalated to the top administration on campus, and the Board of Regents office is notified via fax or phone. A "major incident" is defined as a breach of data involving credit cards, social security information, or other personally identifiable information that could cause detriment or financial harm to individuals or the institution.

2) The President and CEO and/or Chief Information Officer (CIO) of the Board of Regents shall be notified with 24 hours of a major security incident. The CIO then notifies the Executive Branch Chief Information Technology Officer (CITO) and the IT Security Officer (ISOS) for the State. The campuses can also notify the CITO and ISOS, but the Board of Regents office must be notified by the campus. Contacts at the Board of Regents office and State are as follows:

KBOR:	Reginald L. Robinson President & CEO 785-296-1237 rrobinson@ksbor.org	Brad Williams Chief Information Officer 785-296-8729 bwilliams@ksbor.org
State of Kansas:	Denise Moore Executive CITO 785-296-3463 Denise.Moore@da.ks.gov	Larry Kettlewell IT Security Officer 785-296-8434 Larry.Kettlewell@da.ks.gov

3) Updates should then be provided to the Board of Regents, Executive CITO, and State IT Security Officer.