

# DRAFT FOR DISCUSSION ONLY

## Information Technology Policy ##### - State of Kansas Information Technology Security Self-Assessment

1.0 TITLE: State of Kansas Information Technology Security Self- Assessment

1.1 EFFECTIVE DATE: XX/XX/2004

1.2 TYPE OF ACTION: New

1.3 KEY WORDS: Enterprise Security Assessment, Security Self-Assessment, IT Security Assessment

2.0 PURPOSE: To annually determine the status of information systems security through a self-administered assessment

3.0 ORGANIZATIONS AFFECTED: All branches, divisions, departments and agencies of Kansas state government, hereafter referred to as entities.

4.0 REFERENCES:

4.1 K.S.A. 1998 Supp. 75-7203 authorizes the ITEC to: Adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state agencies.

4.2 National Institute of Standards and Technology (NIST) Special Publication 800-26 *Security Self-Assessment Guide for Information Technology Systems*

4.3 NIST Special Publication 800-18, *Guide for Developing Security Plans For Information Technology Systems*

4.4 NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology*

4.5 NIST Special Publication 800-30 *Risk Management Guide for IT Systems*

4.6 Federal Information System Controls Audit Manual (FISCAM)

4.7 ITEC Policy 4230 - Default Information Technology Enterprise Security Policy

4.8 ITEC Policy 4300 - Information Technology Security Council Charter

4.9 ITEC Policy 3200 - Business Contingency Planning

4.10 ITEC Policy 3210 - Business Contingency Planning Implementation

# **DRAFT FOR DISCUSSION ONLY**

4.11 State of Kansas Information Technology Security Self-Assessment (Self-Assessment)

## **5.0 DEFINITIONS, CONCEPTS, TERMS:**

5.1 Self-Assessment- NIST developed the original Security Self-Assessment to evaluate federal agencies. The ITEC Security Council modified the document to make it more appropriate for Kansas state government. Our state version consists of a Microsoft Word document that contains questions to be answered in 16 different areas under three overall headings of Management Controls, Operational Controls, and Technical Controls.

5.2 Rating system – There are six possible ratings for each question, ranging from no practice, informal practice, written policies and/or procedures, Implemented Policies and Procedures, Procedures Tested and Reviewed, and finally not applicable.

5.3 Confidentiality – The completed Self-Assessment shall be considered confidential under the Open Records Act.

5.4 Result Reporting – All results from the completed Self-Assessment shall be reported in summary form only with no information identifiable by agency.

## **6.0 POLICY:**

6.1 ALL entities shall complete the Self-Assessment by October 1<sup>st</sup> of each year.

6.2 ALL entities shall submit the completed Self-Assessment in electronic form to the ITEC Security Council.

## **7.0 PROCEDURES:**

7.1 Agencies are to complete the Self-Assessment in electronic form, maintain it, update it, and submit it annually.

## **8.0 RESPONSIBILITIES:**

8.1 Heads of agencies are responsible for establishing procedures to ensure their organization's compliance with the requirements of this policy.

8.2 The ITEC Security Council will annually report compliance to ITEC.

8.3. The Kansas Information Technology Office is responsible for the maintenance of this policy.

## **9.0 CANCELLATION: None**

10.0 CONTACT PERSON: Kansas Information Technology Office, 785-296-xxxx

**DRAFT FOR DISCUSSION ONLY**