Kansas Information Technology Executive Council

Information Technology Policy 7230 Revision 2 - Information Technology Enterprise Security Policy

1.0 TITLE: Information Technology Enterprise Security Policy

1.1 EFFECTIVE DATE: 11/5/2014

1.2 TYPE OF ACTION: Update

2.0 KEYWORDS: Enterprise Security Policy, Information Security, User Security, Physical Security, Default Security Requirements, Network Security, Security Administration, Security Incident Response.

3.0 PURPOSE: To define the minimum requirements for enterprise information technology security policy, standards, and procedures.

4.0 ORGANIZATIONS AFFECTED: All State of Kansas branches, boards, commissions, departments, divisions, agencies, and third parties used to process transmit or provide business capabilities on behalf of Kansas state government, hereafter referred to as Entities.

5.0 REFERENCES:

5.1 K.S.A. 2013 Supp. 75-7203 authorizes the Kansas Information Technology Executive Council (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 entities.

5.2 Kansas Information Technology Executive Council (ITEC), ITEC Policy 7300R1, Information Technology Security Council Charter.

6.0 DEFINITIONS:

6.1 Security policy is defined as a collection of mandates, actions and required documentation governing the security protections and controls of an entity.

6.2 The Information Technology Security Standards 7230A (7230A) is supplemental to this policy and is defined as a document published by the Kansas Information Technology Executive Council that contains minimum security controls all entities will apply to personnel, processes and assets.

7.0 POLICY:

7.1 Entities shall implement an Information Technology Security Policy for their organization. All Information Technology Security Policies adopted by the Entity must be at least as stringent as this policy. Entities that do not

implement their own Information Technology Security Policy shall implement this policy in accordance with the standards and procedures referenced in the Information Technology Security Standard 7230A.

7.2 Planning and Risk Assessments:

7.2.1 Entities shall ensure risk assessments are performed for information systems in accordance with 7230A Assessments and Security Planning standard and the Risk Management standard.

7.2.2 Entities shall ensure the development and implementation of a security plan for information systems in accordance with the 7230A Assessment and Security Planning standard.

7.2.3 Entities shall preform a vulnerability assessment and security assessments on information systems in accordance with 7230A System Operations standard.

7.3 Awareness and Training:

7.3.1 Entities shall implement Security Awareness and Security Operations Training in accordance with 7230A Awareness and Training Standard.

7.4 Access Control:

7.4.1 Entities shall ensure that only authorized users are granted access to systems and data in accordance with 7230A Access Control standard and Physical Security Standard.

7.4.2 Entities shall ensure authentication accounts are actively managed in accordance with 7230A Access Control Standard and Personnel Security standard.

7.5 Configuration Management:

7.5.1 Entities shall document standardized configurations settings for information systems in accordance with 7230A System Configuration standard.

7.5.2 Entities shall maintain an asset inventory of information systems in accordance with 7230A System Configuration standard.

7.5.3 Entities shall implement a change control process in accordance with 7230A Change Control standard.

7.6 Media Protection:

7.6.1 Entities shall perform data/media sanitization in accordance with 7230A Data Protection standard and Physical Security standard.

7.7 System and Communication Protection:

7.7.1 Entities shall protect information systems with dedicated protection mechanisms in accordance with 7230A System Configuration standard.

7.7.2 Entities shall classify and protect both data and information systems in accordance with 7230A Data Protection, System Configuration, Assessment and Security Planning standards.

7.8 System and Information Integrity:

7.8.1 Entities shall document application development standards in accordance with 7230A Application Processing standard.

7.8.2 Entities shall monitor system configuration integrity in accordance with 7230A System Operation standard.

7.8.3 Entities shall ensure that information systems are configured to log events in accordance with 7230A System Audit standard.

7.8.4 Entities shall ensure that information systems are time synchronized in accordance with 7230A System Audit standard.

7.9 Third Parties:

7.9.1 Entities shall not reduce its security profile for the purpose of conducting third-party audits.

7.9.2 Entities shall ensure that physical and logical security control testing by third parties is conducted within pre-defined and documented parameters.

7.10 Incident Response:

7.10.1 Entities shall document security incident response procedures in accordance with 7230A Incident Response standard.

7.10.2 Entities shall report incidents as in accordance with 7230A Incident Response standard.

7.11 Physical and Environmental Protection:

7.11.1 Entities shall implement physical access controls in accordance with 7230A Physical Security standard.

7.11.2 Entities shall implement physical environmental controls in accordance with 7230A Physical Security standard.

7.12 Personnel Security:

7.12.1 Entities shall document acceptable use of information system in accordance with 7230A Personnel Security standard.

7.13 System and Service Acquisition:

7.13.1 Entities shall ensure proper due diligence in assessing security capabilities and requirements of any third party purchased or provided system in accordance with 7230A Secure Purchasing/Acquisition standard.

8.0 RESPONSIBILITIES:

8.1 Heads of entities are responsible for compliance with the requirements of this policy.

8.2 The State of Kansas Information Technology Security Council (ITSC) is responsible for the maintenance 7230A Information Technology Security Standards.

8.3 The Chief Information Technology Officer, Executive Branch is responsible for the maintenance of this policy.

9.0 CANCELLATION:

9.1 Rescinds: 7900 7900A 7400 7400A 7320 7320A