Kansas Information Technology Executive Council

1.0 TITLE: INFORMATION TECHNOLOGY SECURITY STANDARDS 7230A

1.1 EFFECTIVE DATE: 11/5/2014

1.2 TYPE OF ACTION: Update

1.3 KEYWORDS: Kansas Information Technology Security Council, Enterprise Security Policy, Information Security, User Security, Personally Identifiable Information, Security Incident Response.

2.0 PURPOSE: To define the Information Technology Policy 7230 minimum security standards and procedures for state of Kansas information systems.

3.0 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 Entity or Entities.

4.0 REFERENCES:

4.1 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.

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

4.3 Kansas Information Technology Executive Council (ITEC), ITEC Policy 7230, Revision 1, General Information Technology Enterprise Security Policy.

4.4 NIST Special Publication 800-53 Rev 2 – Recommended Security Controls for Federal Information Systems.

4.5 NIST Special Publication 800-88 – Guidelines for Media Sanitization.

5.0 DEFINITIONS: The following definitions are applied throughout this policy and procedure memorandum.

5.1 Personal Financial Information (PFI): Any non-public personally identifiable financial information that an entity collects about an individual in order to provide a financial product or service.

5.2 Personally Identifiable Information (PII): Any information that can be used on its own or with other information to identify or locate a single person.

5.3 Sensitive Personally Identifiable Information (SPII): Any non-public PII that 1) the data subject has not voluntarily disclosed, 2) is not subject to public release by an entity in accordance with statute or court order, or 3) an entity collected after notice to the data subject that the information is categorized for public release.

5.4 Individually Identifiable Health Information (IIHI): Any information as defined in 45 CFR 160.103 – Code of Federal Regulations TITLE 45 – Public Welfare Part 160.103 Definitions.

5.5 Restricted-Use Information: Includes but is not limited to SPII, IIHI or PFI as defined in this Standard.

5.6 Data Subject: The individual person whose PII is contained in the record or Information Asset.

5.7 Voluntary Disclosure: Information that a data subject provides without request or compulsion by state personnel, or that a data subject provides to the State with notice that it will be made publicly available.

5.8 Information System Component: A discrete, identifiable information technology asset (i.e., hardware, software, firmware, or media (electronic and hardcopy)) that represents a building block of an information system. Information system components include commercial information technology products.

5.9 Information System: A discrete set of information system components organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

5.10 Critical System: Any information system that supports the core entity mission.

5.11 Production Information System: Information Systems used to deliver essential services in the normal operating state of the entity.

5.12 Source Record: The authoritative instance of a record within an entity

5.13 Variance: A deviation from the control mandated in this document.

5.14 Information Asset: A body of information defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

5.15 Security Assessment: An assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

5.16 Vulnerability Scanning: Scans using specialized tools for the detection of vulnerabilities within the Information System.

6.0 RISK MANAGEMENT STANDARD

6.1 Entities shall develop a hierarchal Information Asset classification standard that assigns appropriate controls to each Information Asset classification. The standard shall require the security controls specified in this document to be applied to Restricted-Use Information.

6.2 Entities shall also set a default information classification for all information. If no default standard is created, all information shall be considered Restricted-Use Information.

6.3 Entities shall ensure that Information Asset trustees are appointed for the following Information Assets:

- Intellectual property or
- Data compilations that contain or may be projected to contain Source Records on thirty (30) or more individuals of Restricted-Use Information.

6.4 Information Asset trustees shall perform the following tasks for each information Asset:

- Determine the potential impact to the affected entity, individuals and the State in the event of a loss of confidentiality, integrity, and availability of the Information Asset.
- Classify the asset in accordance with the Entity's Information Asset classification standard.
- Ensure that the asset is handled in accordance with the Entity's Information Asset handling standard.
- Ensure that adverse events are reported to the Entity Information Security Officer (ISO).
- Appoint Information Asset custodians.
- Approve all access and use of the Information Asset.
- Recertify annually the classification, access, users and custodians of the Information Asset.
- Report classification of all Restricted-Use Information Assets to the Risk Management Committee.

6.5 Information Asset custodians shall perform the following responsibilities:

- Implement and operate the safeguards and controls for Information Assets as directed by Information Asset trustees.

6.6 Entities shall maintain a standing Risk Management Committee with the following responsibilities:

- Ensure that Restricted-Use Information Assets are identified.
- Review the classifications of Restricted-Use Information Assets by trustees.
- Ensure that risks are assessed.

- Process and approve variances from requirements in this document based upon risk and mitigating controls.
- Report approved variances in writing to the Enterprise Security Office (ESO), located within the Office of Information Technology Services (OITS), and the Entity Head.
- Direct the investigation, mitigation and acceptance of risks on behalf of the entity.

6.7 The Entity head shall appoint a Risk Management Committee that shall include participants from the following functions or roles if they exist within the entity:

- Legal
- Audit/Risk
- Line of Business Representative(s)
- Information Security Officer

7.0 ASSESSMENT AND SECURITY PLANNING STANDARD

RISK ASSESSMENT

7.1 Entities shall assess and document the risks to information systems that process, store or transmit Restricted-Use Information.

7.2 Entity risk assessments shall identify potential threats and characterize the likelihood and impact of the threat being realized.

7.3 Entities shall assess and document risks prior to placing an information system into service, whenever a significant change is made, and at least once every three (3) years thereafter.

SECURITY PLANNING

7.4 Entities shall document a security plan that specifies security controls based upon a risk assessment for information systems that process, store or transmit Restricted-Use Information.

7.5 The set of security controls in the security plan shall be sufficient to adequately mitigate risks to organizational operations and assets, individuals, other organizations and the state, based on the entity risk tolerance.

8.0 AWARENESS AND TRAINING STANDARD

SECURITY AWARENESS TRAINING

8.1 Entities shall provide and conduct security awareness training for all information system account holders.

8.2 Entities shall require all employees to complete security awareness training within ninety (90) days of hire and on an annual basis thereafter.

8.3 Entities shall retain a form of acknowledgement of training completion.

8.4 Entities shall review their security awareness training materials at least annually or more frequently as needed.

8.5 Awareness training shall address the following topics at a minimum:

- Passwords including creation, changing, aging and confidentiality
- Privacy and proper handling of sensitive information
- Physical security
- Social engineering
- Identity theft avoidance and action
- Email usage
- Internet usage
- Viruses and malware
- Software usage, copyrights and file sharing
- Portable devices
- Proper use of encryption devices
- Reporting of suspicious activity and abuse

9.0 ACCESS CONTROL

IDENTIFICATION AND AUTHENTICATION

9.1 User access to information systems that process, store or transmit Restricted-Use Information shall be authorized by an appropriate Entity official.

9.2 All users of information systems that process, store or transmit Restricted-Use Information shall be authenticated by a unique system identifier.

9.3 The unique system identifier will be associated with a unique information system authenticator (i.e. password, token, etc.).

9.4 Unique information system authenticators shall be delivered in a secure and confidential manner.

9.5 Passwords for system user accounts shall be constructed according to one (1) of the following two (2) methods.

9.5.1 Passwords with complexity shall comply with the following requirements:

- A minimum of eight (8) characters in length
- Contain three (3) of four (4) of the following categories:
  - Uppercase
  - Lowercase
  - Numeral
  - Non-alpha numeric character

- Shall not contain the user id

9.5.2 Passwords without complexity shall be a minimum of sixteen (16) characters in length.

9.6 Passwords shall not be changed more frequently than once every fifteen (15) days without system administrator intervention.

9.7 Passwords for system user accounts shall not have a lifespan that exceeds ninety (90) days.

9.8 Passwords shall be significantly different from the past ten (10) passwords.

9.9 Passwords shall not be viewable in clear text except by the account holder.

9.10 Passwords shall not be transmitted or electronically stored in clear text.

9.11 Passwords shall not be shared and shall be kept confidential.

9.12 Where physical tokens or authenticators are used:

- A defined process must be followed for token distribution.
- A defined process must be followed for token revocation.
- A defined process must be followed for the handling of lost, stolen or damaged tokens.

9.13 Where biometric data is used for authentication:

- A defined process must be followed for capturing user biometric data.
- A defined process must be followed for biometric revocation.
- A defined process must be followed for the handling of user biometric data.

ACCOUNT MANAGEMENT

9.14 All information system accounts shall provide the most restrictive set of privileges required. Separation of duties shall be enforced through account privileges; no single user shall have privileges to authorize, perform, review and audit a single transaction.

9.15 Information system accounts shall be restricted to a maximum of five (5) consecutive failed attempts before being locked out.

9.16 Accounts shall remain locked out for a minimum of thirty (30) minutes without administrator intervention.

SESSION MANAGEMENT

9.17 Information systems shall display a system use notification identifying system ownership, system usage restrictions, prohibition of unauthorized access, implied consent and associated penalties for unauthorized access. The user must acknowledge the system use notification before gaining access to the information system.

9.18 Entity authorization shall be required prior to deploying any remote access solution to information systems containing or processing Restricted-Use Information. Entities shall specify the acceptable methods of connection.

9.19 Remote sessions shall be encrypted, auditable and traverse managed access points.

9.20 Local console sessions on information systems that process, store or transmit Restricted-Use Information shall be locked after a period of thirty (30) minutes of inactivity.

9.21 Remote sessions to information systems that process, store or transmit Restricted-Use Information shall be terminated after a period of thirty (30) minutes of inactivity.

9.22 Authentication shall be required to unlock a console session or reestablish a remote session.

10.0 SYSTEMS CONFIGURATION STANDARD

CONFIGURATION MANAGEMENT

10.1 Entities shall build information systems that process, store or transmit Restricted-Use Information from a standard configuration baseline.

10.2 The standard configuration baseline shall include the specifications of the information system components and the security controls for each component.

10.3 Entities shall maintain an asset inventory of information systems components and update it as it changes and review it at least annually.

10.4 The asset inventory shall also identify and document the relationships between each of the information system components and the ownership of each component.

10.5 Collaborative infrastructure, such as video and teleconferencing, shall be configured to prohibit remote activation.

CHANGE CONTROL

10.6 Entities shall document and adhere to change control processes when making changes to production systems.

10.7 Change control requests shall include proposed change description, justification, risk assessment, implementation plan, test plan, back-out plan, review and approval.

10.8 Entities shall maintain a change log for information systems containing Restricted-Use Information.

10.9 The change log shall include:

- Date and time of maintenance
- Name and organization of person performing change
- Name of escort, if required
- Description of maintenance performed
- List of affected information systems components or component elements

SYSTEMS PROTECTION

10.10 Entities shall implement boundary protection mechanisms with capability to monitor and control network communications.

10.11 Within the boundary, entities shall create security zones based on data and information system classification.

10.12 Entities shall employ malicious code protection mechanisms on systems that contain Restricted-Use Information.

10.13 Entities shall configure malicious code protection mechanisms to perform weekly scans of files on information systems.

10.14 Where malicious code protection mechanisms require regular signature or detection engine updates, entities shall employ a documented update mechanism that includes testing and installation of applicable updates.

11.0 DATA PROTECTION STANDARD

11.1 Entities shall employ mechanism(s) to ensure the confidentiality, availability and integrity of Restricted-Use Information.

11.2 Restricted-Use Information that has met the information retention schedule must be removed, destroyed or deleted in a verifiable manner.

11.3 Restricted-Use Information shall be protected from unauthorized disclosure.

11.4 Restricted-Use Information when transmitted electronically outside of a secure boundary shall be encrypted.

11.5 Media containing Restricted-Use Information shall be disposed of in accordance with NIST Special Publication 800-88 – Guidelines for Media Sanitization.

12.0 APPLICATION PROCESSING STANDARD

12.1 Entities shall define and document principles and procedures for secure application development.

12.2 The application element of all information systems components shall logically separate user functionality from administrative functionality such that the interface for the one cannot be used to operate the other.

13.0 SYSTEMS OPERATIONS STANDARD

ASSESSMENT OPERATIONS

13.1 Entities shall perform Security Assessments against all information systems that process, store or transmit Restricted-Use Information prior to installation on production environments and annually thereafter to ensure that security controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements of the system.

13.2 Entities shall perform Vulnerability Scans against all information systems that process, store or transmit Restricted-Use Information prior to installation into production environments and biannually thereafter.

13.3 Entities shall document and implement a remediation plan for the security issues discovered in Security Assessments and Vulnerability Scanning, assign rankings and establish corrective actions that are reviewed quarterly.

13.4 Entities shall monitor for security alerts and advisories relative to the technologies that are operating within their environments.

13.5 Entities shall implement a documented patch management process that includes 13.4, testing and installation of applicable patches.

INTEGRITY OPERATIONS

13.6 Entities shall implement controls to ensure that configuration settings are within acceptable parameters.

13.7 Entities shall implement integrity monitoring on information systems that process, store or transmit Restricted-Use Information.

13.8 Entities shall document and investigate integrity discrepancies.

13.9 Entities shall validate, then circulate security alerts to appropriate personnel and ensure corrective action is taken.

MAINTENANCE OPERATIONS

13.10 Entities shall not operate information systems containing Restricted-Use Information without either redundant qualified in-house staff or by contract for vendor managed support.

13.11 Entities shall configure critical information systems to be fault tolerant.

13.12 Entities shall ensure that critical data is restorable to a known secure state of operations.

13.13 Entities shall test critical information system's restoration annually.

14.0 SYSTEM AUDIT

14.1 Information systems that process, store or transmit Restricted-Use Information shall be configured such that all user access interactions and system administrators' actions are logged to both internal and external log repositories.

14.2 The following data points shall be logged:

- Event date
- Event time
- Event source
- Event description

14.3 Information systems that process, store or transmit Restricted-Use Information shall be configured to raise alerts to administrative personnel in the event that logging space becomes limited, upon system logging failure or when inappropriate, unusual or suspicious activity is detected.

14.4 Information systems that store logging data shall be configured to continue logging by overwriting the oldest logs in the event available space is limited.

14.5 Information system logging data shall be manually reviewed according to a pre-defined period of time or the logging system configured to automatically raise alerts to administrative personnel based on defined events.

14.6 All Production Information Systems shall be configured to have time synchronized with authoritative time sources.

15.0 INCIDENT RESPONSE STANDARD

15.1 Entities shall adopt a defined incident response plan which addresses the following stages:

15.1.1 Preparation

15.1.1.1 Entities shall appoint team members to incident response roles with the following skills:

- Communication and coordination
- Network analysis
- System administration
- Security analysis

15.1.1.2 Entities shall provide Incident Response (IR) training for all

IR team members within ninety (90) days of initial assignment of the individual to the IR team.

15.1.1.3 Entities shall provide annual IR training for all IR team members.

15.1.1.4 Entities shall annually conduct IR operations testing using classroom, tabletop exercises or live incidents.

15.1.1.5 Entities shall conduct an exercise recreating a significant incident scenario that requires the full-scale execution of IR operations once every five (5) years.

15.1.2 Detection

15.1.2.1 Entities shall define what constitutes a security incident. The following shall be considered Reportable Security Incidents.

- Attempted or successful malicious destruction, corruption or disclosure of Restricted-Use Information or intellectual property.
- Compromised host or network device that processes, stores or transmits Restricted-Use Information.
- Compromised user account with access to Restricted-Use Information.
- Suspected criminal activity, such as theft, fraud, human safety or child pornography.
- Intentionally defeating a security control.

15.1.3 Analysis

15.1.3.1 Entities shall have dedicated tools and a process to conduct incident analysis, such as:

- Dedicated portable workstations
- Forensics analysis software and procedures
- Evidence collection tools and procedures

15.1.4 Containment

15.1.4.1 Entities shall have procedures to isolate and mitigate identified threats to prevent further impact.

15.1.5 Communication

15.1.5.1 Entities shall develop an incident communications plan to ensure adequate communication of an incident, is provided, in a timely basis to stakeholders.

15.1.5.2 State of Kansas Enterprise Information Security Office shall be notified of Reportable Security Incidents.

15.1.6 Recovery

15.1.6.1 Entities shall recover affected systems and system components to a pre-compromised status and return to normal operations.

15.1.6.2 Entities shall maintain heightened monitoring of the affected system(s) for a period of time subsequent to an incident to ensure there are no lingering impacts.

15.1.7 Post-Incident Activity

15.1.7.1 Entities shall perform a post-incident review in order to document lessons learned and to improve information system protection in the future.

16.0 PHYSICAL SECURITY STANDARD

DATA CENTERS

16.1 Entities shall restrict physical access to data centers that process, store or transmit Restricted-Use Information to authorized personnel only.

16.2 Entities shall maintain a list of all authorized personnel with physical access to data centers that process, store or transmit Restricted-Use Information.

- This list shall be reviewed and updated annually.
- This list shall be updated as user access privileges change.

16.3 Entities shall require authorized personnel to authenticate themselves prior to entry to data centers that process, store or transmit Restricted-Use Information.

16.3.1 Visitors to data centers that process, store or transmit Restricted-Use Information shall be escorted by authorized personnel at all times.

16.3.2 Entities shall log all visitor access to data centers that process, store or transmit Restricted-Use Information.

16.4 Data centers shall implement physical environmental controls that mitigate or prevent damage from water, fire, temperature and humidity for information systems that process, store or transmit Restricted-Use Information.

16.5 Entities shall ensure sufficient power protection is available for critical information systems to perform an orderly shutdown.

MEDIA

16.6 Entities shall restrict physical access to media that store Restricted-Use Information to authorized personnel only.

16.7 Media that store Restricted-Use Information shall be stored securely within a controlled area and physical access to that controlled area shall be restricted to authorized personnel.

16.8 Entities shall ensure appropriate safeguards when media is transported by authorized personnel outside of a controlled area.

17.0 PERSONNEL SECURITY STANDARD

ACCEPTABLE USE

17.1 Acceptable use policies shall restrict the use of all equipment and access to public and private networks to approved entity related operations.

17.2 Entities shall require employees and contractors to acknowledge adherence to the entity acceptable use policy prior to being granted access to information systems.

17.3 Entities shall include policy violation consequences in their acceptable use policies.

17.4 Entity acceptable use policies shall assert that violations will be investigated as a security event.

PERSONNEL OPERATIONS

17.5 Entities shall retain a form of acknowledgement of the acceptable use policy.

17.6 Entities shall assign all employees and contractors a user categorization.

17.7 Entities shall assign information system authorizations to users based on user categorization and information system classification.

17.8 Entities shall revoke system access or eliminate unnecessary permissions for accounts assigned to employees and contractors as they are transferred or terminated.

17.9 Entities shall assign review-only access for all accounts assigned to the terminated employee to that employee’s immediate manager for a pre-defined period of time.

17.10 Entities shall recover all property that has been assigned to terminated personnel.

18.0 SECURE PURCHASING/ACQUISITION STANDARD

18.1 Entities shall include system security requirements to ensure that the system or solution proposed by proponents meet the security requirements of the entity with all Requests for Proposal, Information, Quotation (RFP, RFI, RFQ) or contracts.

18.2 All acquisition documents must specify the entity's security requirements and allow for the validation of those security requirements.

19.0 RESPONSIBILITIES:

19.1 The State of Kansas Information Technology Security Council (ITSC) is responsible for the maintenance of these standards.

19.2 These standards will be reviewed by the ITSC, at a minimum, every three (3) years.

19.3 Entities shall ensure demonstrable compliance with these standards no later than July 1, 2016.