Kansas Information Technology Executive Council

1.0 TITLE: INFORMATION TECHNOLOGY SECURITY STANDARDS 7230A

1.1 EFFECTIVE DATE: 07/1/2019

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 7300, Revision 1, Information Technology Security Council Charter.

4.3 Kansas Information Technology Executive Council (ITEC), ITEC Policy 7230, Revision 2, General Information Technology Enterprise Security Policy.

4.4 NIST Special Publication 800-53 Rev 4 (latest version takes precedence)– Security and Privacy Controls for (Federal) Information Systems and Organizations.

4.5 NIST Special Publication 800-88 Rev 1 (latest version takes precedence) – Guidelines for Media Sanitization.

4.6 Federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 – Data security requirements for covered entities and their business associates.

5.0 DEFINITIONS: The following definitions are applied throughout this document.

5.1 Critical System: Any Information System for which the loss, misuse, disclosure, unauthorized access to, or modification of information would result in a significant negative impact of an entity's core mission.

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

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

5.4 Information System Component: A discrete, identifiable information technology asset such as 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.

5.5 Multi-Factor Authentication (MFA): A method of confirming a User's claimed identity in which access is granted only after successfully presenting two or more different pieces of evidence (factors) to an authentication mechanism. Factors include knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

5.6 Password: A memorized secret consisting of a sequence of words, special characters, or other text used to authenticate a User's identity.

5.7 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.

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

5.9 Portable Electronic Devices and Portable Electronic Media: Any electronic device or electronic media designed for easy transport. Examples of these items include but are not limited to: smart phones, tablets, laptops, USB flash media, SD cards, diskettes, CDs, DVDs, external hard drives, etc.

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

5.11 Protected Health Information (PHI): Any information, in any form or medium, held or transmitted, about health status, provision of health care, or payment for health care that is created or collected by a covered entity or the business associates of a covered identity and can be linked to a specific individual. (Also see 45 CFR 160.103 – Code of Federal Regulations TITLE 45 – Public Welfare Part 160.103 Definitions).

5.12 Remote Access: Any access to an agency Information System by a User communicating through an external network (i.e. internet).

5.13 Restricted-Use Information (RUI): Includes PFI, PII, and PHI as defined in this Standard, as well as other regulated data (e.g. tax or criminal justice information) or information agencies designate as Restricted-Use Information due to their confidential or sensitive nature (e.g. physical or logical security information for state agencies and their systems).

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

5.15 System Service Account: A special user account that an application or service uses to interact with an Information System.

5.16 User: Includes employees, contractors, or other agents acting on behalf of the state or carrying out state agency functions.

5.17 Variance or Exception: A deviation from a control mandated in this document.

6.0 RISK MANAGEMENT STANDARD

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

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

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

6.3.1 Intellectual property or
6.3.2 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 must perform the following tasks for each Information Asset:

6.4.1 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.

6.4.2 Classify the asset in accordance with the entity's Information Asset classification standard.

6.4.3 Ensure that the asset is handled in accordance with the entity's Information Asset handling standard.

6.4.4 Ensure that adverse events are reported to the entity's Information Security Officer (ISO).

6.4.5 Appoint Information Asset custodians.

6.4.6 Approve all access and use of the Information Asset.

6.4.7 Recertify annually the classification, access, users, and custodians of the Information Asset.

6.5 Information Asset custodians must perform the following responsibilities:

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

6.6 Entities must implement a documented risk management process that addresses risk identification, tracking, mitigation, reporting, and acceptance.

6.7 Entities must document and track all outstanding risks (i.e. risk register).

6.8 Entities must periodically review existing risks.

6.9 Entities must process and approve any Variances or Exceptions to the requirements in this policy.

6.10 Entities must document, track, and report any approved Variances or Exceptions.

7.0 ASSESSMENT AND SECURITY PLANNING STANDARD

RISK ASSESSMENT

7.1 Entities must assess and document the risks to Information Systems that process, store or transmit Restricted-Use Information.

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

7.3 Entities must 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 must 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 must 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 must provide and conduct security awareness training for all Users.

8.2 Entities must require all Users to complete security awareness training within ninety (90) days of hire or initial access, and on an annual basis thereafter.

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

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

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

8.5.1 Passwords including creation, changing, aging, and confidentiality
8.5.2 Privacy and proper handling of sensitive information
8.5.3 Physical security
8.5.4 Social engineering
8.5.5 Identity theft avoidance and action
8.5.6 Email usage
8.5.7 Internet usage
8.5.8 Viruses and malware
8.5.9 Software usage, copyrights, and file sharing
8.5.10 Portable Electronic Devices and Portable Electronic Media
8.5.11 Proper use of encryption devices
8.5.12 Reporting of suspicious activity and abuse

9.0 ACCESS CONTROL

IDENTIFICATION AND AUTHENTICATION

9.1 User access to Critical Systems or Information Systems that process, store or transmit Restricted-Use Information must be authorized by an appropriate Entity official through established protocols within the entity.

9.2 Users of Critical Systems or Information Systems that process, store or transmit Restricted-Use Information must be authenticated by a unique system identifier.

9.3 Users with administrative rights or elevated privileges must use a separate account to perform tasks that require elevated privileges or administrative rights.

9.3.1 Administrative rights and elevated privilege accounts must only be used for activities that require elevated privileges (i.e. not for email access or internet browsing).

9.3.2 Multi-Factor Authentication must be used for administrative rights or elevated privilege accounts.

9.3.3 User accounts with administrative rights or elevated privileges must not have an email account or mailbox provisioned or associated with it.

9.4 System Service Accounts must be approved and documented for proper business use prior to creation and must be reviewed and approved annually for continued use.

9.5 System Service Accounts must be configured with least privilege and only used for a single task or service.

9.6 Unique system identifiers will be associated with a unique Information System authenticator (i.e. password, token, etc.).

9.7 Unique Information System authenticators must be delivered in a secure and confidential manner.

9.8 Passwords must not be viewable in clear text except by the account holder.

9.9 Passwords must not be transmitted or electronically stored in clear text.

9.10 Passwords must not be shared and must be kept confidential.

9.11 Passwords for system User accounts must be constructed with the following requirements:

9.11.1 A minimum of twelve (12) characters in length.

9.11.2 Contain three (3) of four (4) of the following categories:

- Uppercase
- Lowercase
- Numeral
- Non-alpha numeric character

9.11.3 Must not contain the user ID.

9.11.4 Must not be changed more frequently than once every one (1) day without system administrator intervention.

9.11.5 Must not have a lifespan that exceeds one hundred eighty (180) days.

9.11.6 Must be different from the previous twenty-four (24) Passwords.

9.12 Passwords for System Service Accounts must be constructed with the following requirements:

9.12.1 A minimum of twelve (12) characters in length.

9.12.2 Contain three (3) of four (4) of the following categories:

- Uppercase
- Lowercase
- Numeral
- Non-alpha numeric character

9.12.3 Must not contain the user ID.

9.12.4 Must not have a lifespan that exceeds three hundred sixty-five (365) days.

9.13 Where tokens, whether soft tokens or physical tokens, as authenticators are used:

9.13.1 A documented process must be followed for token distribution.
9.13.2 A documented process must be followed for token revocation.
9.13.3 A documented process must be followed for the handling of lost, stolen or damaged tokens.

9.14 Where biometric data is used for authentication:

9.14.1 A documented process must be followed for capturing user biometric data.
9.14.2 A documented process must be followed for biometric revocation.
9.14.3 A documented process must be followed for the handling of user biometric data.

ACCOUNT MANAGEMENT

9.15 All Information System accounts must be configured according to the principle of least privilege.

9.16 Separation of duties must be enforced through account privileges.

9.16.1 No single user account can have privileges to authorize, perform, review, and audit a single transaction.
9.16.2 When available, role-based access controls (RBAC) must be implemented and enforced for systems that contain Restricted-Use Information or systems designated as a Critical System.

9.17 Information System accounts must be restricted to a maximum of five (5) consecutive failed attempts before being locked.

9.18 Accounts must remain locked for a minimum of thirty (30) minutes without administrator intervention.

SESSION MANAGEMENT

9.19 Information Systems must 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.

9.20 Entities must establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of Remote Access allowed.

9.21 Entities must authorize Remote Access to an Information System prior to allowing such connections.

9.22 When available, entities must deploy MFA for Remote Access to Critical Systems or systems containing Restricted-Use Information.

9.23 Remote Access sessions must be encrypted, auditable, and traverse managed access points.

9.24 Remote Access sessions to Information Systems that process, store or transmit Restricted-Use Information must be terminated after a period of thirty (30) minutes of inactivity.

9.25 Local console sessions on Information Systems that process, store or transmit Restricted-Use Information must be locked after a period of thirty (30) minutes of inactivity.

9.26 Authentication must be required to unlock a console session or reestablish a remote session.

10.0 SYSTEMS CONFIGURATION STANDARD

CONFIGURATION MANAGEMENT

10.1 Entities must build Information Systems that process, store or transmit Restricted-Use Information from a standard configuration baseline.

10.2 The standard configuration baseline must include the specifications of the Information System Components and the security controls for each component.

10.3 Entities must maintain an asset inventory of Information Systems' components, update the inventory as changes occur, and review the inventory at least annually.

10.4 The asset inventory must 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, must be configured to prohibit remote activation.

CHANGE CONTROL

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

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

10.8 Entities must maintain a change log for Information Systems containing Restricted-Use Information.

10.9 The change log must include:

10.9.1 Date and time of the maintenance
10.9.2 Name and organization of the person performing change
10.9.3 Name of escort, if required
10.9.4 Description of the maintenance performed
10.9.5 List of affected Information System(s) Components or component elements

SYSTEMS PROTECTION

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

10.11 Within the boundary, entities must create security zones based on data and Information System classification.

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

10.13 Entities must 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 must employ a documented update mechanism that includes testing and installation of applicable updates.

11.0 DATA PROTECTION STANDARD

11.1 Entities must 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 must be protected from unauthorized disclosure.

11.4 Entities must use encryption modules, ciphers, or algorithms found within the NIST FIPS 140-2 validated list when encrypting Restricted-Use Information.

11.5 Restricted-Use Information when transmitted electronically outside of a secure boundary must be encrypted.

11.6 Restricted-Use Information must be encrypted when stored on Portable Electronic Media or Portable Electronic Devices.

MEDIA

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

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

11.9 Media containing Restricted-Use Information must be transported by authorized personnel when leaving a controlled area and must be transported in a manner that ensures appropriate safeguards are applied.

12.0 APPLICATION PROCESSING STANDARD

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

12.2 The application element of all Information Systems Components must 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 must perform security assessments against all Critical Systems and all Information Systems that process, store or transmit Restricted-Use Information prior to installation in production environments and at least annually thereafter. Security assessments are required 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.

13.1.1 Entities must have a documented remediation plan for security issues discovered in security assessments.
13.1.2 Entities must prioritize and establish timelines for implementing corrective actions for all security issues within the remediation plan.
13.1.3 Entities must review all remediation plans and update them at least quarterly.

13.2 Entities must perform vulnerability scans against all Information Systems prior to installation into production environments.

13.3 Entities must perform vulnerability scans against all network connected Information Systems at least monthly.

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

13.5 Entities must have a documented patch management process.

13.5.1 Patch requirements discovered or resulting from vulnerability scans or continuous monitoring must be addressed expeditiously.
13.5.2 Entities must use a risk-based approach to patch vulnerabilities or deploy mitigating controls when unable to patch vulnerabilities.

INTEGRITY OPERATIONS

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

13.7 Entities must implement integrity monitoring on Information Systems that process, store or transmit Restricted-Use Information.

13.8 Entities must document and investigate integrity discrepancies.

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

MAINTENANCE OPERATIONS

13.10 Entities must 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 must configure critical Information Systems to be fault tolerant.

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

13.13 Entities must test critical Information System's restoration annually.

13.14 Entities must update Information Systems when the support for the components of the Information System are no longer available from the developer, vendor, or the manufacturer.

14.0 SYSTEM AUDIT

14.1 Critical Systems and Information Systems that process, store or transmit Restricted-Use Information must be configured such that all user access interactions and system administrators' actions are logged to both the internal system and to an external log repository (not on the local system).

14.2 The following data points must be logged:

14.2.1 Event date
14.2.2 Event time
14.2.3 Event source
14.2.4 Event description
14.2.5 Identity of any individual(s) or subject(s) associated with the event(s).

14.3 Logs for Critical Systems and Information Systems that process, store or transmit Restricted-Use Information must be stored and maintained for at least 120 days (180 days recommended) on an external log repository or in accordance with other regulatory requirements.

14.4 Critical Systems and Information Systems that process, store or transmit Restricted-Use Information must be configured to raise alerts to the system administrative personnel if logging space becomes limited, upon system logging failure, or when suspicious activity is detected within the system logging component.

14.4.1 Entities must actively review and address alerts raised from the logging component.

14.5 Information Systems that store logging data must be configured to continue logging by overwriting the oldest logs in the event available space is limited.

14.6 Information System logging data must be manually reviewed according to a pre-defined period of time or the logging system configured to automatically raise alerts to the system administrative personnel.

14.7 All Production Information Systems must be configured to have time synchronized with authoritative time sources.

15.0 INCIDENT RESPONSE STANDARD

15.1 Entities must adopt a documented incident response plan which addresses the following stages: preparing for a security incident, detecting and analyzing a security incident; containing a security incident; eradicating and recovering from a security incident; and post incident activities.

15.2 Entities must define and document what constitutes a security incident. Security incidents must include intentional and unintentional incidents.

15.3 Entities must define and document a process to track and categorize the severity of all incidents which must drive the associated response, reporting, and communication activities.

15.4 Entities must appoint team members or outside staff/contractors to incident response roles with the following skills:

15.4.1 Communication and coordination
15.4.2 Network analysis
15.4.3 System administration
15.4.4 Security analysis
15.4.5 Legal counsel
15.4.6 Privacy

15.5 Entities must ensure that Incident Response (IR) training for all IR team members has been completed within ninety (90) days of initial assignment of the individual to the IR team. In the event the entity contracts for IR services, the entity must receive assurance that the contractor has the necessary skills and training to carry out incident response services.

15.6 Entities must ensure annual IR training for all IR team members as identified above.

15.7 Entities must annually conduct IR operations testing using classroom, tabletop exercises, or live incidents.

15.8 Entities must conduct an exercise recreating a significant incident scenario that requires an operations-based functional exercise (or a major live incident) to validate the IR plan, procedures, and agreements, to clarify roles and responsibilities, and to identify resource gaps once every five (5) years.

15.9 Entities must have dedicated tools and documented processes to conduct incident response activities. If the entity does not have the tools, resources, or expertise, then the entity must identify a service provider to assist with incident response activities.

15.10 Entities must have a documented incident communications strategy to provide adequate and timely communication to all appropriate stakeholders.

15.11 For significant security incidents, entities must perform a post-incident review within a reasonable timeframe upon containment, to document lessons learned and to improve Information System protection and incident response capabilities in the future. Post-incident review documentation must be communicated to entity leadership.

16.0 PHYSICAL SECURITY STANDARD

DATA CENTERS

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

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

16.2.1 This list must be reviewed and updated annually.
16.2.2 This list must be updated as user access privileges change.

16.3 Entities must 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 must be escorted by authorized personnel at all times.
16.3.2 Entities must log all visitor access to data centers that process, store or transmit Restricted-Use Information.

16.4 Data centers must 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 must ensure sufficient power protection is available for critical Information Systems to perform an orderly shutdown.

17.0 PERSONNEL SECURITY STANDARD

ACCEPTABLE USE

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

17.2 Entities must require users to acknowledge adherence to the entity acceptable use policy prior to being granted access to Information Systems.

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

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

PERSONNEL OPERATIONS

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

17.6 Entities must assign all users to a user categorization based upon their role and least privilege.

17.7 Entities must assign Information System authorizations to users based on user categorization and Information System classification.

17.8 Entities must revoke system access or eliminate unnecessary permissions for user accounts as users are transferred, terminated, or their role has changed.

17.9 Entities must recover all property that has been assigned to terminated personnel.

18.0 SECURE PURCHASING/ACQUISITION STANDARD

18.1 Entities must include system security requirements with all Requests for Proposal, Information, Quotation (RFP, RFI, RFQ) and all 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 least every three (3) years.

19.3 Entities must ensure verifiable compliance with these requirements no later than three (3) months from the effective date. Entities should ensure Variances or Exceptions are in place, in accordance with this standard, for any requirements they cannot meet.