ITEC Policy 8010A - Kansas DATA Review Board Standards10 TITLE: Kansas Data Compliance Requirements

1.1 EFFECTIVE DATE: July 1, 2021

Revised: March 9, 2021

1.2 TYPE OF ACTION: New Standards

2. PURPOSE: To define the Information Technology Policy 8010 minimum security standards and procedures for state of Kansas information systems. Ii will also define the requirements for Kansas data compliance for all agency business and information technology initiatives and acquisitions. Additionally, this policy will also define controls to establish formal oversight of the people, processes, and technologies that influence data throughout its lifecycle, with the intent of reducing risk and improving outcomes of processes that depend on or use data. These controls will provide increased assurance that data is reliable, accurate, timely, fit for use, interoperable, consistent, and protected from loss and unintended disclosure or alteration.

3.0 ORGANIZATIONS AFFECTED: All branches, boards, commissions, departments, divisions, and agencies of state government, hereafter referred to as Entities.

3.1 These standards apply to all employees and contractors within State Budget Units (BUs) who work with data or repositories of data while executing business functions, activities or services for or on behalf of the BU or its customers.

3.2 Applicability of these standards to third parties is governed by contractual agreements entered between BUs and the third party. For contracts in force as of the effective date, subject matter experts (SMEs) acting under the guidance of the Kansas Data Review Board (KDRB) should ascertain the applicability of these standards to third parties before seeking amendments. Prior to entering into new contracts, SMEs shall ascertain the applicability of these standards to third parties and include compliance requirements in the terms and conditions.

3.3 Applicability of these standards to specific information systems shall be determined by the Kansas Data Review Board (KDRB) as defined below. BUs may implement additional controls, roles, or organizational structures as they deem necessary to suit their business or project needs.

4.0 REFERENCES:

4.1 K.S.A. 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 8000, Revision 1, Information Technology Security Council Charter.

4.3 Kansas Information Technology Executive Council (ITEC), ITEC Policy 8010, Revision 1, General Information Technology Enterprise Data Governance Policy.

4.4 Kansas Information Technology Executive Council (ITEC), ITEC Standards 8010A, Revision 1, General Information Technology Enterprise Data Governance Standards.

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

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

4.7 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 DATA PROTECTION STANDARD([ITEC 7230A Paragraph 11](https://ebit.ks.gov/docs/default-source/itec/itec-7230a.pdf?sfvrsn=f3990f07_0))

* Entities must employ mechanism(s) to ensure the confidentiality, availability, and integrity of Restricted-Use Information.
* Restricted-Use Information that has met the retention requirements of a State Records Board-approved agency retention and disposition schedule must be removed, destroyed, or deleted in a verifiable manner.
* Restricted-Use Information must be protected from unauthorized disclosure.
* Entities must use encryption modules, ciphers, or algorithms found within the NIST FIPS 140-2 validated list when encrypting Restricted-Use Information.
* Restricted-Use Information when transmitted electronically outside of a secure boundary must be encrypted.
* Restricted-Use Information must be encrypted when stored on portable electronic media or devices. All portable media and devices, regardless of factor, shall be encrypted.
* Media containing Restricted-Use Information must be disposed of in accordance with NIST Special Publication 800-88 – Guidelines for Media Sanitization.
* 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.

6.0 CLASSIFICATION STANDARD: The data standard establishes how the agency’s data should be classified towards ensuring that the agency understands when it has sensitive data, the impacts of managing those classification types, and the controls to which it must adhere in order to proactively manage and secure sensitive data.

[ITEC 7230A Section 6](https://ebit.ks.gov/docs/default-source/itec/itec-7230a.pdf?sfvrsn=f3990f07_0) requires agencies classify their data.  While calculating classification cannot be easily quantified, the following table from Federal Information Processing Standards (FIPS) Publication 199 may help determine classification levels.

As the potential impact increases from Low to High, the classification should move from least restrictive to most restrictive.  If you are having difficulties determining the classification level of your data, please reach out to Information Security for assistance.

|  |  |  |  |
| --- | --- | --- | --- |
| **POTENTIAL IMPACT** | | | |
| **Security Objective** | **LOW** | **MODERATE** | **HIGH** |
| ***Confidentiality***  Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information could be expected to have a **limited**adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious**adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic**adverse effect on organizational operations, organizational assets, or individuals. |
| ***Integrity***  Guarding against improper  information modification  or destruction, and includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information could be expected to have a **limited**adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious**adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic**adverse effect on organizational operations, organizational assets, or individuals. |
| ***Availability***  Ensuring timely and reliable access to and use of information. | The disruption of access to or use of information or an information system could be expected to have a **limited**adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious**adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic**adverse effect on organizational operations, organizational assets, or individuals. |
| Data Examples  Guidance for the sensitivity of various types of information. |  | Employee employment applications, personnel files, benefits, salary, personal contact information   Non-public policies, manuals, and contracts   Internal memos and email, non-public reports, budgets, plans, financial info | Social Security Number   Date of Birth   Driver's License/State ID Number   Bank/Financial Account Number   Credit/Debit Card Number   Visa/Passport Number   Electronic Protected Health Information (ePHI)   Export controlled information under U.S. laws   Donor contact information and non-public gift information  **Caveats:** SSA, New Hire, HIPPA, |

All data and information systems must be classified into one of the following three categories.  Any data or system that is not classified by the data or system owner is automatically placed at the Restricted level.

**Restricted Data:** Data should be classified as Restricted when its unauthorized disclosure, alteration, or destruction could cause serious or catastrophic harm or risk to the agency and the Citizens of Kansas. The most restrictive security controls will be applied to this classification.

**Private Data:** Data should be classified as Private when its unauthorized disclosure, alteration, or destruction could result in a moderate level of harm or risk to the agency and the Citizens of Kansas.

**Public Data:** Data should be classified as Public when its unauthorized disclosure, alteration, or destruction would result in little to no harm or risk to the agency and the Citizens of Kansas.

**Determine How Much Protection Your Information Needs**

The amount and type of protection to be applied to your information depends on an assessment of the need for ***Confidentiality*** and/or the critical nature of the information.

These classifications are in line with the Federal Government Data classifications found in Executive Order 13292. The exception is that the Federal Government has no consistent designation for Public Data. In some cases, the term Unclassified is used to denote non-Confidential, non-Secret, and non-Top Secret Data.

For clarity, the State of Kansas chooses to use the terms Public Data rather than non-Confidential, non-Secret, and non-Top Secret Data. One core value that distinguishes a classification from another is the risk of harm. What is the risk that harm can result from the inappropriate disclosure or use of this information?

|  |  |
| --- | --- |
| **Data Element** | **Classification Recommendation** |
| Social Security Number | Restricted |
| Employee ID | Restricted |
| Bank Account Number | Restricted |
| Credit Card Number | Restricted |
| Mother’s Name | Private |
| Father’s Name | Private |
| Place of Birth | Private |

**Data that could be classified as: State of Kansas Public**

|  |  |
| --- | --- |
| **Data Element** | **Classification** |
| Audit Reports | Excluding data that provides knowledge that could be used to injure the State, its Citizens, or business partners. |
| Agency Policies | Excluding data that provides knowledge that could be used to injure the State, its Citizens, or business partners. |
| Computer Usage History | Excluding data that provides knowledge that could be used to injure the State, its Citizens, or business partners. |
| Expenditure Data | Excluding data that is covered by agreement or contract, for example non-disclosure agreements. |
| Revenue Data | Excluding data that is not Public because of law. |

**Data that could be classified as: State of Kansas Private**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Information/Data Type** | **PII**  **Personally**  **Identifiable**  **Information** | **PFI**  **Personal**  **Financial**  **Information** | **PHI**  **Personal**  **Health**  **Information** | **Other** |
| Payroll records | **X** | **X** | **X** |  |
| Personnel records | **X** | **X** | **X** |  |
| Elections records | **X** |  |  |  |
| Personal income tax records | **X** | **X** |  |  |
| Financial institution information on one person or business |  | **X** |  |  |
| Information covered by non-disclosure agreements or federal law |  |  |  | **X** |
| Facts on disaster recovery plans |  |  |  | **X** |
| Information about an investigation |  |  |  | **X** |
| Passwords giving access to data. (For example, a citizen’s password granting access only to their Confidential record) |  |  |  | **X** |
| Technical documentation, i.e., detailed network port/IP diagrams and system architectures for systems containing public, private, or restricted data |  |  |  | **X** |
| Defendant or witness PII records | **X** |  |  |  |

*\*records may contain multiple types of sensitive data.*

# **Data that could be classified as: State of Kansas Restricted**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **\*Information/Data Type** | **PII**  **Personally**  **Identifiable**  **Information** | **PFI**  **Personal**  **Financial**  **Information** | **PHI**  **Personal**  **Health**  **Information** | **Other** |
| Payroll files | **X** | **X** | **X** |  |
| Personnel files | **X** | **X** | **X** |  |
| Elections files | **X** |  |  |  |
| Personal income tax files | **X** | **X** |  |  |
| Financial institution information on one person or business |  | **X** |  |  |
| Passwords giving access to restricted data |  |  |  | **X** |
| Data that is specifically protected by law, for example: HIPAA or GLBA |  |  |  | **X** |
| Disaster recovery plan information, such as location of recovery sites, activation codes, PII on individual roles in a disaster, etc. |  |  |  | **X** |
| Information about investigations, audits, etc. |  |  |  | **X** |
| Information covered by non-disclosure agreements or federal law | **X** |  |  |  |
| Technical documentation, i.e., detailed network port/IP diagrams and system architectures for systems containing restricted data |  |  |  | **X** |
| Expunged court cases |  |  |  | **X** |
| Sealed court cases or child support information |  |  |  | **X** |
| Information about investigations, undercover officers, police raids, etc. |  |  |  | **X** |
| Passwords giving access to restricted data |  |  |  | **X** |
| Defendant or witness PII records | **X** |  |  |  |
| Information regarding an individual’s health |  |  | **X** |  |

*\*files may contain multiple types of sensitive data.*

[For Definitions of PII, PFI and PHI, see ITEC 7230A sections 5.7, 5.8, and 5.11](https://ebit.ks.gov/docs/default-source/itec/itec-7230a.pdf?sfvrsn=f3990f07_0)

# **Data that could be classified as: Federal Restricted**

Below is a partial list of federal sensitive data types, not all of which will apply to state agencies.

|  |  |  |
| --- | --- | --- |
| **DATA TYPE** | **State PIA Y/N** | **Full Name** |
| [FTI](https://www.irs.gov/pub/irs-pdf/p4761.pdf) | Y | Federal Tax Information |
| [SSA](https://www.ssa.gov/dataexchange/privacyinfo.html) | Y | Social Security Administration data |
| [NDNH](https://www.dshs.wa.gov/esa/interface-data/national-directory-new-hires-ndnh) | Y | National Directory of New Hires |
| [HPI](https://en.wikipedia.org/wiki/History_of_the_present_illness) | Y | Health Insurance Portability and Accountability Act |
| [PII](https://en.wikipedia.org/wiki/Personal_data) | Y | Personal Identifiable Information data |
| [SOX](https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf) | Y | Sarbanes–Oxley Act |
| [PCI](https://www.pcisecuritystandards.org/) | Y | Payment Card Industry Data Security Standard |
| [GLBA](https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act) | N | Gramm-Leach-Bliley Act |
| [GDPR](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation) | Y | General Data Protection Regulation |
| [COPPA](https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step2) | Y | Children’s Online Privacy Protection Act |
| [CJIS](https://datastandards.cjis.gov/#:~:text=The%20Criminal%20Justice%20Information%20Services,law%20enforcement%20and%20public%20safety.&text=The%20Department%20of%20Justice%20(DOJ,the%20technology%20for%20exchanging%20data.) | Y | Criminal Justice Information Services |
| [FISMA](https://www.cisa.gov/federal-information-security-modernization-act) | N | Federal Information Security Management Act of 2002 |

**6.1 Data Privacy Standards:** Agencies must abide by all federal and state privacy laws. Data privacy or information privacy is a branch of data security concerned with the proper handling of data – consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around:

* Whether or how data is shared with third parties.
* How data is legally collected or stored.
* Regulatory restrictions such as [GDPR](https://www.varonis.com/blog/gdpr-requirements-list-in-plain-english/), [HIPAA](https://www.varonis.com/blog/hipaa-compliance/), [GLBA](https://www.varonis.com/blog/we-need-to-talk-about-gramm-leach-bliley-glb-the-safeguards-rule-will-be-changing/), or [CCPA](https://www.varonis.com/blog/california-consumer-privacy-act-ccpa/).
* Fulfilling required privacy posting notices when collecting data.
* A [Privacy Impact Assessment](https://www.sec.gov/about/privacy/piaguide.pdf) should be completed for sensitive data, the table below shows where this is required.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DATA TYPE** | **PIA Y/N** | **Full Name** | **Parameters** | **Notes** |
| [FTI](https://www.irs.gov/pub/irs-pdf/p4761.pdf) | N | Federal Tax Information | Publication 1075 Safeguards - NIST Moderate Controls | This is directed to Tax information received from the IRS or derived from IRS FTI Data. |
| [SSA](https://www.ssa.gov/dataexchange/privacyinfo.html) | N | Social Security Administration data | SSA Safeguards and Pub 1075 | Corresponding state privacy statute (K.S.A 44-714e) and regulation KAR 50-4-2; also Information Exchange Agreement with SSA for SSA data |
| [NDNH](https://www.dshs.wa.gov/esa/interface-data/national-directory-new-hires-ndnh) | Y | National Directory of New Hires | NDNH Safeguards | Confidentiality and security requirements outlined in computer matching agreement with US Dept. of HHS. |
| [HIPAA](https://en.wikipedia.org/wiki/History_of_the_present_illness) | Y | Health Insurance Portability and Accountability Act | [PIA Privacy Impact Assessment](https://www.sec.gov/about/privacy/piaguide.pdf) | This Act only applies to health plans, health care clearing houses and health care providers which transmit health care information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA. |
| [PII](https://en.wikipedia.org/wiki/Personal_data) | Y | Personal Identifiable Information data | [PIA Privacy Impact Assessment](https://www.sec.gov/about/privacy/piaguide.pdf) | See Data Sensitivity Worksheet |
| [SOX](https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf) | N | Sarbanes–Oxley Act (not applicable to state agencies) | [SOX Controls](https://www.sarbanes-oxley-101.com/) | All publicly-traded companies are required to implement and report internal accounting controls to the SEC for compliance. In addition, certain provisions of Sarbanes-Oxley also apply to privately-held companies. |
| [PCI](https://www.pcisecuritystandards.org/) | Y | Payment Card Industry Data Security Standard | [PCI Controls](https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1612544251303) | This is an industry standard established by the five credit card companies, American Express, Discover, JCB, MasterCard and Visa. It only applies to merchants who accept credit card payments and retain the cardholder information from those transactions. |
| [GLBA](https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act) | Y | Gramm-Leach-Bliley Act | [Privacy Rules](https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-privacy-rule-auto-dealers-faqs) | This applies to companies that offer consumer products or services such as loans, financial or investment advice or insurance. Agencies offering Federal Loans may check this for applicability. |
| [GDPR](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation) | Y | General Data Protection Regulation | [PIA Privacy Impact Assessment](https://www.sec.gov/about/privacy/piaguide.pdf) | This is an international agreement that only applies to U.S. companies that offers goods and/or services to residents of Europe or European Economic Areas, (EU/EEA) or monitors the behavior of users inside the EU/EEA. Agencies that recruit EU companies to create a presence in the US may have applicability. |
| [COPPA](https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step2) | Y | Children’s Online Privacy Protection Act | [Steps](https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step6) | Applies only to entities that maintain websites or online services that collect information form minors under the age of thirteen. |
| [PHI](https://en.wikipedia.org/wiki/Protected_health_information) | Y | Protected Health Information | [PIA Privacy Impact Assessment](https://www.sec.gov/about/privacy/piaguide.pdf) | This can be non HIPPA Health information provided to Agencies (gaming ect) |
| Consumer Information | Y | Protection of Consumer Information 50-7a02 | Reporting obligations under 50-7a02 in event of breach | State statutes 50-7a01, et seq., has reporting obligation to affected Kansas residents in the event of a breach of Consumer Information. Work with Legal. |
| Public Data | N | Non Restricted Unclassified Data | Best Practice | There are Unemployment Insurance regs (UI-PIL). These aren't really regs as much as they are recommended practices. |

**6.2 Data Retention Standards**

All agency data and information must be retained, archived, and destroyed in accordance with federal and state laws and regulations, general administrative practices, and records management principles. All archival and disposition procedures must be documented and performed in such a way as to ensure that confidentiality and security are maintained.

**A. Statutory Authority**

The primary statutes and regulations governing state agency records are the Government Records Preservation Act (K.S.A. 45-401 through 45-414), the Public Records Act (K.S.A. 75-3501 through 75-3518), K.A.R. 53-3-1, the Kansas Open Records Act (K.S.A. 45-215 through 45-229), the Kansas Open Meetings Act (K.S.A. 75-4317 through 75-4320c). Under the Public Records Act, the State Records Board (SRB) oversees the permanent preservation of important state records and to provide for the orderly destruction of other state records. The Electronic Records Committee (ERC), a subcommittee of the SRB and the Information Technology Advisory Board (ITAB), recommends and reviews policies, guidelines, and best practices for the creation, maintenance, and long-term preservation of and access to electronic records created by state agencies.

All agencies must appoint a staff member to serve as the agency records officer pursuant to K.A.R. 53-4-1.

**B. Records Retention and Disposition Schedules**

All state agencies are required to create, follow, and maintain retention and disposition schedules for all records they create or receive. These schedules are designed to assure the identification and protection of vital records, ensure compliance with the Kansas Open Records Act, provide clear guidance on the length of time to retain records, and identify the appropriate disposition for all records. The information found in a retention and disposition schedule includes the record series title and description, a ***minimum*** retention period, final disposition requirements, and access restrictions. All agencies must follow two sets of retention and disposition schedules for their records. The [General Records Retention and Disposition Schedule](https://www.kshs.org/recmgmt/retention_schedule_entries/search/agency:000/submit:SEARCH/searchtype:state/limit:1000) includes guidelines for record series maintained by most state agencies, such as annual and special reports, meeting minutes, and employee personnel files. An [Agency Records Retention and Disposition Schedule](https://www.kshs.org/recmgmt/retention_schedule_entries/browse) addresses records unique to a particular agency. All retention and disposition schedules must be approved by the SRB to ensure that the agency is in compliance with all applicable statutes and regulations. If a state agency is retaining records in electronic format for more than ten years, it must also present an Electronic Recordkeeping Plan to the ERC.

**C. Electronic Records**

Kansas statutes define records by their function rather than their physical format. According to K.S.A. 45-402(d) (emphasis added):

*“Government records” means all volumes, documents, reports, maps, drawings, charts, indexes, plans, memoranda, sound recordings, microfilms, photographic records and other data, information or documentary material,* ***regardless of physical form or characteristics****, storage media or condition of use, made or received by an agency in pursuance of law or in connection with the transaction of official business or bearing upon the official activities and functions of any governmental agency.*

Records retention and disposition schedules likewise apply to records regardless of their physical format. An agency must retain one official copy of all records it creates or receives. However, it is up to each agency to decide whether to retain this record copy in paper or electronic format.

**Disposition of Records**

Records may only be destroyed if they have met their retention and disposition requirements. Unauthorized destruction of records is a Class A misdemeanor under K.S.A. 21-5920. To ensure the confidentiality of agency data, paper records containing personally identifiable information must be shredded or burned and all computer equipment must be sanitized prior to reassignment or disposal.

**Review of Schedules**

An agency’s retention and disposition schedules must be reviewed periodically to determine their usefulness and accuracy for agency interpretation. Agency personnel should contact the Public Records staff at the Kansas Historical Society for assistance in creating or modifying their agency’s retention and disposition schedules or for any questions regarding records management.

7.0 PROCEDURES:

7.1 Each agency will be required to have Data Policies and Controls that are aligned with [ITEC 7230A](https://ebit.ks.gov/docs/default-source/itec/itec-7230a.pdf?sfvrsn=f3990f07_0) as well as ITEC 8010A and any other compliance requirements.  These should be clearly defined in their policy and supporting evidence should be available upon request for audits.   Best practice states agencies will review policies, standards and agreements annually and record evidence of the reviews.

7.2 Each year agencies will be required to complete a [Data Sensitivity Assessment](https://teams.microsoft.com/l/file/56BDDF12-A106-4D7A-9641-8D9084E4C3ED?tenantId=dcae8101-c92d-480c-bc43-c6761ccccc5a&fileType=xlsx&objectUrl=https%3A%2F%2Fsokansas.sharepoint.com%2Fsites%2FITECPolicyReviewTeam-8000%2FShared%20Documents%2FGeneral%2FPolicies%2FData%20Sensitivity%20Worksheet.xlsx&baseUrl=https%3A%2F%2Fsokansas.sharepoint.com%2Fsites%2FITECPolicyReviewTeam-8000&serviceName=teams&threadId=19:a68391611b8345e78714f7ae74cc6de2@thread.tacv2&groupId=cdd96872-8b03-421a-ad65-dc4a2052a446) which declares what types of data it manages and supporting evidence should be available upon request for audits.  This is to be completed by the last Friday of February annually and submitted to the Chief Information Technology Architect (CITA) and the State Archivist.

7.2 Any agency managing sensitive data as determined by their Data Sensitivity Assessment will also provide a copy of its Data Policies and Controls by the last Friday of February annually, submitted to the CITA and the State Archivist. Agencies are required to perform and record annual reviews of their policies.

7.3 Agencies which share (either receive or send) restricted data will be required to have a data sharing agreement in place for such data to be made available upon request for audits. Agencies are required to perform and record annual reviews of their data sharing agreements.

7.5 For state agencies managing federal and state designated sensitive data and other types of sensitive information subject to privacy laws, it is suggested as a matter of due diligence and best practice they conduct a [Privacy Impact Assessment (PIA)](https://www.nist.gov/system/files/documents/2017/05/09/NIST-TIP-PIA-Consolidated.pdf) and post the proper privacy notices as required on collection instruments and customer facing applications as well as ensure they are reviewed and updated annually. A more complete list of federal data types requiring a PIA appear in section 6.3.

8.0 RESPONSIBILITIES:

8.1 Heads of entities will establish procedures for their organization's compliance with the requirements of this policy.

8.2 The Chief Information Technology Officer, Executive Branch, is responsible for the review and maintenance of this policy no less than every 3 years.

8.3 The CITA and Chief Information Security Officer (CISO) will work together to ensure that the compliance guidance meets the state’s requirements.

9.0 GUIDES AND AIDS FOR AGENCIES:

9.1 [Sample Data Policies](https://teams.microsoft.com/l/file/77941C52-708F-4162-B189-94DEDC2DF321?tenantId=dcae8101-c92d-480c-bc43-c6761ccccc5a&fileType=docx&objectUrl=https%3A%2F%2Fsokansas.sharepoint.com%2Fsites%2FITECPolicyReviewTeam-8000%2FShared%20Documents%2FGeneral%2FPolicies%2FNIST%20800-53%20R4%20Moderate%20Policy_Examples.docx&baseUrl=https%3A%2F%2Fsokansas.sharepoint.com%2Fsites%2FITECPolicyReviewTeam-8000&serviceName=teams&threadId=19:a68391611b8345e78714f7ae74cc6de2@thread.tacv2&groupId=cdd96872-8b03-421a-ad65-dc4a2052a446) and Controls

9.2 [GSA Privacy Policy and Procedures Guide](https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-and-procedures-guide)

9.3 We strongly advocate a [NIST 800-53](https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) Moderate Control set for agencies managing restricted data.

9.4 A [Privacy Impact Assessment (PIA)](https://www.nist.gov/system/files/documents/2017/05/09/NIST-TIP-PIA-Consolidated.pdf)

9.5 Definitions

**Physical Data and Media:** All forms of paper based or physical static representations of data, both private and restricted, should be properly labeled by its owner with, classification and retention period and stored securely at all times while it is not being actively used. Cover pages should be used for all document collections. Cabinets and drawers should be locked and the data owner should have an inventory of all physical data.

**Electronic media:** Includes television, radio, Internet, fax, CD-ROMs, DVD, and any other medium that requires electricity or digital encoding of information. The term 'electronic media' is often used in contrast with print media.

**Example for Email** - Perhaps one of the most well known and ubiquitous forms of electronic communication, email provides a channel for exchanging messages in much the same method as traditional mail. One user generates a message, addresses it to a recipient, sends it and, if one is warranted, waits for a reply. The asynchronous nature of email makes it ideal for users who do not want to become involved in, or do not have time for, a lengthy conversation. See [ITEC 6401G](https://ebit.ks.gov/docs/default-source/itec/itec-6401-email-guidelines-0609206ac296b844744ed09d2780ab4455b27d.pdf?sfvrsn=aeb6d815_2) for additional policy.

**Example for Instant Messages** - Much like email, instant messages allow you to generate a message, send it and wait for a reply. Unlike email, though, instant messages connect users through a central server that instantly delivers the electronic communication. Because both the sender and the recipient must typically be logged in to start an instant message communication, the immediate message delivery facilitates a near real-time conversation. When the instant message server connects multiple users to each other, it acts as a chat room where many users can instantly exchange messages with one another, meet new people and even set up private instant messaging conversations.

**Example for Text Messages** - Mobile [phone](http://rover.ebay.com/rover/13/0/19/DealFrame/DealFrame.cmp?bm=413&BEFID=96392&acode=439&code=439&aon=&crawler_id=519394&dealId=Gd9pGccAe43JYtDs_Fh3cg%3D%3D&searchID=&url=http%3A%2F%2Fclickserve.dartsearch.net%2Flink%2Fclick%3Flid%3D92700014253699823%26ds_s_kwgid%3D58700000493190863%26ds_s_inventory_feed_id%3D97700000001002072%26ds_e_product_id%3DMN5X2LL%2FA%26ci_customer_id%3D1001292%26ci_cse_id%3D1004%26ci_feed_id%3D1004591%26ds_e_product_merchant_id%3D1378784%26ds_e_product_country%3DUS%26ds_e_product_language%3Den%26ds_e_product_channel%3Donline%26ds_url_v%3D2%26ds_dest_url%3Dhttps%3A%2F%2Fwww.verizonwireless.com%2Fsmartphones%2Fapple-iphone-7-plus%2F%2523sku%253Dsku2150075%253Fcmp%253Dcse-Shopping-MN5X2LL%2FA%2526cmp%253DCSE-C-HQ-NON-R-AC-NONE-NONE-2C0PX0-PX-EBAY-MN5X2LL%2FA%2526cvosrc%253Dcse.EBAY.MN5X2LL%2FA%2526cvo_crid%253D%257Bcampaign%257D&DealName=Apple%C2%AE%20iPhone%C2%AE%207%20Plus%20128GB%20in%20Jet%20Black&MerchantID=519394&HasLink=yes&category=0&AR=-1&NG=1&GR=1&ND=1&PN=1&RR=-1&ST=&MN=msnFeed&FPT=SDCF&NDS=1&NMS=1&NDP=1&MRS=&PD=0&brnId=2455&lnkId=8070676&Issdt=180108051904&IsFtr=0&IsSmart=0&dlprc=769.99&SKU=MN5X2LL%2FA) users can use electronic communication on the go with a service known as Short Messaging Service. SMS messages, which are more commonly known as text messages, allow you to send an electronic communication of up to 160 characters to another SMS-enabled [device](http://rover.ebay.com/rover/13/0/19/DealFrame/DealFrame.cmp?bm=413&BEFID=96424&acode=456&code=456&aon=&crawler_id=519394&dealId=e2EuKNGiqzJ15_Fb6_DE8w%3D%3D&searchID=&url=http%3A%2F%2Fclickserve.dartsearch.net%2Flink%2Fclick%3Flid%3D92700027451226249%26ds_s_kwgid%3D58700000493190863%26ds_s_inventory_feed_id%3D97700000001002072%26ds_e_product_id%3DMQK82LL%2FA%26ci_customer_id%3D1001292%26ci_cse_id%3D1004%26ci_feed_id%3D1004591%26ds_e_product_merchant_id%3D1378784%26ds_e_product_country%3DUS%26ds_e_product_language%3Den%26ds_e_product_channel%3Donline%26ds_url_v%3D2%26ds_dest_url%3Dhttps%3A%2F%2Fwww.verizonwireless.com%2Fconnected-devices%2Fapple-watch-series-3-stainless-steel-42mm-case-with-sports-band%2F%2523sku%253Dsku2680254%253Fcmp%253Dcse-Shopping-MQK82LL%2FA%2526cmp%253DCSE-C-HQ-NON-R-AC-NONE-NONE-2C0PX0-PX-EBAY-MQK82LL%2FA%2526cvosrc%253Dcse.EBAY.MQK82LL%2FA%2526cvo_crid%253D%257Bcampaign%257D&DealName=Apple%C2%AE%20Watch%20Series%203%2C%2042mm%20Stainless%20Steel%20Case%20with%20Soft%20White%20Sport%20Band%2C%20Adult%20Unisex%2C%20Silver%2FSoft%20White&MerchantID=519394&HasLink=yes&category=0&AR=-1&NG=1&GR=1&ND=1&PN=1&RR=-1&ST=&MN=msnFeed&FPT=SDCF&NDS=1&NMS=1&NDP=1&MRS=&PD=0&brnId=2455&lnkId=8070676&Issdt=180108051904&IsFtr=0&IsSmart=0&dlprc=649.99&SKU=MQK82LL%2FA). Though mobile phone owners typically use text messages to communicate directly with another individual via phone, SMS can allow users to interact with almost any SMS-capable machine.

**Example for Audio** - Electronic audio communication dates back to the 1876 invention of the telephone, a device that converts sounds into electrical impulses and sends them over copper wires to a remote unit that converts them back into sound. Today, though, audio traverses an array of electronic channels that includes radio, television, mobile phones and even Internet-connected electronic devices.

**Example for Video** - Many are familiar with video as an electronic communication channel like TV or movies, but modern broadband Internet allows video to serve as a somewhat more interactive medium. By capturing a rapid series of photos, bundling them with sound and transmitting them over the Internet to a remote user, webcams allow users to instantly communicate via full-motion video chat.

**Example for Storage Devices** - Hard Drives, USB Drives, Flash cards and any other viable means of electronically storing data.