|  |  |
| --- | --- |
| LOGO | *Data Security* *Policy* |
| Information Security Policy (All) | Policy # 6.800  Page 1 of 127 |
| Approved:  Name, Secretary | Adopted: DATE  Revised: DATE, DATE, DATE |

**EXAMPLE ONLY**

<Your Agency Name Here> search and replace all “include <>

**Information Security Policy**

**NIST 800.53 R4**

|  |  |  |  |
| --- | --- | --- | --- |
| **TABLBLE of CONTENTS** | **Page #** |  |  |
| **Title Page** | **1** |  |  |
| **Table of Contents** | **2** |  |  |
| **Purpose Scope Intent** | **3** |  |  |
| **Roles & Responsibilities** | **3** |  |  |
| **Policy & Control Structure** | **6** |  |  |
| **Policy Structure** | **6** |  |  |
| **Control Selection Variable & Implementation** | **8** |  |  |
| **information Security Policies** | **15** |  |  |
| **AC – Access Controls policy** | **15** |  |  |
| **AC – Visitors Policy** | **21** |  |  |
| **AC – Digital Certificate Management Policy** | **25** |  |  |
| **AC – Data Leakage Protection Policy** | **28** |  |  |
| **AC – Remote Access Policy** | **30** |  |  |
| **AC – Mobile Device Policy** | **31** |  |  |
| **AC – Telecommute Policy** | **38** |  |  |
| **AC – Acceptable Use of Information Technology Resources Policy** | **47** |  |  |
| **AU – Security Audit and Accountability Policy** | **52** |  |  |
| **AT – Security Awareness Policy** | **56** |  |  |
| **CM – Configuration Management Policy** | **58** |  |  |
| **CP – Contingency Planning Policy** | **61** |  |  |
| **IR – Privacy and Incident Response Policy** | **62** |  |  |
| **IA – Identification and Authorization Policy** | **66** |  |  |
| **MA – Systems Maintenance Policy** | **73** |  |  |
| **MP – Media Protection Policy** | **75** |  |  |
| **MP – Data Classification Policy** | **77** |  |  |
| **MP – Media Sanitization Policy** | **81** |  |  |
| **MP – Data Encryption Policy** | **85** |  |  |
| **PS – Personnel Security Policy** | **94** |  |  |
| **PE – Physical Environment Policy** | **97** |  |  |
| **PL – Security Planning Policy** | **99** |  |  |
| **PM – Security Program Management Policy** | **101** |  |  |
| **RA – Security Risk Assessment Policy** | **103** |  |  |
| **RA – Approval Policy** | **106** |  |  |
| **CA - Security Assessment and** Authorization **Policy** | **108** |  |  |
| **SC - System and Communications Protection Policy** | **110** |  |  |
| **SI - Security System and Information Integrity Policy** | **113** |  |  |
| **SA - System and Services Acquisition Policy** | **117** |  |  |
| **AP – Privacy Policy (includes SE, AP, AR, DI, DM, IP, TR, & UL)** | **118** |  |  |
| **Policy Compliance** | **123** |  |  |
| **Policy Authority** | **124** |  |  |
| **Document Version Control** | **124** |  |  |
|  |  |  |  |
|  |  |  |  |

## Purpose

This policy establishes the <Your Agency Name Here> Security Policy, in order to properly secure <Your Agency Name Here> information assets; access controls are necessary and required. This policy encompasses the controls from (NIST 800-53 – R4) that are embedded in this policy. Additional policies and control language have been added as well as required to meet both state and agency standards.

## Scope

The scope of this policy is applicable to all Employees, Information Services (IS) resources owned or operated by the <Your Agency Name Here>. Any information not specifically identified as the property of other parties, that is transmitted or stored on resources (including e-mail, messages and files) is the property of each state or federal agency and resides in their associated <Your Agency Name Here> instance. All users <Your Agency Name Here> employees, each states employee’s, contractors, vendors or others) of IS resources are responsible for adhering to this policy.

## Intent

The overall body of <Your Agency Name Here> Information Security Policies serve to be consistent with best practices associated with standard organizational Information Security management and the NIST 800-53 R4 adopted controls and the Kansas ITECH 7230 standards the agency uses. It is the intention of this body of policies to establish a security standard throughout <Your Agency Name Here> to help the organization implement security best practices with regard to access to <Your Agency Name Here> IS systems.

## Responsibilities

The agency manages its security through a virtual security organization structure which roles up in relation to its internal Governance, Compliance and Risk Management Council.  These Role apply to all policies unless otherwise noted or otherwise supplemented with additional role and responsibility notifications.

|  |  |  |  |
| --- | --- | --- | --- |
| **IT System Name, Acronym, and Designation** | **Security Roles and Responsibilities** | **Column1** | **Column2** |
| **Role** | **Responsibility** | **Job Title** | **Reports To** |
| Agency Head | Oversee State Agency IT Security Program | \*Outside or <Your Agency Name Here> Agency Leader | Reports to the State Executive Management |
| Information Security Officer | Overall security of Agency Data and liaison to the CISO of the State of Kansas. | \*Outside or <Your Agency Name Here> Agency ISO | Reports to the State Data Owner |
| Privacy Officer | Provide guidance on privacy laws. | \*Outside or <Your Agency Name Here> Agency PO | Reports to the State Data Owner |
| Data Owner | Responsible for the overall security of the IT system. Accountable to the Agency Head. | \*Outside or <Your Agency Name Here> Agency Leader | Reports to the State Agency Head |
| Data Custodian | A Data Custodian is responsible to protect data from unauthorized access, alteration, destruction, or usage and in a manner consistent with <Your Agency Name Here> IT security policies and standards applicable to the assigned classification level | \*Outside or <Your Agency Name Here> Agency Data Owner Appointee | Reports to the State Data Owner |
| Data User & End User | Read/comply with Agency IT security requirements | \*Outside or <Your Agency Name Here> Agency End Users | Acknowledged through acceptable use policy and privacy policy upon signup or internally on an annual basis as a part of awareness training. |
| System Owner | Spreads IT security awareness to data users. Develops any additional local requirements, guidelines and procedures needed to protect the data. | <Your Agency Name Here> IT <IT Director Title> of Commerce | Reports to the Agency Head or Designee |
| System Security and Network Security Administrator | Day-to-day administration of the IT system. Implements requirements of the IT Security Management Program. | <Your Agency Name Here> IT Manger | Reports to the System Owner |
| System Account Administrator | Responsible for user access and permissions within the application | <Your Agency Name Here> IT <IT Director Title> of Commerce | Reports to the Agency Head or Designee |
| System Program Manager | Responsible for Application Development Delivery | <Your Agency Name Here> Program Manager | Reports to the Agency Head or Designee |
| System Privacy Officer | Responsible for Application Development Delivery | <Your Agency Name Here> Customer Relations Manager | Reports to the System Owner if Applicable |
| System Information Security Officer | Overall security of System and liaison to the CISO of the State of Kansas. | <Your Agency Name Here> ISO | Reports to the KISO CISO and System Owner if Applicable |
| <Your Agency Name Here> Support Staff – includes all contracted agents and designees supporting <Your Agency Name Here> systems | Accountable to the Agency Secretary of XXXXXXXX to manage the day to day development and operations of the <Your Agency Name Here> systems. | All <Your Agency Name Here> Staff | Reports to the System Owners Management Team and/or the System Owner Directly. |
| \*Outside - Defined | Any agency \*Outside <Your Agency Name Here> for whom the data belongs | External Agency or Data Owning Organization | NA |

## Policies & Control Structure

These policies encompass and are derived from the (NIST 800-53 – R4). Additional policies and control language maybe be added and will be noted appropriately as required to meet both state and agency standards.

Additionally, the agency has derived policies from the NIST 800-53 R4 Privacy Controls. Controls and agency specific control variables will be listed in the controls section of this document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Abbreviation** | **Control** | **Policy #** | **Policy Name** |
| **AC** | Access Controls | 6.800.01 | Information Security Access Controls Policy |
| **AC** | Access Controls | 6.800.02 | Visitors Policy |
| **AC** | Access Controls | 6.800.03 | Digital Certificate Management Policy |
| **AC-3 (3)** | Access Controls | 6.800.04 | Data Leakage Protection |
| **AC-17** | Access Controls | 6.800.05 | Remote Access |
| **AC-19** | Access Controls | 6.800.06 | Mobile Device Policy |
| **AC** | Access Controls | 6.800.07 | Telecommute Policy |
| **AC** | Access Controls | 6.800.08 | Acceptable Use of Information Technology Resources |
| **AU** | Audit and Accountability | 6.800.09 | Information Security Audit and Accountability |
| **AT** | Awareness and Training | 6.800.10 | Information Security Awareness Policy |
| **CM** | Configuration Management | 6.800.11 | Configuration Management Policy |
| **CP** | Contingency Planning | 6.800.12 | Contingency Planning Policy V1.0 |
| **IR** | Incident Response | 6.800.13 | Privacy & Security Incident Reporting |
| **IA** | Identification and Authentication | 6.800.14 | Identification and Authentication - Was PW Protection |
| **MA** | Maintenance | 6.800.15 | Security Systems Maintenance |
| **MP** | Media Protection | 6.800.16 | Information Security Media Protection (MP-1-5) MP7-8) |
| **MP** | Media Protection | 6.800.17 | Data Classification |
| **MP** | Media Protection | 6.800.18 | Media Sanitization Policy (MP-6) |
| **MP** | Media Protection | 6.800.19 | DATA Encryption Policy |
| **PS** | Personnel Security | 6.800.20 | Information Security Personnel Security |
| **PE** | Physical Environmental Protection | 6.800.21 | Information Security Physical and Environmental |
| **PL** | Planning | 6.800.22 | Information Security Planning |
| **PM** | Program Management | 6.800.23 | Information Security Program Management |
| **RA** | Risk Assessment | 6.800.24 | Information Security Risk Management |
| **RA** | Risk Assessment | 6.800.25 | Approval Process |
| **CA** | Assessment, Authorization, and Monitoring | 6.800.26 | Information Security Assessment and Authorization |
| **SC** | System and Communications Protection | 6.800.27 | Information Security System and Communications Protection |
| **SI** | System and Information Integrity | 6.800.28 | Information Security System and Information Integrity |
| **SA** | System and Services Acquisition | 6.800.29 | Information Security System and Services Acquisition |
|  |  |  |  |
| **SE** | Security and Privacy | 6.800.30 | Master Privacy Policy |
| **AP** | Authority and Purpose | 6.800.30 | Inserted in Privacy Policy |
| **AR** | Accountability Audit & Risk Management | 6.800.30 | Inserted in Privacy Policy |
| **DI** | Data Quality and Integrity | 6.800.30 | Inserted in Privacy Policy |
| **DM** | Data Minimization | 6.800.30 | Inserted in Privacy Policy |
| **IP** | Individual Participation | 6.800.30 | Inserted in Privacy Policy |
| **TR** | Transparency | 6.800.30 | Inserted in Privacy Policy |
| **UL** | Use limitation | 6.800.30 | Inserted in Privacy Policy |

## Control Implementation

|  |  |  |  |
| --- | --- | --- | --- |
| **Agency NIST 800-53 R4 Moderate Control Implementation – Tailored** | | | |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [AC](https://nvd.nist.gov/800-53/Rev4/family/ACCESS%20CONTROL) | Access Controls | AC-1, AC-2 (1) (2) (3) (4), AC-3, AC-4, AC-5, AC-6 (1) (2) (5) (9) (10), AC-7, AC-8, AC-11 (1), AC-12, AC-14, AC-17 (1) (2) (3) (4), AC-18 (1), AC-19 (5), AC-20 (1) (2), AC-21, AC-22 | AC-2(5)(6)(7)(13), AC-6(7)(7), AC-19(4) |
|  | AC-1(b1,b2) | Annual |  |
|  | AC-2(2) | Disables within 1 hour after authorized usage expires |  |
|  | AC-2(3) | 180 days |  |
|  | AC-2(5) | 30 Minutes |  |
|  | AC-2(13) | 1hour |  |
|  | AC-7(a) | 3 Attempts in 10 minutes |  |
|  | AC-11(a) | 30 minutes |  |
|  | AC-17(3) | 1 |  |
|  | AC-22(d) | 180 days |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [AU](https://nvd.nist.gov/800-53/Rev4/family/AUDIT%20AND%20ACCOUNTABILITY) | Audit and Accountability | AU-1, AU-2(3), AU-3(1), AU-4, AU-5, AU-6(1)(3), AU-7(1), AU-8(1), AU-9(4) | None |
|  | AU-1 | Annually |  |
|  | AU-2(3) | Annually - Auditable Events are in Appendix A. |  |
|  | AU-4(1) | 30 Days or when File System is Full |  |
|  | AU-6(a) | Continuous with SIEM (Splunk) as defined in the SIEM. |  |
|  | AU-8(b) | 30 Seconds |  |
|  | Top of Form  **AU-8 (1)(a)**  Bottom of Form | 60 seconds with GMT |  |
|  | Top of Form  **AU-8 (1)(b)**  Bottom of Form | 1 Second |  |
|  | AU-9(2) | 30 Days or when File System is Full |  |
|  | AU-11 | Minimum of 2 Years or as mandated by federal or state regulation. FTI = 7 Years |  |
|  | **AU-12(3)** | Logical Audit Trail within 5 seconds |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [AT](https://nvd.nist.gov/800-53/Rev4/family/AWARENESS%20AND%20TRAINING) | Awareness and Training | AT-1, AT-2(1), AT-3, AT-4 | None |
|  | AT-1 | Annual review and updates |  |
|  | AT-2 | Annual review and with significant updates if advised |  |
|  | AT-3 | Annual or as changes occur |  |
|  | AU-4 | 5 Year Minimum |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**CM**](https://nvd.nist.gov/800-53/Rev4/family/Configuration%20Management) | Configuration Management | CM-1, CM-2(1)(3)(7),CM-3(2), CM-4,CM-5, CM-6, CM-7(1)(2)(4), CM-8(1)(3)(5), CM-9, CM-10, CM-11 | CM-3(1), CM-3(4), CM-3(6), CM-8(2) |
|  | CM-5(2) | Monthly |  |
|  | CM-5(5) | Quarterly |  |
|  | CM-7(1) | BI-Annual |  |
|  | CM-7(4) | BI-Annual |  |
|  | CM-8(3) | Antivirus & Malware Protection Software |  |
|  | CM-11 | Annually |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**CP**](https://nvd.nist.gov/800-53/Rev4/family/Contingency%20Planning) | Contingency Planning | CP-1, CP-2(1)(3)(8), CP-3, CP-4(1), CP-6(1)(3), CP-7(1)(2)(3), CP-8(1)(2), CP-9(1), CP-10(2) | None |
|  | CP-1 | Annual |  |
|  | CP-1 | Annual |  |
|  | CP-2 | 3 Years |  |
|  | CP-3 | 5 Years or with significant changes |  |
|  | CP-4 | 5 Years or with significant changes |  |
|  | CP-7 | 5 Years or with significant changes |  |
|  | CP-9 | Annual |  |
|  | CP-9 | Daily |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**IA**](https://nvd.nist.gov/800-53/Rev4/family/Identification%20and%20Authentication) | Identification and Authentication | IA-1, IA-2(1)(2)(3)(8)(11)(12), IA-3, IA-4, IA-5(1)(2)(3)(11), IA-6, IA-7, IA-8(1)(2)(3)(4) | None |
|  | IA | Annual |  |
|  | IA-4 | 10 years |  |
|  | IA-4 | 180 days |  |
|  | IA-5(1b) | 4 |  |
|  | IA-5(1d) | 1 day and 90 days |  |
|  | IA-5(1e) | 15 |  |
|  | IA-5(11) | 256 bit |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected**  Bottom of Form |
| [**IR**](https://nvd.nist.gov/800-53/Rev4/family/Incident%20Response) | Incident Response | IR-1, IR-2, IR-3(2), IR-4(1), IR-5, IR-6(1), IR-7(1), IR-8 | None |
|  | IR-1 & IR-8 | Annual |  |
|  | IR-2 | 30 days and annual thereafter |  |
|  | IR-3 | Annual |  |
|  | IR-6 | 48 hours |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**MA**](https://nvd.nist.gov/800-53/Rev4/family/Maintenance) | Maintenance | MA-1, MA-2, MA-3(1)(2), MA-4(2), MA-5, MA-6 | None |
|  | MA-1 | Annual |  |
|  |  | 14 days |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**MP**](https://nvd.nist.gov/800-53/Rev4/family/Media%20Protection) | Media Protection | MP-1, MP-2, MP-3, MP-4, MP-5(4), MP-6, MP-7(1) | None |
|  | MP-1 | Annual |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**PS**](https://nvd.nist.gov/800-53/Rev4/family/Personnel%20Security) | Personnel Security | PS-1, PS-2, PS-3, PS-5, PS-6, PS-7, PS-8 | None |
|  | PS-1 | Annual |  |
|  | PS-2© | 30 days |  |
|  | PS-4(a) | 1 day |  |
|  | PS-4(f) | 48 Hours |  |
|  | PS-5(a) | 48 hours |  |
|  | PS-5(d) | 48 Hours |  |
|  | PS-6(2) | Annual |  |
|  | PS-6(d) | 5 Working Days |  |
|  | PS-7(d) | 48 Hours |  |
|  | PS-8(b) | 24 hours |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**PE**](https://nvd.nist.gov/800-53/Rev4/family/Physical%20and%20Environmental%20Protection) | Physical Environmental Protection | PE-1, PE-2, PE-3, PE-4, PE-5, PE-6(1), PE-8, PE-9, PE-10, PE-11, PE-12, PE-13(3), PE-14, PE-15, PE-16, PE-17 | None |
|  | PE-1 | Annual |  |
|  | PE-2 | Quarterly |  |
|  | PE-3(f) | Year |  |
|  | PE-3(g) | 90 Days |  |
|  | PE-6(b) | 30 days |  |
|  | PE-8(a,b) | 180 days and Every 30 days |  |
|  | PE-9 | Unshielded Twisted-Pair n For less than 3 kVA: 50 mm (2 in) for pathways and 50 mm (2 in) for spaces n For > 3 < 6 kVA: 1.5 m (5 ft) for pathways and 3 m (10 ft) for spaces n For > 6 kVA: 3 m (10 ft) for pathways and 6 m (20 ft) for spaces Screened and Shielded Cables n For less than 3 kVA: 0 mm (0 in) for pathways and 0 mm (0 in) for spaces n For > 3 < 6 kVA: 0.6 m (2 ft) for pathways and 0.6 m (2 ft) for spaces n For > 6 kVA: 0.9 m (3 ft) for pathways and 0.9 m (3 ft) for spaces |  |
|  | PE-10 | Plain line of sight from access point |  |
|  | PE-14 | Continuously |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**PL**](https://nvd.nist.gov/800-53/Rev4/family/Planning) | Planning | PL-1, PL-2(3), PL-4(1), PL-8 | None |
|  |  | Annual |  |
|  |  | Annual |  |
|  |  | Annual |  |
|  |  | Annual |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**PM**](https://nvd.nist.gov/800-53/Rev4/family/Program%20Management) | Program Management | Variables Reserved for Revision 5 Implementation | None |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**RA**](https://nvd.nist.gov/800-53/Rev4/family/Risk%20Assessment) | Risk Assessment | RA-1, RA-2, **RA-3**, RA-5(1)(2)(5) | None |
|  | RA-1 (b1,2) | Annual |  |
|  | RA-3 [e] | Annual |  |
|  | RA-5 | Daily |  |
|  | RA-5(d) | Critical within 15 days, High within 30 days, Medium within 60 days, All others within 90 Days |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**CA**](https://nvd.nist.gov/800-53/Rev4/family/Security%20Assessment%20and%20Authorization) | Security Assessment, Authorization, and Monitoring | CA-1, CA-2(1), CA-3(5), CA-5, CA-6, CA-7(1), CA-9 | CA-2(3), CA-3(3), CA-3(4), CA-6, CA-7, CA-8(1), CA-9(1) |
|  | CA-1 | Annual |  |
|  | CA-2(2) | 3 Years |  |
|  |  | 3 Years |  |
|  | CA-3 | 3 Years |  |
|  | CA3(5) | Deny All |  |
|  | CA6 [c] | 3 Years |  |
|  | CA7 | 3 Years |  |
|  | CA-7 | Annual |  |
|  | CA-8 | 2 years |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**SC**](https://nvd.nist.gov/800-53/Rev4/family/System%20and%20Communications%20Protection) | System and Communications Protection | SC-1, SC-2, SC-4, SC-5, SC-7(3)(4)(5)(7), SC-8(1), SC-10, SC-12, SC-13, SC-15, SC-17, SC-18, SC-19, SC-20, SC-21, SC-22, SC-23, SC-28, SC-39 | None |
|  |
|  | SC-1 | Annual |  |
|  | SC-7 (4)[e] | Annual |  |
|  | SC-10 | 30 minutes |  |
|  | SI-7(1) | At Boot with installed Antivirus |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**SI**](https://nvd.nist.gov/800-53/Rev4/family/System%20and%20Information%20Integrity) | System and Information Integrity | SI-1, SI-2(2), SI-3(1)(2), SI-4(2)(4)(5), SI-5, SI-7(1)(7), SI-8(1)(2), SI-10, SI-11, SI-12, SI-16 | None |
|  | SI-1 | Annual |  |
|  | SI-1 | 30 days |  |
|  | SI-2(2) | Nessus, Acunetix |  |
|  | SI-3 | as the files are downloaded |  |
|  | SI-4(4) | IPS Monitored |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**SA**](https://nvd.nist.gov/800-53/Rev4/family/System%20and%20Services%20Acquisition) | System and Services Acquisition | SA-1, SA-2, SA-3, SA-4(1)(2)(9)(10), SA-5, SA-8, SA-9(2), SA-10, SA-11 | None |
|
|  | SA-1 | Annual |  |
|  |  |  |  |
| [**Privacy Controls NIST 800-53 R4 – Appendix J**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | | | |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**AP**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | Authority and Purpose | AP-1, AP-2 | None |
|  | AP-1 (Added) | Annual |  |
|  | No variables |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**AR**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | Accountability Audit & Risk Management | AR-1, AR-2, AR-3, AR-4, AR-5, AR-6, AR-7, AR-8 | None |
|  | AR-1 | Annual |  |
|  | AR-4 | Annual |  |
|  | AR-5 | Annual |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**DI**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | Data Quality and Integrity | DI, DI-1, DI-2 | None |
|  | DI-1 | Minimum Annual |  |
|  | DI-1 | Minimum Annual |  |
|  |  |  |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**DM**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | Data Minimization | DM, DM-1, DM-2, DM-3 | None |
|  | DM (Added) | Annual |  |
|  | DM-1 | Annual |  |
|  | DM-2 | As directed by business need or by law |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**IP**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | Individual Participation | IP-1, IP-2, IP-3, IP-4 | None |
|  | IP (Added) | Annual |  |
|  | IP-4 | 48 Hours |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**SE**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | Security and Privacy | SE-1, SE-2 | None |
|  | SE- Added | Annual |  |
|  | SE-1 | 3 Years, 3 years |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**TR**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | Transparency | TR-1, 2 & 3 | None |
|  | TR (Added) | Annual |  |
|  |  |  |  |
|  |  |  |  |
| **FAMILY** | **Control Name** | **Moderate Baseline** | **Optional Selected** |
| [**UL**](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) | Use limitation | UL-1, UL-2 | None |
|  | UL (Added) | Annual |  |
|  |  |  |  |

### **INFORMATION SECURITY POLICY**

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

### 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.

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

### 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.

### 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.

### Protected Health Information (PHI): “Individually identifiable health information” basically becomes “protected health information” when it is communicated, written or printed on paper, or stored or sent in digital files. There are some exceptions for education and employment records, and for records of people dead for more than fifty years, but in general most health information needs to be treated like PHI if it identifies specific people.

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

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

### 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.

### 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.

### 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.

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

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

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

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

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

### Elevated Privileges: Privileges that allow you to perform configuration changes or other advanced functions on an information system that ordinary users are not authorized to perform. Additionally, the account may have access to large amounts of sensitive information. Examples include but are not limited to install software, make a change to a database, change an application, change a website, change a computer policy, log onto a server or network device, create users/grant access to a system.

### 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.

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

### **Policy Exceptions**

### The initial exceptions noted within each section of this policy are officially approved through this policy approval and its approval authority. Future exceptions may be approved and updated to this policy which will represent their formal approval.

## AU- Access Control Policies

# 6.800.01 AC - Information Security Access Controls Policy

### **Purpose, Scope & Intent**

### The purpose of the Information Security Access Controls Policy is to ensure that only authorized users access the agency’s assets and resources. The intent is to communicate the policy to employees and external partner resources. The scope of the policy covers all physical and electronic access to the agencies resources.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### **Identification and Authentication**

### The <Your Agency Name Here> requires that information system access and physical access will be granted to users only after sufficient research is done for the user’s background and financial history check depending on the position being filled. The user must be uniquely identified within the information systems and must provide an acceptable form of authentication to be allowed to use any information system that houses privileged information. Users must provide proper identification and have the approved authorization to enter certain work areas.

# The use of authorization, identification and authentication controls ensures that only known users make use of the information system.

# Prior to being granted access to an information system, users must be provided with formal authorization by an appropriate official (i.e., the owner of the information system, the data owner or their designated custodian of the data housed within the information system or a designee of these individuals).

# This authorization will be based on definitive and verifiable identification of the user. Further, this authorization will be logged by the authorizing official and shared with systems and user management areas of the <Your Agency Name Here> . As each agency/organization is the owner of their data, they will be accountable for their data and their designated end users that access and use the system.

# Once a system Identity is created, it will use the systems authentication and authorization system to facilitate access.

# Once authorization has been granted, the user will be provided with a unique information system identifier. Examples of identifiers include user ids and smart cards. This identifier will be delivered to the authorized user in such a manner as to ensure that it is received only by the authorized user.

# Additionally, the user will be provided with a unique information system authenticator that is tied to the assigned identifier. Examples of authenticators include passwords, tokens and certificates. This authenticator will also be delivered to the authorized user in such a manner as to ensure that it is received only by the authorized user. To minimize risk, identifiers and authenticators for both critical and non-critical information systems must not be provided together. In circumstances where authentication must be cryptographically protected, the solution that provides this functionality must meet the minimum specifications of [FIPS 140-2](https://www.bing.com/search?q=fips%20140-2%20%2B%20.gov&qs=n&form=QBRE&sp=-1&pq=fips%20140-2%20%2B%20.gov&sc=8-16&sk=&cvid=CAE766FC876A4A33B740926B2798A874).

# Should an information system user’s account be disabled for any reason (see the Account Management section) the user’s identifier and authenticator will also be disabled, where applicable.

# Physical access to work areas must also be controlled by an Identification and Authorization mechanism. This access control not only protects information systems but also protects employee safety and other types of information. Access to work areas must be approved by managers and individuals must have a business reason for access.

# **Passwords**

# Passwords form the primary means of authentication. To ensure that passwords present as much security as possible, the following restrictions apply to them:

# Passwords must be constructed according to set requirements as established in the Access Control Procedures.

# Passwords will have both minimum and maximum lifespan.

# Passwords may not be reused for a set number of generations.

# Passwords may not be displayed while they are being entered.

# Password should not be transmitted in clear text.

# Passwords are to be individually owned and kept confidential – they are not to be shared.

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

# 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

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

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

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

# Passwords shall be significantly different from the past ten (15) passwords.

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

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

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

# 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.

# 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

# **Information system accounts**

# <Your Agency Name Here> requires that all information system accounts be actively managed by appropriate administrative staff. Active management includes the acts of establishing, activating, modifying, disabling and removing accounts from information systems.

# Information system accounts are the only legitimate method by which <Your Agency Name Here> information systems may be accessed.

# Information system accounts are to be constructed such that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. Further, accounts shall be created such that no-one account can authorize, perform, review and audit a single transaction to eliminate conflicts of interest.

# Information system accounts are to be reviewed to identify accounts with inappropriate privileges (either too high or too low) on at least an annual basis. Should information system accounts be discovered with inappropriate privileges those privileges will be manually reset to the established level.

# Information systems accounts are to be reviewed to identify inactive accounts. Should information system accounts that are associated with an employee or third party be discovered that have been inactive for a period of 180 days, it will be manually disabled. Inactive accounts that are not associated with an employee or third party but are associated with a system process (such as inter-system information transfer) that has been explicitly logged will not be disabled but will be reviewed on an annual basis. Inactive accounts that are not associated with employees, third parties, or system processes (including those that have not been explicitly logged) will be manually disabled.

# Login attempts to information systems will be restricted such that after a set number of 3 failed attempts within a 10 minute period of time, they will be locked out. Account lockout will remain in effect until unlocked by an administrator.

# **Session Management**

# The <Your Agency Name Here> requires that all communications sessions with information systems be both authenticated and actively managed by administrative staff. Active management includes the acts of monitoring, suspending, disabling and terminating communications to and from information systems. Communications between components of information systems or between information systems themselves involve the transmission of information making that information susceptible to attack. Without session management, the potential exists that communications can be established or used illegitimately thereby exposing <Your Agency Name Here> information to an increased likelihood of loss or corruption.

# All <Your Agency Name Here> information systems will display a system use notification that indicates that the user is accessing a <Your Agency Name Here> information system; that system usage is monitored, recorded and subject to audit; that unauthorized use is prohibited and subject to punitive action; that use of the information system implies consent to these controls. The system use notification will also indicate appropriate security and privacy notices. Finally, this notification will be displayed until the user acknowledges it prior to completing authenticated system access.

# Remote access to information systems will be strictly controlled. These controls include previous authorization of remote access privileges and the use of encrypted communications sessions. Further, all sessions must be actively monitored and must pass through managed access points. Finally, remote access is only to be used to execute privileged functions where sufficient rationale can be provided and such access will be preapproved and documented. Refer to the remote access policy and controls for additional information.

# All <Your Agency Name Here> information systems shall impose restrictions on open sessions that are inactive for 30 minutes. If the open session is established internally, the session will be locked until the session is re-authenticated. If the open session is established remotely the session will be terminated. These restrictions apply only to user accounts and not to system accounts used for inter-system communications. All <Your Agency Name Here> information systems shall positively and definitively identify and authenticate devices that participate in inter-system communications prior to establishing a network connection. Appropriate authentication methods include the use of shared known information (such as MAC or TCP/IP addresses) or a defined authentication solution (such as 802.11x, EAP or Radius).

# Information systems external to the control of the <Your Agency Name Here> may not establish communication or access <Your Agency Name Here> information systems unless the security controls of the third-party information system can be verified to meet the requirements of the <Your Agency Name Here> . Additionally, connection agreements must be in place with the third-party host of the external information system and all communications will be both encrypted and actively monitored. Further, all such remote access to <Your Agency Name Here> information systems must pass through defined and controlled access points. Finally, information systems external to the control of the <Your Agency Name Here> shall not be used for systems administration or other privileged functions without compelling reasons (such as during contingency operations) that have been documented and accepted by <Your Agency Name Here> .

# **Access Revocation**

# Access to both information systems and physical access will be revoked under any of several circumstances.

# Employee Termination – Information system and building access will be disabled upon termination of employee

# Managers/ HR are to notify IS Security immediately upon the termination of an employee

# Manager must also collect employee ID/ door badge immediately.

# Employee Disciplinary Action – Information system and building access may be revoked if an employee is facing disciplinary action

# The manager at their discretion may suspend access;

# During the course of a security investigation

# Restrict need to know (i.e. no longer needed to perform job)

# May disable for account Inactivity

# Additional controls outside the NIST 800-53 R4 will be listed if applicable.

# <Your Agency Name Here> shall document and adhere to change control processes when making changes to production systems.

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

# <Your Agency Name Here> shall maintain a change log for information systems containing Restricted-Use information. 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

# **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

# **Current Exceptions**

# Wipe Mobile Communication and Information Devices after ten consecutive, unsuccessful device logon attempts. After implementation of a complete MDM this will be possible.

# AC - Visitors Policy

### **Purpose, Scope & Intent**

# The Visitors Policy purpose is to direct enforcement of the controls for non-employee visits to agency facilities. The intent is to safeguard the agencies employees and resources and its scope applies to all facilities.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy All Victors**

# Visitors should sign in at the front door and show some form of identification.

# Visitors will receive passes and return them to front door once the visit is over.

# Employees must always tend to their visitors while they are inside our premises.

# Our [internet usage](https://resources.workable.com/workplace-visitor-policy-template), data protection and confidentiality policies temporarily cover our visitors while they are on company premises. They must not misuse our internet connection, disclose confidential information or take photographs of restricted areas. If they don’t conform, they may be escorted out or face prosecution if appropriate.

# Visitors are allowed during working hours. After-hours visitors must have written authorization from management.

# Personal visitors in the workplace; employees may not allow access to our buildings to unauthorized personal visitors. Exceptions on a case-by-case basis can be requested and approved by your manager. Employees may bring visitors to company events or after obtaining authorization from [HR/ Security Officer/ Facility Manager.] To avoid confusion or misunderstanding, authorization should be in writing. [HR/ Security Officer/ Facility Manager] may also give verbal authorization, when appropriate, but must also inform reception and security guards.

# Common areas, like lobbies, may be open to visitors. We advise our employees to only permit visitors in those areas for a short time and for specific reasons. Employees are responsible for accompanying any of their underage visitors at all times.

# **Contractors and service vendors**

# Contractors, suppliers and service vendors, like IT technicians and plumbers, can enter our premises only to complete their job duties. The Facility Manager is responsible for providing contractors and vendors with badges and for instructing them to wear those badges at all times on our premises.

# **Other kinds of visitors**

# Our company may occasionally accept the following types of visitors:

# Students

# Investors

# Customers

# Job candidates

# Business partners

# Those visitors should receive written authorization from HR or management before entering our premises. They should always be accompanied by an employee while on company property.

# **Solicitation**

# In accordance with our [non-solicitation policy](https://resources.workable.com/solicitation-company-policy), visitors must not try to proselytize employees, gather donations or request participation in activities while on our premises. Any visitors who violate this policy may be escorted out.

# **Deliveries**

# Anyone who delivers orders, mail or packages for employees should remain at the building’s reception area. The Facility Manager is responsible for notifying the employee who expects the delivery. If that employee is unable to receive their order, Facility Manager may accept the order on the employee’s behalf upon request.

# The Facility Manager must sign for and disseminate all business orders and mail.

# Large deliveries (e.g. supplies) should be delivered to designated spaces (e.g. warehouses.) The Facility Manager should check appropriate documents, like bills of lading, before allowing access to delivery vehicles.

# **Dangerous or restricted areas**

# Employees may not bring or accept visitors in areas where there are dangerous machines or chemicals, confidential records or sensitive equipment.

# Representatives of regulatory bodies and stakeholders (e.g. investors) may be exempted, if they have received official authorization from [HR/ Security Officer/ Office manager.] In these cases, employees should provide visitors with the necessary badges and protective equipment to enter premises when needed.

# **Unauthorized visitors**

# Security staff who spot unauthorized visitors may ask them to leave. Visitors who misbehave (e.g. engage in hate speech, cause disruption or steal property) will be asked to leave and prosecuted if appropriate.

# Employees who spot unauthorized visitors may refer them to [security/facility manager.]

# **VISITOR PROCEDURE**

# **Physical Access Controls for Entry into Agency Facilities**

# Any person(s) granted access to <Your Agency Name Here> for permanent work duties must pass a KBI criminal background check, or be escorted by someone who has.

# Electronic Key card access is required for any IT staff who have been granted permission to access to the building on a regular reoccurring bass.

# Access logs for all visitor access to the facilities are kept by the <Your Agency Name Here> office Manager.

# Once inside, <Your Agency Name Here> equipment is additionally protected by a numeric keypad lock.

# Network and other application and systems access requires a background check,and completed NDA and approval by the Agency Secretary of Commerce.

# Physical Access Controls for the Landon State Office Building Production Data Center

# Any person(s) granted access to a State of Kansas data center must pass a KBI criminal background check or be escorted by someone who has.

# Electronic Key card access is required for any IT staff who have been granted permission to access to the data center.

# Access logs for all visitor access to the data center are kept by the State of Kansas.

# Once inside the data center, <Your Agency Name Here> equipment is additionally protected by a caged infrastructure area requiring physical key access.

# Key access to the server racks is also required.

# The data center is monitored by CCTV cameras managed by the Office of Information Technology Services (OITS).

# Physical Access Controls for the **Disaster Recovery Center**

# Any person(s) granted access to <Your Agency Name Here> ’s disaster recovery data center must have approval from the Secretary of Commerce.

# To gain entry into the building, individuals must either ring a buzzer or call the Datacenter Network Operations Center (NOC) helpdesk. The NOC helpdesk will ascertain whether said individuals are on the access approval list and, if so, allow physical access to the building.

# Once permitted access inside, individuals must provide their driver’s license and have it scanned in order to create a temporary key badge.

# Biometric hand scanners are used to gain entry into the data center itself.

# Access Entry logs are kept by the Datacenter NOC.

# Datacenter NOC personnel will unlock and lock <Your Agency Name Here> server racks as needed.

# The data center is monitored by CCTV cameras managed by the Monitored by the NOC.

# **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

# **Current Exceptions**

# Background Checks have not been instituted yet.

# AC - Digital Certificate Management Policy

### **Purpose, Scope & Intent**

### The purpose of this policy is to identify the appropriate use and implementation of digital certificates at <YOUR AGENCY NAME HERE> , in support of <Your Agency Name Here> ’s Minimum Network Connectivity Requirements.

### Digital certificates ("certificates") are used to confirm identity, secure communications between parties, and ensure integrity of transmissions. The use of certificates is one method of encrypting restricted data while in transit over the network. This policy applies to digital certificates used in <Your Agency Name Here> communications to secure data in transit.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> with restricted sensitive information that is transmitted or stored to and from and or on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <Your Agency Name Here> .

### It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices for Data Encryption, data communication, transfer and storage.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **POLICY**

### This section outlines the acceptable use of digital certificates at <YOUR AGENCY NAME HERE> . Additional strength, configuration, validity, and Certificate Authority (CA) requirements are included in FIPS-140-2 and FIPS 200.

### Requests for certificates that do not meet the requirements in this policy may be denied. Certificates that do not meet the requirements in this policy may be revoked.

### Acceptable Use Requirements

### A. Wildcard, SAN, and UCC Certificates

### No one may own or manage a wildcard certificate for the domain (\*.<YOUR AGENCY NAME HERE> .net)

### Wildcard certificates are not permitted on sub-domains that handle restricted data

### <Your Agency Name Here> may obtain wildcard certificates for their sub-domain(s) and servers (e.g. \*.mydomain.thedomainhere.net) after appropriate consultation on risk with System Stewards/Data Owners and Service Providers

### <Your Agency Name Here> should obtain Subject Alternative Name (SAN) or Unified Communication Certificate (UCC) (aka Multi-Domain certificates) instead of wildcard certificates, where feasible

### Requirements for management of private keys are listed under "Private Key Management".

### **Self-Signed Certificates**

### Self-signed certificates are not allowed on systems with restricted data

### Self-signed certificates are only allowed on systems without restricted data under the following circumstances:

### Technical, contractual, or vendor requirements preclude using a certificate issued by a trusted Certificate Authority

### Temporary development on a host that is not customer-facing

### Factory-installed certificates on devices that are not customer-facing

### **Private Key Management**

### Private keys must be protected to the same standard as the Data Encryption Policy requires for the data the key is protecting.

### When an employee who has access to private keys protecting restricted data leaves the organization, private keys and associated certificates must be replaced

### Units may not install the same private key on multiple hosts, except for clustered and load-balanced services. Where certificates are shared or span across multiple hosts, the security requirements of the most sensitive member prevail.

### The same private key and certificate should only be used with one set of restricted data (e.g., payment data, student data, health records, etc.), to reduce the risk of compromise across multiple data sets

### **Renewing, Replacing and Revoking Certificates**

### Certificates must be renewed or replaced before expiration

### Certificates must be revoked when one or more of the following occur:

### A private key has been compromised

### The service is being retired or decommissioned

### When the private key is no longer in use

### **ITS Certificate Service**

### All <Your Agency Name Here> -related certificates must be issued by the State’s Certificate Management Team or a State approved certificate vendor. . Additional approval is required for certificates issued outside of this service.

### **CONDITIONS REQUIRING ADDITIONAL APPROVAL**

### Uses of digital certificates that do not comply with this policy must be approved and documented by the Information Security Officer (ISO). The ISO may require additional review in order to evaluate requests and/or implementation of compensating controls.

### **Audit Controls and Management**

### On-demand documented procedures and evidence of practice should be in place for this operational policy as part of <Your Agency Name Here> operational methodology.

### <Your Agency Name Here> shall maintain an inventory certificates and validate implementation of them at least annually.

### Documentation shall exist for certificate management procedures.

### Exception logs exist and can be produced for those resources that are excluded from this policy.

### **Exceptions**

### Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### Current Exceptions

### NONE

# AC - Data Leakage & Loss Prevention Policy

### **Purpose, Scope & intent**

### This policy establishes the Agency Data Leakage & Loss Prevention Policy, which refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data securely, transparently and with respect towards individual rights.

### The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <YOUR AGENCY NAME HERE> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IT resources (including e-mail, messages and files) is the property of <YOUR AGENCY NAME HERE> .

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### It is the intention of this policy to establish a policy that employees of our agency and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also included. Generally, the scope of our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

### **Policy**

### As part of our agency operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

### Our agency collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

### Our data will be:

* Accurate and kept up-to-date
* Collected fairly and for lawful purposes only
* Processed by the company within its legal and moral boundaries
* Protected against any unauthorized or illegal access by internal or external parties

### Our data will not be:

* Communicated informally
* Stored for more than a specified amount of time
* Transferred to organizations, states or countries that do not have adequate data protection policies
* Distributed to any party other than the ones agreed upon by the data’s owner (exempting legitimate requests from law enforcement authorities)

### In addition to ways of handling the data the Agency has direct obligations towards people to whom the data belongs. Specifically, we must:

* Let people know which of their data is collected
* Inform people how their data is protected
* Inform people about how we’ll process their data
* Inform people about who has access to their information
* Have provisions in cases of lost, corrupted or compromised data
* Allow people to request that we modify, erase, reduce or correct data contained in our databases

### **Added Controls**

### To exercise data protection, we’re committed to:

* Restrict and monitor access to sensitive data
* Develop transparent data collection procedures
* Train employees in online privacy and security measures
* Build secure networks to protect online data from cyberattacks
* Establish clear procedures for reporting privacy breaches or data misuse
* Include contract clauses or communicate statements on how we handle data.
* Deploy Data Leakage & Loss Protection Controls as appropriate for our computing infrastructure.

### **Exceptions**

### Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### NONE

# AC - Remote Access

### **Purpose, Scope & intent**

### The purpose of this policy is to define standards for connecting to <Your Agency Name Here> 's network from an external agency device. These standards are designed to minimize the potential exposure to <Your Agency Name Here> from damages which may result from unauthorized use of <Your Agency Name Here> resources. Damages include the loss of sensitive or agency confidential data, intellectual property, damage to public image, damage to critical <Your Agency Name Here> internal systems, etc.

### The <Your Agency Name Here> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a system and information integrity capability throughout <Your Agency Name Here> and its bureaus to help the organization implement security best practices with regard to system configuration, security, and error handling.

### This policy applies to all <Your Agency Name Here> employees, contractors, vendors and agents with a business need to connect to the <Your Agency Name Here> network remotely. This policy applies to remote access connections used to do work on behalf of <Your Agency Name Here>, including reading or sending email and viewing intranet web resources.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### It is the responsibility of <Your Agency Name Here> employees and contractors with remote access privileges to <Your Agency Name Here> 's network to ensure that their remote access connection is given the same consideration as the user's on-site connection <Your Agency Name Here>.

### Secure remote access must be strictly controlled and enforced.

### Remote access must be requested through the <Your Agency Name Here> Infrastructure Management Team.

### Remote access to the <Your Agency Name Here> network can only be done with agency/state owned equipment.

### All remote access to the <Your Agency Name Here> network must go through Two-Factor Authentication.

### Remote access to the KD network will be conducted through agency approved software or solutions.

### At no time may <Your Agency Name Here> employees, contractors, vendors and agents connect to the <Your Agency Name Here> network from outside of the United States.

### At no time should any <Your Agency Name Here> employee provide their login or password to anyone, not even family members.

### <Your Agency Name Here> employees and contractors with remote access privileges must ensure that their <Your Agency Name Here> -owned computer or workstation, which is remotely connected to <Your Agency Name Here> 's agency network, is not connected to any other network at the same time.

### All hosts that are connected to <Your Agency Name Here> internal networks via remote access technologies must use the most up-to-date anti-virus software. Third party connections must comply with this requirement as well.

### **Exceptions**

### Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### 2 Factor Authentication for Remote Access is not in place for all employees.

# AC - Mobile Device Policy

### **Purpose, Scope & intent**

### To inform <Your Agency Name Here> employees of the policies regarding use of <Your Agency Name Here> issued mobile devices.

### This is to include Smart Phones, Tablets, Laptops, Portable Storage, mobile hot spots (JetPacks, MIFI, and cellular hot spots), and any future technology that would fall into the category of mobile device or mobile storage.

### This document is to be made available to all employees of <Your Agency Name Here>. Individuals issued such devices, as mentioned above, must read and provide a signed acknowledgement of this policy upon receiving the device. The acknowledgment form is located at the back of this policy manual.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### <Your Agency Name Here> does not authorize the use of personal mobile devices to support <Your Agency Name Here> business functions

### All mobile devices are subject to <Your Agency Name Here> ’s acceptable use policy. Any violations or misuse may result in disciplinary actions.

### Special care must be taken to prevent loss or theft of devices

### Do not leave unattended

### Do not place in the open

### Secure the device when not in use

### Individuals may be responsible for replacement of lost, stolen, or damaged devices

### If a device is lost or stolen, notify the <Your Agency Name Here> Help Desk immediately

### The help desk is available 24X7

### All devices must be password or pin protected

### All devices must be encrypted

### All mobile devices are the property of <Your Agency Name Here> and must be returned upon request or when no longer needed to fulfill job responsibilities.

### **Smart Phones**

### Smart Phones are to be used for <Your Agency Name Here> business:

### Calls and text message usage is monitored by budget and auditors

### Individuals may be responsible for reimbursement of costs related to inappropriate use

### Smart Phones are to be treated in the same manner as <Your Agency Name Here> Computers

### Do not install unapproved software/APPS

### If there is an APP you need, send a request to your phone administrator

### <Your Agency Name Here> IS will install any needed apps

### All Smart Phones must be encrypted

### All Smart Phones will be monitored and controlled by a Mobile Device Management Suite at all times.

### This security suite provides Anti-Virus, monitors compliance and allows administrative controls of the phone such as resetting the pin or wiping the device

### Any tampering with these control mechanisms can be monitored and will be considered a security violation subject to disciplinary action up to and including dismissal

### All Smart Phones will require a Password for access

### Do not use patterns

### Do not use us a PIN number

### **Tablets**

### Tablets must be encrypted

### Tablets are to be treated in the same manner as <Your Agency Name Here> Computers

### Do not install unapproved software/APPS

### If there is an APP you need, send a request to your phone administrator and <Your Agency Name Here> IS will install any needed apps

### **Laptops Computers**

### Laptop Computers must be encrypted

### Laptops are to be treated in the same manner as <Your Agency Name Here> Desktop Computers

### **Mobile Hot Spots (Mifi, JetPacks, Cellphones with Hot Spot Feature)**

### Mobile hot spots are to be used by only <Your Agency Name Here> personnel

### Do not share the connection with any other individuals

### This is for business Use (Bandwidth becomes throttled after a data limit)

### Do not connect to both a mobile Hot Spot and the physical <Your Agency Name Here> network at the same time. This poses a major security risk that could result in significant damage to the network

### **Portable Storage (USB Flash Drives, USB Hard Drives, and other portable media)**

### **Portable hard drives**

### Personal portable hard drives are strictly prohibited unless specifically approved by IS Security

### Only <Your Agency Name Here> issued portable hard drives may be used in <Your Agency Name Here> systems

### All portable hard drives must be encrypted

### **USB Flash Drives**

### Only authorized users may use flash drives in <Your Agency Name Here> systems

### Only <Your Agency Name Here> issued flash drives may be used in <Your Agency Name Here> systems

### All flash must be encrypted

### **Other Portable Media (i.e. Data CD/DVD)**

### Contents must be encrypted

### CD/DVD Blu-Ray Burners are prohibited unless specifically approved by IS Security

### **USAGE:**

### **Operating a Vehicle**

### Whether conducting State business or personal business, use of a smart-device or cellular phone, either hands on or hands off, while operating a state vehicle is prohibited. Use of any cellular phone or any smart device, either hands on or hands off, to conduct State business while operating a privately-owned vehicle is also prohibited.

### Prohibitions include receiving or placing calls, sending text messages, surfing the Internet, responding to email, checking for phone messages, or any other purpose related to your employment; the business; our customers; our vendors; volunteer activities, meetings, or civic responsibilities performed for or attended in the name of the company; or any other company or personally related activities not named here while driving. Further, if state or local laws are more restrictive, the employee must follow the appropriate law.

### **Employee Responsibility**

### Mobile devices either owned by the organization or personally owned and used to conduct business must be used appropriately, responsibly, and ethically. The following must be observed:

### Organization issued mobile devices are the property of the organization and must be treated, used, and safeguarded as such. If an employee damages or loses an organization issued mobile device, the employee must notify <Your Agency Name Here> Infrastructure Management Team (IMT) agency services immediately to have the device de-activated. Charges associated with using a mobile device issued by the organization for personal communications, including text messages, email and voice calling, counts towards the monthly consumption limit. Therefore, personal use of a mobile device issued by the organization should be minimized.

### No employee is to use organization-owned devices for the purpose of illegal transactions, harassment, or obscene behavior, in accordance with other existing employee policies.

### Devices must be kept up to date with manufacturer or network provided patches. At a minimum, patches should be checked for weekly and applied at least once a month.

### Mobile devices must not be loaned to, or used by, others.

### Commonly referred to as “jail-breaking”, devices must not be modified in a way that circumvents the vendor’s limitations imposed upon users or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

### Devices must not be connected to a non-state PC which does not have up-to-date and enabled antimalware protection, and which does not comply with State policy.

### If employee suspects that unauthorized access to State data has taken place via a mobile device, the incident must be reported immediately to technical support.

### Employees must report all lost or stolen Smart Devices authorized to connect to State resources or authorized to conduct State business, to the <Your Agency Name Here> IMT agency IT services group immediately.

### **Device Support**

### <Your Agency Name Here> IMT services are only responsible for fixing or repairing broken or malfunctioning smart devices if the device was issued by the State. If the smart device is personally owned, it is the responsibility of the employee.

### Not all smart device operating systems are supported on organizational security controls, therefore only the following operating systems shall be approved for use:

### Android

### Apple IOS

### Microsoft

### **Secure Operation**

### In order to join a personal or organization owned smart device to the organizational resources the agency specific <Your Agency Name Here> Smart Device Activation Request must be signed and authorized. The <Your Agency Name Here> Smart Device Activation Request must be reviewed and renewed annually. Once approved, the <Your Agency Name Here> chosen security policy / configuration shall be applied to the device.

### **Personal Smart Device Use for Business**

### Before requesting authorization to join personal devices to organization resources, employees must be aware that once joined, organization security controls can render smart devices inoperable for various security events or on demand (such as in the case of a lost smart device). In addition, the security controls addressed previously in paragraph 4. “Secure Operation” must also be applied.

### **Liability**

### <Your Agency Name Here> will not assume liability for personal wireless devices. All Employees that are eligible for an organization issued mobile device will receive an organization issued device.

### <Your Agency Name Here> will not assume liability for early termination of employee paid personal wireless devices.

### <Your Agency Name Here> will not assume liability for accidental deletion of data from government issued or employee paid personal wireless devices.

### <Your Agency Name Here> will not transfer any personal phone numbers to organization issued mobile devices unless not transferring a personal phone number would negatively impact the organization.

### <Your Agency Name Here> will not assume liability for data usage charges on personal devices except in the instance of your agency approving your position for a business use reimbursement.

### <Your Agency Name Here> will not collect ANY personal device or application data from a device that is not provided by your agency.

### **Exceptions**

Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

**Current Exceptions**

### Currently <Your Agency Name Here> does not have a full MDM system deployed. The agency partially implements one with Microsoft OS365 MDM and is reviewing options for a full feature MDM solution.

# AC - Telecommute Policy

### **Purpose, Scope & Intent**

### To provide guidelines for designating employees to work at alternate work locations for all or part of their workweek in order to promote general work efficiencies, ensure security, and provide <Your Agency Name Here> with the flexibility to address specific needs.

### This policy covers all telecommuters, this includes all employees, contractors or remote agents working on behalf of the agency. It also covers all computing assets and controls used to facilitate the telecommuting arrangement.

### It is the intention of this policy to establish a system and information integrity capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, security, and error handling.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### This policy establishes a system and information integrity capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to telecommuting.

### Telecommuting is a work arrangement in which supervisors direct or permit employees to perform their usual job duties away from their central workplace in accordance with a telecommuting agreement. <Your Agency Name Here> reserves the right to modify this policy at any time, for any reason deemed appropriate by the Secretary of Commerce.

### **Definitions**

### Alternate Work Location: A workstation in or at the employee's residence or other approved remote location and not an <Your Agency Name Here> leased or owned facility, and which is assigned pursuant to this policy by way of a telecommuting agreement.

### Information Technology (IT) Resources: These include, but are not limited to, software, hardware, fax machines, cell phones, E-mail, Internet, PKI digital certificates, computer printers, voice mail, application development, and maintenance.

### Central Workplace: The <Your Agency Name Here> main office location where the <Your Agency Name Here> employee would be assigned and/or where the direct supervisor is located.

### Secretary: Shall mean the Secretary of XXXXXXXX or his/her designee.

### Telecommuter: An employee who works away from his/her central workplace part of the work week, either at his/her residence or at another approved remote work location.

### Telecommuting Agreement: The written agreement signed by the employee that details the terms and conditions of an employee's work away from his or her central workplace.

### Telecommuter Work Schedule: The employee’s hours of work in the central workplace and in alternate work locations.

### **Controls**

### Information Technology Resources-General

### <Your Agency Name Here> IT Resources will not be issued to the approved telecommuter until the <Your Agency Name Here> telecommuting agreement is signed and forwarded to The <Your Agency Name Here> Human Resources for filing. The agreement shall be signed by the telecommuter, his/her supervisor, his/her department manager, the <Your Agency Name Here> Secretary of XXXXXXXX.

### IT Resources, data, supplies and furniture, provided by <Your Agency Name Here> for use at the alternate work location are for purposes of conducting official <Your Agency Name Here> business and may not be used by any non-<Your Agency Name Here> employees. Limited personal use by the <Your Agency Name Here> employee is allowed.

### The telecommuter shall be expected to adhere to the <Your Agency Name Here> Acceptable Use Policy all other <Your Agency Name Here> policies.

### <Your Agency Name Here> Infrastructure Management Team (IMT) is responsible for determining the necessary computing infrastructure to be an approved telecommuter and then installed.

### Employees shall not install on <Your Agency Name Here> IT Resources, attach to <Your Agency Name Here> IT Resources, nor use any hardware on <Your Agency Name Here> IT Resources, whether wired or wireless, which <Your Agency Name Here> does not supply or paid.

### Employees are responsible for protecting <Your Agency Name Here> IT Resources from theft, damage, and unauthorized use.

### <Your Agency Name Here> IS staff is responsible for transporting and installing all <Your Agency Name Here> IT Resources, unless they have granted permission to other <Your Agency Name Here> associates.

### <Your Agency Name Here> IT staff must inventory and maintain a record of <Your Agency Name Here> IT Resources, and other property located in the alternate work location.

### <Your Agency Name Here> IT Resources used in the normal course of employment will be maintained, serviced, and repaired by <Your Agency Name Here> IS staff, unless they have granted permission to other <Your Agency Name Here> associates.

### The Telecommuter will return <Your Agency Name Here> IT Resources, supplies, documents and other information or property to the central workplace prior to termination of telecommuting or employment.

### IT Resources Maintenance and Support

### The Telecommuter will be responsible for promptly notifying his/her supervisor of any equipment malfunction or failure that prevents the telecommuter from performing assigned tasks. The telecommuter may be assigned to perform different tasks, or to report to another work location depending on current work assignments.

### <Your Agency Name Here> IS staff is responsible for testing, maintenance, and repair of the equipment and upgrades of software when telecommuters use <Your Agency Name Here> IT Resources, unless permission is granted to other <Your Agency Name Here> associates.

### <Your Agency Name Here> IS staff will provide technical support for telecommuters utilizing <Your Agency Name Here> IT Resources.

### <Your Agency Name Here> IS staff will not support employee-owned IT Resources.

### With advance notice and upon proper identification, the telecommuter shall allow authorized <Your Agency Name Here> staff access to the alternate work location, during normal business hours (defined as 8:00 a.m. CST to 5:00 p.m. CST, Monday through Friday) or during any hours during which the telecommuter is on duty as defined by the telecommuting agreement, for the purpose of repair and/or maintenance of <Your Agency Name Here> IT Resources, if necessary.

### **Data**

### The telecommuter must provide security for the data and information that is transported to and from their alternate work location. Simple measures such as removing hard drives, thumb drives, and documents that contain sensitive data from desk areas and placing them in secure storage may prevent a major and potentially costly security breach or loss of information for <Your Agency Name Here> and the State of Kansas.

### The telecommuter is responsible for protecting the privacy and confidentiality of data at the alternate work location and must take the necessary precautions, so authorized <Your Agency Name Here> employees are the only individuals with access to said data.

### All data classified as State or Federal Confidential shall be encrypted during transmission and when at rest on storage devices by using <Your Agency Name Here> supplied encryption software.

### **General Employment**

### Nothing herein or in any telecommuting agreement shall alter or change the employment relationship between the employee and <Your Agency Name Here> , including, but not limited to, the employee's duty to comply with all federal and state employment laws, standards of conduct and all <Your Agency Name Here> policies, procedures and applicable regulations.

### All state employment benefits such as salary, leave time, and state sponsored insurance shall not be affected by the telecommuting agreement.

### Telecommuting does not change an employee's exempt or non-exempt status as determined under the Fair Labor Standards Act (FLSA). Supervisory approval must be obtained before taking leave, rearranging work time, or, in the case of non-exempt employees, before performing work that would result in overtime hours.

### If during the course of the telecommuter's employment <Your Agency Name Here>, he/she should be relieved from duty with or without pay or be suspended from his/her employment with <Your Agency Name Here>, the telecommuter shall not perform any <Your Agency Name Here> work or duties at the alternate work location during such period of relief from duty or suspension, and that such period of time shall not be considered as hours worked for pay or benefits purposes.

### **Workers' Compensation**

### An employee is covered by the State of Kansas Workers' Compensation laws while in telecommuting status, if such law is applicable.

### Approval of the telecommuting agreement may be subject to said alternate work location being inspected for safety hazards by authorized <Your Agency Name Here> Staff or a <Your Agency Name Here> Designated Representative. Said inspection shall be limited to only that portion of the residence designated as the alternate work location. By entering into a telecommuting agreement, the telecommuter consents to such an inspection and agrees to correct any hazards identified during the inspection at the telecommuter's expense. The Secretary may waive such inspection at his/her discretion.

### Any injury that occurs within the course and scope of employment must be reported to the telecommuter’s supervisor immediately, using the agency's standard injury reporting process.

### For purposes of Workers’ Compensation coverage, the employee's designated alternate work location is considered an extension of <Your Agency Name Here> work space only during scheduled telecommuting working hours.

### **Work Schedule/Performance**

### The work schedule, including normal work day hours and core hours, will be determined by the telecommuter’s supervisor and the telecommuter according to agency policy as outlined in the telecommuter work schedule included in the telecommuting agreement. The supervisor and the telecommuter shall determine the number of days per work week/work period that the employee will telecommute.

### Core hours are those hours during which the telecommuter will be available to communicate with the supervisor, co-workers, or the public by telephone, e-mail, fax, etc.

### Unless other arrangements are made, the telecommuter shall be expected to attend all assigned and requested office meetings at the central workplace. The telecommuter shall not conduct any work-related meetings at the alternate work location, unless approved by the direct supervisor.

### The telecommuter who is scheduled to be working at his/her home on a day that is declared to be a weather emergency at the central workplace is expected to work at home as scheduled unless power outages or other unique weather-related circumstances preclude such work.

### The telecommuter will provide regular reports required by the supervisor to help judge work performance. A decline in work performance, as determined by the supervisor, may result in termination of the telecommuting agreement.

### The telecommuter is to perform only official duties and not conduct personal business while on work status at the alternate work location. Personal business includes but is not limited to caring for dependents or making home repairs.

### With advance notice and upon proper identification, the telecommuter shall allow authorized <Your Agency Name Here> staff access to the alternate work location, during normal business hours (defined as 8:00 a.m. CST to 5:00 p.m. CST, Monday through Friday) or during any hours during which the telecommuter is on duty as defined by the telecommuting agreement.

### **Location and Travel**

### The telecommuter may work from his/her alternate work location that has been approved by his/her direct supervisor.

### Travel to and from the central workplace shall be considered compensable hours.

### Mileage between the alternate work location and the telecommuter's central workplace shall be considered commute mileage and not subject to reimbursement.

### **Liability**

### The telecommuter's designated alternate work location is considered an extension of <Your Agency Name Here> during the agreed upon working hours.

### The designated alternate work location must accommodate any equipment to be used in work performed and the telecommuter must protect the work space from hazards and dangers that could affect themselves or the equipment, such as faulty or ungrounded electrical outlets. An <Your Agency Name Here> representative may make visits to the alternate work location, with advanced notice, to ensure that the equipment and work area are safe and free from hazards.

### <Your Agency Name Here> IS responsible for insuring <Your Agency Name Here> equipment. The telecommuter has the same responsibility for taking appropriate steps to minimize damage to <Your Agency Name Here> property at the alternate work location as at the central workplace.

### The telecommuter shall not place or cause to be placed any signage, or otherwise hold said alternate work location out to the public as an office of <Your Agency Name Here>, nor shall said alternate work location be open to the public except as may be allowed under terms and conditions specifically set forth in the telecommuting agreement.

### **Telecommuter Workspace Responsibility**

### The telecommuter shall be responsible for establishing and maintaining adequate work space at their alternate work location.

### The telecommuter shall designate an alternate work location, subject to the approval of the supervisor and authorized <Your Agency Name Here> staff.

### The telecommuter shall be responsible for obtaining written approval from any owner or landlord for the installation of any improvements, remodeling or electrical modifications at such alternate work location.

### The telecommuter shall be responsible for absorbing all costs related to permanent improvements in such an alternate work location such as remodeling or electrical modifications.

### The agency will not be responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities, insurance, taxes) whatsoever associated with use of the telecommuter's residence or personal computer equipment. The agency will reimburse the telecommuter for expenses previously authorized by telecommuter's supervisor and incurred while conducting business for the agency.

### **Supplies and Expenses**

### The supervisor and the telecommuter will determine necessary work-related supplies to be supplied by <Your Agency Name Here> and the best method for their distribution. Out-of-pocket expenses for supplies regularly available at <Your Agency Name Here> Central Supply will not be reimbursed unless previously approved by <Your Agency Name Here>.

### **PROTECTION OF PII AT ALTERNATIVE WORKSITES**

### All communication from alternative worksite to <Your Agency Name Here> core network will be conducted over [FIPS 140-2](https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf) compliant encryption mechanisms.

### All remote access to <Your Agency Name Here> core network must be conducted on <Your Agency Name Here> issued equipment

### All remote access will be subjected to second factor authentication

### **ACTION**

### Each telecommuter is required to read, complete, and sign the telecommuting agreement.

### Human Resources will ensure that each telecommuter will receive a copy of this policy and the completed and signed telecommuting agreement.

### Any questions regarding this policy should be directed to the telecommuter’s supervisor, <Your Agency Name Here> Human Resources or IT as appropriate.

### All work done on <Your Agency Name Here> IT resources are subject to monitoring as if the telecommuter were in the workplace.

### Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

### **Exceptions**

### Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX review and approval.

### Current Exceptions

### Currently, employees working remotely utilize at times personal printers, keyboards and mice. The Agency is looking at possible solutions for this.

# AC - Acceptable Use of Information Technology Resources

### **Purpose, Scope & Intent**

# The for purpose of the Acceptable Use of Information Technology Resources is to ensure employee and contract resources understand the terms for acceptable and unacceptable use of agency and state electronics & computing resources. The intent is to ensure all employees review and agree to the terms. The scope applies to all internal users of these Information Technology Resources. The following Policies should be reviewed prior to completing the review and signoff on this policy.

# <Your Agency Name Here> Data Classification Policy

# <Your Agency Name Here> Remote Access Policy

# <Your Agency Name Here> Telecommuting Policy – as applicable

# <Your Agency Name Here> Mobile Device Policy & User Agreement – as applicable

# All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

# **Policy**

* + - * 1. Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the State's IT resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals.
        2. Periodic monitoring, including recording of phones and computer screen activity, will be conducted of systems used, including but not limited to all computer files and all forms of electronic communication, including email, text messaging, instant messaging, VOIP telephones, cell/smart phones, computer systems and other electronic records. In addition to the notice provided in this policy, users may also be notified about this monitoring and reminded that unauthorized use of the State's IT resources is not permissible through the use of warning banner text at system entry points where users initially sign on. The user is responsible for reading and adhering to the warning.
        3. <Your Agency Name Here> may impose restrictions, at the discretion of their executive management, on the use of a particular information technology resource. For example, <Your Agency Name Here> may block access to certain websites or services not serving legitimate business purposes or may restrict users’ ability to attach devices to the <Your Agency Name Here> information technology resources (e.g., personal USB drives, iPods).
        4. Users accessing internal <Your Agency Name Here> applications and information technology resources may not use personal devices. See <Your Agency Name Here> Remote Access Policy.

# **Acceptable Use**

* + - * 1. All uses of information technology resources must comply with State policies, standards, procedures, and guidelines, as well as any applicable Federal, State and local laws, including copyright laws and licensing agreements.
        2. Consistent with the foregoing, acceptable use of information technology resources encompasses the following duties:
        3. Protection of all forms of confidential information from unauthorized use or disclosure;
        4. Observing authorized levels of access and utilizing only approved information technology devices or services; and
        5. Immediately reporting suspected computer security incidents to the appropriate manager and the Information Security Officer (ISO)/designated security representative.

# **Unacceptable Use**

* + - * 1. The following list is not intended to be exhaustive, rather, it is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during the course of their authorized job responsibilities, after approval from <Your Agency Name Here> leadership, in consultation with the <Your Agency Name Here> IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).
        2. Unacceptable use includes the following:
        3. Disclosure of confidential information as designated in K.S.A. 75-3520, K.S.A. 75-5133, K.S.A. 75-5133(b), K.S.A. 79-3234, K.S.A. 79-1119 , K.S.A. 79-3303, K.S.A. 79-3420, K.S.A. 79-3499, K.S.A. 79-34,113, K.S.A. 79-3614, K.S.A. 74-2012, all requirements of the IRS Publication 1075 in regards to Federal Tax Information (FTI), or Personal Individual Information (PII) of any kind (e.g., taxpayer information, driver’s license information, etc.) via electronic communication systems is strictly prohibited unless required in the lawful performance of assigned duties;
        4. Accessing records from any <Your Agency Name Here> information system which you are not authorized to access;
        5. Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, hate-filled harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, political, offensive jokes, offensive images, or intentionally false or inaccurate information. The determination of the Secretary of XXXXXXXX as to what constitutes as offensive is final.
        6. Remove or make changes to any state equipment.  Notify PC Support who is responsible to install, change, or remove state IT equipment;
        7. Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (the state has recognized the inherent risk in using commercial email services as email is often used to distribute malware);
        8. Usage of the internet and social media; do not access online games, including games found on social websites., do not use streaming media unless its use is business related, to access the Internet, use only software that is part of the IT standard software suite or that has been approved by IT. This software must incorporate all vendor-provided security patches required by IT. If using blogs or websites, do not discuss state or agency business matters or publish material that shows the state or agency in a negative light. The user will not blog or make personal posts on state time or resources. Do not make data available on the states or agencies websites without ensuring that the material is accessible to only those groups and individuals who are authorized.
        9. Make sure content on all state and agency websites is business related and has been approved by the department publishing the information. Do not make offensive or harassing material available through the state or agency websites.
        10. Purporting to represent <Your Agency Name Here> or the State of Kansas in matters unrelated to official authorized job duties or responsibilities;
        11. Remove or make changes to any <Your Agency Name Here> equipment. Notify PC Support who is responsible to install, change, or remove <Your Agency Name Here> IT equipment;
        12. Connecting unapproved devices to the <Your Agency Name Here> or the State network or any State information technology resource;
        13. Connecting State information technology resources to unauthorized networks;
        14. Connecting to any wireless network while physically connected to a State wired network;
        15. Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review;
        16. Sharing your password to any IT System with anyone, this includes <Your Agency Name Here> IT;
        17. Using State information technology resources to circulate unauthorized solicitations or advertisements for non-State purposes including religious, political, for profit, or not-for-profit entities. Officially sanctioned state charities are exempted from this policy;
        18. Providing unauthorized third parties, including family and friends, access to <Your Agency Name Here> or State IT resources or facilities;
        19. Using State information technology resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
        20. Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using State information technology resources;
        21. Using <Your Agency Name Here> resources to cause or result in a disruption in day to day agency and State of Kansas operations;
        22. Using <Your Agency Name Here> resources to cause a disruption to any external entity; and
        23. Tampering, disengaging or otherwise circumventing <Your Agency Name Here> or third-party IT security controls.

# **Occasional and Incidental Personal Use**

* + - * 1. Occasional and incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with this policy and the requirements of, is limited in amount and duration, and does not impede the ability of the individual or other users to fulfill the <Your Agency Name Here> ’s responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. <Your Agency Name Here> may revoke or limit this privilege at any time.
        2. For example, users may make occasional and incidental personal use of information technology resources for light and appropriate internet browsing.
        3. Your judgment regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in the exercise of good judgment by providing the above guidelines. If you are unclear about the acceptable "personal" use of a state-provided resource, seek authorization from your immediate supervisor.

# **Individual Accountability**

* + - * 1. Individual accountability is required when accessing all IT resources. Each individual is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure, including sharing. Credentials must be treated as confidential information, and must not be disclosed or shared.

# **Restrictions on Off-Site Transmission and Storage of Information**

* + - * 1. Users must not transmit non-public, confidential, sensitive, or restricted <Your Agency Name Here> information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct State business unless explicitly authorized. Users must not store non-public, confidential, sensitive or restricted <Your Agency Name Here> information on a non-State issued device, or with a third-party file storage. Users must refrain from placing confidential, sensitive, or restricted <Your Agency Name Here> information on Office 365 OneDrive for Business.
        2. Devices that contain <Your Agency Name Here> information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

# **User Responsibility for Information Technology Equipment**

* + - * 1. Users are routinely assigned or given access to information technology equipment in connection with their official duties.  This equipment belongs to the State and must be immediately returned upon request or at the time an employee is separated from <Your Agency Name Here> service.  Users may be financially responsible for the value of equipment assigned to their care if it is not returned to <Your Agency Name Here> . Should State IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident.  Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment.  <Your Agency Name Here> has the discretion to not issue or re-issue information technology devices and equipment to users who repeatedly lose or damage State IT equipment.

### **Exceptions**

### Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

## Current Exceptions

* + - * 1. NONE

# AU - Information Security Audit and Accountability

### **Purpose, Scope & Intent**

### This policy establishes the Enterprise Information Security and Audit Policy to ensure the security of <Your Agency Name Here> systems, information and services by granting professional rights and responsibilities to Information Services staff and defining basic guidelines for system auditing.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <Your Agency Name Here> .

### It is the intention of this policy to establish an information security and audit standard throughout <Your Agency Name Here> to help the organization implement security best practices with regard to access to <Your Agency Name Here> IS systems.

# All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### Information Security is the process that ensures the availability, integrity and confidentiality of IT systems, information and services. Effective IT Security is essential to ensure that the <Your Agency Name Here> meets its obligations for security, privacy and preservation of sensitive information.

### <Your Agency Name Here> recognizes that all Authorized Users should be made aware of their responsibilities for IT Security and for the need for effective IT Security Management, as outlined in <Your Agency Name Here> ’s Acceptable Use Policy.

### **Professional Rights and Responsibilities of Information Services Staff**

### In the course of completing their professional duties, <Your Agency Name Here> information Services staff;

### Require a level of access to computing and communications infrastructure, information and support systems, account details and data on the <Your Agency Name Here> network, computers and storage commensurate with their professional duties in the workplace;

### By virtue of their level of access to computing and communications infrastructure, information and support systems, have the ability to view account details and data on the <Your Agency Name Here> network, computers and storage;

### Are charged with the logical and physical security of account details and data on the <Your Agency Name Here> network, computers and storage and also with dealing with security incidents or requests for information by approval of the CISO, CIO, the Secretary, or the Governor.

### Will not view account details and data on the <Your Agency Name Here> network, computers and storage unless it is required as need-to-know with approval; or in the course of undertaking their professional duties in the workplace.

### **Right to Monitor**

### As owner, the <Your Agency Name Here> has the right to monitor the use of its IT systems and services.

### Monitoring will be undertaken routinely by Information Services staff in the normal course of their duties to maintain technical security and operational efficiency of the systems and services.

### Any extraordinary action taken by Information Services staff to monitor systems and services must be authorized by their direct line manager and the Chief Information Officer.

### Monitoring will occur in cases of suspected breach of law, condition of employment, or <Your Agency Name Here> policy

### In these cases, inspection of personal information will be undertaken in accordance with requirements of Privacy policy and law and only after approval of the Agency Secretary of XXXXXXXX or Information Security Officer.

### Electronic data, information and material created by Authorized Users will be treated as confidential during monitoring and all monitoring references destroyed if determined not relevant.

### Access to such information will be strictly on a need-to-know basis for technical or administrative purposes.

### Except for normal administrative processes, the accounts, files, stored data and network data including e-mail messages created by Authorized Users, are held secure from intervention by other users.

### Information Services staff may disconnect equipment from the <Your Agency Name Here> network when monitoring detects a breach in IT security or a breach of the law or <Your Agency Name Here> policy.

### Such disconnection would normally be preceded by notice to the relevant Authorized User and their supervisor, but in an emergency, notice will follow disconnection.

### In the event of a breach in the law or <Your Agency Name Here> policy, disciplinary proceedings, where appropriate, will be instituted in accordance with State of Kansas Statutes and regulations, or according to relevant contracts and/or workplace agreements.

### **Log retention**

### Wherever possible, security logs will be retained for an appropriate length of time based on the data/system sensitivity, legal requirements, and division Secretary of XXXXXXXX ’s direction.

### **Auditing Levels**

### Levels and complexity of auditing frameworks will be based on system criticality, vulnerability and risk of disclosure. All systems containing Identifiable Information (PII) will be treated with the utmost in scrutiny.

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

### The following data points shall be logged:

### Event date

### Event time

### Event source

### Event description

### 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.

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

### 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.

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

### **Exceptions**

### Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

# None

# AT – Awareness and Training

### **Purpose, Scope & Intent**

### This policy establishes the Information Security Awareness and Training Policy ensures the agency develops, documents and maintains a training awareness policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The agency shall conduct security awareness training and policy attestation annually.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> (<Your Agency Name Here> ). Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <Your Agency Name Here> . All users <Your Agency Name Here> employees, contractors, vendors or others) of IS resources are responsible for adhering to this policy.

### It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, data communication and transfer.

# All users <Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### This policy specifies the information security awareness program to train and motivate all workers of their information security duties and obligations.

### In order to protect information assets all workers must be informed about relevant, current information security matters and through training and awareness provide them the necessary knowledge of security concepts to successful work and operate within the agency.

### <Your Agency Name Here> shall retain a form of acknowledgement of training completion.

### <Your Agency Name Here> shall review their security awareness training materials at least annually or more frequently as needed.

### 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

### <Your Agency Name Here> will ensure that within 30 days it will have facilitated awareness and any new training required to support significant policy and or procedure changes.

## Exceptions

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

## Current Exceptions

### **NONE**

# CM- Configuration Management Policy

### **Purpose, Scope & Intent**

### The purpose of this policy is to protect the integrity of system configurations for <Your Agency Name Here> systems. The enterprise-wide CM approach aligns to the CM process already published and aligned to the National Institute of Standards and Technology (NIST) SP 800-128. Implementation considerations for enterprise CM that are based on the four stages are listed below.

### The scope of the policy applies to all IS System Resources.

### The intent of this policy is to give guidance to all agents of <Your Agency Name Here> to protect the citizens of Kansas from having their information accidentally disclosed when <Your Agency Name Here> disposes of media.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### <Your Agency Name Here> has chosen to adopt the Configurations Management principles established in NIST SP 800-53 “Controls,” as the official policy for this domain. Each <Your Agency Name Here> business System is then bound to this policy and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

### <Your Agency Name Here> must meet or exceed all State and Federal regulatory policies and procedures which affect Configuration and Change Management processes to be implemented on <Your Agency Name Here> information technology assets.

### Planning Configuration Management (CM) will:

### Define how the types of assets and Configuration Items (CI’s) are to be selected, grouped, classified, and defined by the appropriate characteristics; to ensure they are manageable and traceable throughout the lifecycle.

### Define the approach to identification, uniquely naming and labeling all the assets or service components of interest across the service lifecycle; and define the relationships between them.

### Define the roles and responsibilities of the owner or custodian of the configuration item type at each stage of its lifecycle (e.g., the service owner for a service package or release at each stage of the service lifecycle).

### Identifying and Implementing Configurations: An enterprise secure baseline will address configuration settings, software loads, patch levels, documentation, how 9 information is physically or logically arranged, and how various security controls are implemented. Automation will enable tool interoperability and baseline configuration uniformity across the information system.

### Controlling Configuration Changes: Changes to CIs will be approved prior to their implementation, with the exception of an emergency change. Access restrictions will be established, including:

### Access controls

### Process automation

### Abstract layers

### Change windows

### Verification and audit activities to limit unauthorized and/or undocumented changes to the information systems.

### Monitoring: Enterprise monitoring activities will validate the information system assets to adhere to organizational policies, procedures, and the approved secure baseline configuration.

### <Your Agency Name Here> must document, implement, and maintain Configuration and Change Management processes. These processes must include the following:

### Documenting and maintaining the configuration baseline(s) applicable to the deployed system;

### Effectively managing and tracking all system configuration and associated document changes, as well as the integrity, availability and maintainability of the system;

### Effectively planning to ensure the ability to reverse a deployment or implementation; and

### Effectively tracking all system changes made, including installation of patches, to hardware, software, firmware, and documentation, through development, approval, testing, and controlled implementation of changes delivered into production environments.

### Configuration and Change Management processes must incorporate applicable industry best practices, which support optimum production system availability and effective system management. These practices include:

### Using standardized documented methods, processes, and procedures;

### Effectively tracking and communicating all system changes made to hardware, software, firmware, and documentation, through planning, approving, notifying, developing, testing, scheduling, and managing the implementation of changes;

### Making effective risk-based decisions to maintain each system’s mission capability, authorized security posture and minimized risk; and

### Maximizing <Your Agency Name Here> resources.

### Program Offices and Regions that maintain a network infrastructure connected to the <Your Agency Name Here> network must establish Change Advisory Boards (CAB) as appropriate to ensure changes to the <Your Agency Name Here> Infrastructure are reviewed and processed in accordance with established <Your Agency Name Here> Configuration and Change Management processes and procedures.

### Each Program Office and Region must utilize a Configuration Management Database (CMDB) or manual equivalent that contains and tracks relevant information about configuration items, their attributes, baselines, documentation, changes, and relationships. Existing or new systems may fulfill this requirement. <Your Agency Name Here> , IT will establish an IT-wide standard to which all existing and new CMDBs may conform.

### Any changes to portions of <Your Agency Name Here> ’s IT environments that might impact network security, performance, or operations must be recorded in a central tracking application and database. These include changes to portions of <Your Agency Name Here> ’s IT environments, including network, LAN, WAN, telecommunications, mainframe, hosting, and servers. IT has provided specific guidance as to the types of changes that must be recorded. For more information refer to the Agency Change Management Process and Procedures, under Related Documents.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# CP- Contingency Planning Policy V1.0

### **Purpose, Scope & Intent**

### The purpose of this is to define the Contingency Planning Policy. These Policies are designed to minimize the potential exposure to <Your Agency Name Here> from damages which may result from unforeseen incidents or disasters that may occur. Damages include the loss of sensitive or agency confidential data, intellectual property, damage to public image, damage to critical <Your Agency Name Here> internal systems, or loss of agency facilities.

### The scope of the policy applies to all IS System Resources.

### It is the intention of this policy to establish a system and information integrity capability throughout <Your Agency Name Here> to help the organization implement security best practices regarding system configuration, security, and error handling.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### <Your Agency Name Here> has chosen to adopt the Contingency Planning principles established in NIST SP 800-34 “Contingency Planning Guide for Federal Information Systems,” as the official policy for this domain. The NIST CP family of controls outline the Contingency Planning standards that constitute <Your Agency Name Here> policy. Each <Your Agency Name Here> business System is then bound to this policy and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

### The agency will complete a Business Impact Assessment, facilitate Contingency Planning and Disaster Recovery Planning. The processes will follow a formal documented process and be aligned with the agency risk management program.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# IR - Incident Response

### **Purpose, Scope & Intent**

### It is the responsibility of all State of Kansas employees to report suspected privacy and security concerns, threats, issues, incidents, or violations as quickly as possible. The ultimate goal, regardless of category of incident, is the safety of people, protection of state assets and data, containment of damage, apprehension of the perpetrator, and restoration of service.

### Security Incident: Any perceived situation that places people or state assets, including computer data, at risk.

### Data Breach/Compromise: An incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an unauthorized individual.

### Personally Identifiable Information (PII): Any information that can be used to distinguish or trace an individual’s identity, such as their name, Social Security Number, state identification number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, medical, educational, financial, and employment information, etc. PII also includes other information that, alone or in combination, would allow a reasonable person in the community, who does not have personal knowledge of the relevant circumstance, to identify the person with reasonable certainty.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> (<Your Agency Name Here> ). Any restricted information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <Your Agency Name Here> . All users (<Your Agency Name Here> employees, contractors, vendors or others) of IS resources are responsible for adhering to this policy.

### It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, data communication and transfer.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Additional Responsibility Definition**

### This section will provide summary of the additional roles and responsibilities. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Roles** | Incident Response Team | Data Owner | System Owner | System Admin | Information Security Officer |
| **Tasks** |  |  |  |  |  |
| Require service provider to document and implement threat detection practices |  |  | I |  | A/R |
| Require service provider to document and implement monitoring and logging |  |  | I |  | A/R |
| Document incident handling practices | R |  | I |  | A |
| Incident response training | R |  | I |  | A |
| Incident response testing | R |  | I |  | A |
| Implement an incident handling capability | R |  | I |  | A |
| Identify and document all locations containing personal and medical information | I | R |  | R | A |
| Redact personal and medical information | I | R |  | R | A |
| Provide appropriate notice to affected individuals upon the unauthorized release of personal or medical information | I | R |  |  | A |
| Incident reporting | I |  |  | R | A |
| Incident response assistance | R |  |  |  | A |
| Develop and incident response plan | R |  |  |  | A |

### **Policy**

### <Your Agency Name Here> shall adopt a defined incident response plan which addresses the following stages:

### **Preparation**

### <Your Agency Name Here> shall appoint team members to incident response roles with the following skills:

* + Communication and coordination
  + Legal counsel
  + Network analysis
  + System administration
  + Security analysis
  + Communication (left off here)
    - * 1. Security analysis <Your Agency Name Here> 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.
        2. <Your Agency Name Here> shall provide annual IR training for all IR team members.
        3. <Your Agency Name Here> shall annually conduct IR operations testing using classroom, tabletop exercises or live incidents.
        4. <Your Agency Name Here> shall conduct an exercise recreating a significant incident scenario that requires the full-scale execution of IR operations once every five (5) years.
      1. **Detection** 
         1. <Your Agency Name Here> 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.

### **Analysis**

### <Your Agency Name Here> shall have dedicated tools and a process to conduct incident analysis, such as:

* Dedicated portable workstations
* Evidence collection tools and procedures
* Forensics analysis software and procedures
  + - 1. **Containment** 
         1. <Your Agency Name Here> shall have procedures to isolate and mitigate identified threats to prevent further impact.
      2. **Communication**

<Your Agency Name Here> shall develop an incident communications plan to ensure adequate communication of an incident, is provided, in a timely basis to stakeholders.

State Any incident that is reported to a Federal Partner, other state entity, other state, or any regulatory body must be reported to the Kansas Information Security Office concurrently or no longer than a maximum of 48 hours.

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.

### **Recovery**

### <Your Agency Name Here> shall recover affected systems and system components to a pre-compromised status and return to normal operations.

### <Your Agency Name Here> 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.

### **Post-Incident Activity**

### <Your Agency Name Here> shall perform a post-incident review in order to document lessons learned and to improve information system protection in the future.

### Reviews of the policy, procedures and artifacts shall occur:

### Annually for procedures and artifacts

### Every three years for policies

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# IA -Identification and Authentication

### **Purpose, Scope & Intent**

### The purpose for this policy is to establish a standard for the creation of passwords, the protection of those passwords, and the frequency of which passwords must change.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <Your Agency Name Here> .

### It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, data communication and transfer.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### In accordance with Kansas Information Technology Security Standards 7230A, <Your Agency Name Here> maintains the following password policies.

### **Identification**

### Primary Account Creation & Identifier and Authenticator Management

### A primary ID enables agency users to access basic services. The services are to be listed on the access request form and the request is to be submitted through the manager to validate that the requested basic access follows the need to know and rule of least privilege.

### These services include, Network access that enables the user to access e-mail and public agency files. Enables access to e-mail. Enables access to all the applications on the user’s computer. May also provide access to other applications and services as applicable and defined by an organization.

### **Issuance**

### All requests for new network and system accounts (Identifiers and Authenticators) must be sent through the agency Secretary of XXXXXXXX /Secretary or their authorized proxy, the agency Infrastructure Manager and Information Security Officer.

### Only Authorized individuals can request new network or system accounts

### Authorized individuals include the supervisor, manager, or authorized contact of the individual that the account will be issued to;

### Authorized individuals cannot request accounts for themselves

### A valid use case and need to know is required for the account to be created

### Data owners at any time can deny creation of an account

### The Infrastructure Manager will review the request and make the initial approval or denial through the approved access management process.

### System Administrators will distribute identifier and authenticator through a secure means, either in person or in multiple parts electronically.

### New User Initial accounts will be sent to the Supervisor/Requestor

### Accounts for existing employees will be sent to the employee directly

### System Identifier and Authenticator will follow the following documented system requirements as closely as possible

### The <Your Agency Name Here> will maintain a list of roles\positions that will be required to provide a list of positions or roles that should have secondary accounts include but are not limited too:

* Workstation Administrators
* Network Administrators
* Server Administrators
* Database Administrators
* System Administrators
* Application Developers
* Website Administrators
* Information Security Administrator
* Information Security Analyst
* Information Security Officer/Manager
* Helpdesk staff

### Network Authenticator requirements

* Enforce password history -15 passwords remembered
* Maximum password age - 90 days
* Minimum password age - 15 days
* Minimum password length - 8 characters
* Password must meet complexity requirements

### Complex passwords must contain characters from three of the following four categories:

* Uppercase characters (ABCD……. Z)
* Lowercase characters (abcd……. z)
* Base 10 digits (Numbers 0 through 9)
* Non-alphanumeric characters: ` ~ ! @ # $ % ^ & \* ( ) \_ - + = { } [ ] \ | : ; " ' < > , . ? /

### Account Lockout Policy

* Account lockout threshold - 3 invalid logon attempts within 10 minutes
* Account lockout duration - 10 minutes or Administrator Intervention
* Reset account lockout counter after 10 minutes
* Passwords will be required to be changed after first log-on

### Use;

* Systems will not display passwords while being entered
* Systems will encrypt passwords in transit and while being stored
* Identifiers will be disabled after 90 days of Inactivity
* Management, Information Security, Data Owners, HR, Law Enforcement may request accounts to be suspended/disabled at any time

### Recovery;

* User can contact the <Your Agency Name Here> helpdesk to reset lost/compromised or damaged credentials
* If user indicates the authenticator was compromised, the helpdesk will immediately notify <Your Agency Name Here> information Security

### Retirement

* Authorized individuals will submit a request for access withdrawal through the Security Management Database upon an individual’s separation from the agency
* Security Management Database will notify the System Administrators that an individual has left the agency.
* System Administrators will retire the Identifier within the system (disable/inactivate)
* Systems should maintain a record of user Identifiers after retirement

### **Management of Identifiers**

* + - * 1. The Security Management Database in some cases will also hold a history of individuals and associated identifies Uniqueness. Each identifier is to be unique; that is, each identifier is associated with a single person or other entity.
        2. One Identifier per Individual. An individual may have no more than one ID unless they are a designated administrator where a separate ID should be created for administrative access.
        3. Non-Reassignment. Once and identifier is assigned to a particular person it is always associated with that person. It is never subsequently reassigned to identify another person or entity.
        4. Social Security Number. Social Security Numbers shall not be used to identify employees or students.

### **Authentication**

### Access to IT resources will be achieved by individual and unique logins, and will require authentication, minimally a username and password combination. Authentication credentials will not be coded into programs or queries unless they are encrypted, and only when no other reasonable options exist.

### **Authentication Methods**

### Authentication methods involve presenting both a public identifier (such as a user name or identification number) and private authentication information such as a personal identification number (PIN), password, token, or information derived from a cryptographic key.

### Authentication against the agency computing infrastructure is recommended when possible. One of the following methods must be implemented:

* Strictly controlled passwords
* Biometric identification
* Tokens in conjunction with a PIN

### **No Unencrypted Authentication**

* + - * 1. Unencrypted authentication and authorization mechanisms are only as secure as the network they use. Traffic across the network may be monitored, rendering these mechanisms vulnerable to compromise. Therefore, all agency services must use only encrypted authentication mechanisms unless otherwise authorized. In particular historically insecure services, such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

### **User Responsibilities**

### Official Actions. Use of a ID and authentication method to identify oneself to an on-line system constitutes an official identification of the user to the agency, in the same way that presenting an ID Card does. Users can be responsible for all actions taken during authenticated sessions.

### Integrity. Regardless of the authentication method used, users must use only the ID and authentication information that they have been authorized to use (i.e. a user must never identify themselves falsely as another person or entity).

### Confidentiality. Regardless of the authentication method used, users must keep authentication information confidential (i.e. a user must not knowingly or negligently make it available for use by an unauthorized person).

### Reporting Problems. Anyone suspecting that their authentication information was compromised should immediately contact the IT Help Desk.

### Security Precautions. Users are encouraged to change their password regularly (at least once every three months), to limit possible abuse of passwords that may have been compromised without the user’s knowledge. Passwords should be chosen so that they are not easily guessable (i.e. not based on the user’s name or birth date).

### Disciplinary Action. Individuals who are found to have knowingly violated one of these provisions will be subject to disciplinary action. The possible disciplinary actions for violations, which can include termination of employment will depend on the facts and circumstances of each use.

### **Authorization**

### Access to information and IT system resources will be granted on a “need to know” or “minimum necessary” basis and must be authorized by the immediate information owner. Any of the following methods are acceptable for providing access:

### Context-based access. Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external” factors might include time of day, location of users, strength of user authentication, etc.

### Role-based access. Access control model that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organizations structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges need to perform that role.

### User-based access. Security mechanism used to grant users of a system access based upon the identity of the user.

### **Identification and Authentication of Local Systems**

### This section contains recommendations and requirements for systems and services that use local identification and authentications methods rather than centrally supported methods.

### Use IDs. Systems should use assigned IDs to identify their users. This will be less confusing for users and will ease future transition to centrally supported authentication.

### Avoid Clear-Text Passwords. Systems may not transmit reusable passwords across the network unencrypted. Such passwords are vulnerable to capture and abuse.

### Support Password Quality. System should check proposed passwords and reject those that are likely to be easily guessable.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### NONE

# MA - Security Systems Maintenance Policy

### **Purpose, Scope & Intent**

### This policy establishes the Enterprise System Maintenance Policy, for managing risks from information asset maintenance and repairs through the establishment of an effective System Maintenance program. The system maintenance program helps the <Your Agency Name Here> implement security best practices with regard to enterprise system maintenance and repairs.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <YOUR AGENCY NAME HERE> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <YOUR AGENCY NAME HERE> .

### It is the intention of this policy to establish a system maintenance capability throughout <Your Agency Name Here> and its bureaus to help the organization implement security best practices with regard to enterprise system maintenance and repairs.

### All users <Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### This Policy drives assurance for the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

### System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.

### **Change Control**

### <Your Agency Name Here> shall document and adhere to change control processes when making changes to production systems.

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

### <Your Agency Name Here> shall maintain a change log for information systems containing Restricted-Use Information.

### 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

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# MP - Media Protection

### **Purpose, Scope & Intent**

### This policy establishes the Enterprise Media Protection Policy, for managing risks from media access, media storage, media transport, and media protection through the establishment of an effective Media Protection program. The media protection program helps the <Your Agency Name Here> implement security best practices with regard to enterprise media usage, storage, and disposal.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of <YOUR AGENCY NAME HERE> .

### <Your Agency Name Here> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a media protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to enterprise media usage, storage, and disposal.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### This Media Protection Policy was developed for <Your Agency Name Here> using the NIST 800-53 Controls as a reference towards ensuring secure management and handling of security media. Electronic media includes but is not limited to the following:

### Electronic media that takes advantage of electronic technology. They may include 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 most 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.

### **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.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# MP - Data Classification

### **Purpose, Scope & Intent**

### The purpose of this Policy is to establish a framework for classifying <Your Agency Name Here> data based on its level of sensitivity, value and criticality to the Agency as required by State of Kansas Information Security Policy ITEC 7230 and 7230A. Classification of data will aid in determining appropriate baseline security controls for the protection of the data. Data classification is meant to reflect the level of impact that a compromise of Confidentiality, Integrity, or Availability of data/information would have on the Agency and the Citizens of the states it supports.

### This policy applies to all information within the <Your Agency Name Here> . This includes but is not limited to an individual record, data set, entire information system, intellectual property, or business processes.

### The intent of this policy is to ensure that all data is properly identified, classified and assigned the appropriate level of security protections based on the classification.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### The policy establishes how the agencies 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 it must adhere to maintain secure and proactive management sensitive data.

### The agency will identify the sensitive data types it receives, processes, stores and transmits. All data will be classified to the following classification scheme.

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

### Private Data: Data should be classified as Private when the unauthorized disclosure, alteration or destruction of the data could result in a moderate level of harm or risk to the agency and the and the Citizens of the states it supports.

### Public Data: Data should be classified as Public when the unauthorized disclosure, alteration or destruction of the data would result in little to no harm or risk to the agency and the and the Citizens of the states it supports.

### Caveats can be applied to each classification level. A caveat will be applied to any data or information system that has special regulatory compliance and may require additional security controls beyond the standard baseline of the classification level.

### Health Insurance Portability and Accountability (HIPPA)

### Social Security Administration (SSA)

### **Calculating Classification**

### While calculating classification cannot be easily quantified, the below chart can help determine the impact of a compromise to help determine classification level. The below table is from Federal Information Processing Standards Publication 199. As the potential impact increases from Low to High, the classification should move from least restrictive to more 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. |
| **Security Levels** | **LOW** | **MODERATE** | **HIGH** |
| ***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 three categories. Any data or system that is not classified by the data owner or system owner is automatically placed at the Restricted level.

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

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

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

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

### All portable media and devices, regardless of factor, shall be encrypted

### Media containing Restricted-Use Information shall be disposed of in accordance with NIST Special Publication 800-88 Rev 1 – Guidelines for Media Sanitization.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# MP - Media Sanitization and Destruction Policy

### **Purpose, Scope & Intent**

### The purpose of this policy is to outline the proper disposal/sanitization/destruction of media (physical or electronic). These rules are in place to protect sensitive information, employees, and citizens of Kansas.

### The following Data Classification Types (Data Classification details can be found in the data classification procedures) all fall within the scope of this policy.

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

### Private Data: Data should be classified as Private when the unauthorized disclosure, alteration or destruction of the data could result in a moderate level of harm or risk to the agency and the and the Citizens of the states it supports.

### Public Data: Data should be classified as Public when the unauthorized disclosure, alteration or destruction of the data would result in little to no harm or risk to the agency and the and the Citizens of the states it supports.

### The intent of this policy is to give guidance to all agents of <Your Agency Name Here> to protect the citizens of Kansas from having their information accidentally disclosed when <Your Agency Name Here> disposes of media.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### The policy is instituted to prevent unauthorized disclosure of Agency Data:

### media leaving control of the responsible department and destined for reuse or disposal must have all Agency Data purged in a manner that renders the data unrecoverable.

### media that will be reused within the agency should likewise have all Agency Data purged to prevent unauthorized disclosure.

### media containing Agency Data authorized by the appropriate administrative head for transfer to individuals or organizations outside the agency are exempt.

### **Added Controls**

### When no longer needed, hard drives, diskettes, tape cartridges, CDs. DVDs, ribbons, hard copies, print-outs, and other items used to process, store and/or transmit restricted use and sensitive information shall be properly disposed of in accordance to this policy.

### Minimum sanitization requirements are established from (NIST-800-53R4). All <Your Agency Name Here> data is considered a Moderate Security Categorization. All contracts regarding media sanitization and disposal must include proper language from Federal requirements including but not limited to the IRS and the SSA based on the type of information being sanitized and disposed.

### Digital\Electronic Media

### All digital media will be sanitized according to NIST 800-88 guidelines.

### The approved method for Sanitization is Destruction

### Clear and Purge are NOT approved sanitization methods for <Your Agency Name Here>

### Must use Appropriate method for the storage medium as defined in NIST 800-88 Table A-1

### Physical Media (Print-outs and other physical media)

### Shredding using <Your Agency Name Here> issued cross-cut shredders

### Placed in a <Your Agency Name Here> approved shredding bin for Channel Management to collect and cross-cut shred

### Placed in a <Your Agency Name Here> approved shredding bin for a private contractor to collect and cross-cut shred on-site

### Must be witnessed by <Your Agency Name Here> staff

### <Your Agency Name Here> also follows the 800-543 R4 Controls for media Sanitization.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### Must be witnessed by <Your Agency Name Here> staff – <Your Agency Name Here> uses and Accredited Service and Accepts the Risk of not witnessing the destruction. Ticket # 27700.

# MP - Data Encryption

### **Purpose, Scope & Intent**

* + - * 1. To establish a standard to secure sensitive agency data and comply with federal and state policies.   Encrypting sensitive information helps protect against data exposure if the storage device is lost or stolen and against some types of unauthorized physical access to the device. Encrypting sensitive data in transit protects against other kinds of threats including “sniffing” and “man‐in‐the‐middle” attacks
        2. This policy also outlines the requirements for managing and protecting encryption keys. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use.
        3. The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> restricted sensitive information that is transmitted or stored to and from and or on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <YOUR AGENCY NAME HERE> . All users <Your Agency Name Here> employees, contractors, vendors or others) of IS resources are responsible for adhering to this policy.
        4. The data classification policy should be strictly adhered to and data should be first classified before applying the Encryption policy.
        5. The storage and management of encryption keys also falls within the scope of this policy. Therefore, this policy applies to all encryption keys and to the person responsible for any encryption.
        6. It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to Data Encryption, data communication, transfer and storage.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

* + - * 1. Encryption and Encryption Key Management, if not done properly, can lead to compromise and disclosure of data and private keys use to secure sensitive data and hence, compromise of the data.

### **Encryption**

* + - * 1. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information shall be used. The use of proprietary encryption algorithms are not allowed unless reviewed by qualified experts outside of the vendor in question and approved by <Your Agency Name Here> management.

### **ACCESS**

* + - * 1. <Your Agency Name Here> - TS shall ensure:
        2. Policies, procedures, scenarios, and processes must identify Confidential Information or PII that must be encrypted to protect against persons or programs that have not been granted access.
        3. <Your Agency Name Here> implements appropriate mechanisms to encrypt and decrypt Confidential Information or PII whenever deemed appropriate. Internal procedures shall specify how <Your Agency Name Here> transmits sensitive information as well as how often the information is transmitted.
        4. When encryption is needed based on data classification to protect Confidential Information or PII during transmission. Procedures shall specify the methods of encryption used to protect the transmission of Confidential Information or PII.
        5. Logical user access is managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials) when disk encryption is used rather than file or column level database encryption.

### **ENCRYPTION KEY LENGTH**

* + - * 1. <Your Agency Name Here> uses software encryption technology to protect Confidential Information or PII. To provide the highest-level security while balancing throughput and response times, encryption key lengths should use current industry standard encryption algorithms for Confidential Information or PII. See FIPS 140-2.

### **AT-REST ENCRYPTION**

* + - * 1. Hard drives that are not fully encrypted (e.g., disks that one or more un-encrypted partitions, virtual disks) but connect to encrypted USB devices, may be vulnerable to security breach from the encrypted region to the unencrypted region. Full disk encryption avoids this problem and shall be the method of choice for user devices containing Confidential Information or PII.
        2. Confidential Information or PII at rest on computer systems owned by and located within <Your Agency Name Here> controlled spaces, devices, and networks should be protected by one or more of the following mechanisms:
        3. Disk/File System Encryption (e.g. Microsoft EFS technology)
        4. Use of Virtual Private Networks (VPN’s) and Firewalls with strict access controls that authenticate the identity of those individuals accessing the Confidential Information or PII
        5. Sanitizing, redacting, and/or de-identifying the data requiring protection during storage to prevent unauthorized risk and exposure (e.g., masking or blurring PII)
        6. Supplemental compensating or complimentary security controls including complex passwords, and physical isolation/access to the data
        7. Strong cryptography on authentication credentials (i.e. passwords/phrases) shall be made unreadable during transmission and storage on all information systems
        8. Password protection to be used in combination with all controls including encryption
        9. File systems, disks, and tape drives in servers and Storage Area Network (SAN) environments are encrypted using industry standard encryption technology
        10. Computer hard drives and other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure upon return for redistribution or disposal

### **PORTABLE DEVICE ENCRYPTION**

* + - * 1. Portable devices (e.g. smart-phones, flash cards, SD cards, USB file storage) represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of Confidential Information or PII are the result of stolen or lost portable computing devices. The most reliable way to prevent exposure is to avoid storing Confidential Information or PII on these devices.
        2. As a general practice, Confidential Information or PII shall not be copied to or stored on a portable computing device or <Your Agency Name Here> owned computing device. However, in situations requiring Confidential Information or PII to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen. The following procedures shall be implemented when using portable storage:
        3. Hard drives (laptops, tablets, smartphones and personal digital assistants (PDAs)) shall be encrypted using products and/or methods approved by <YOUR AGENCY NAME HERE> . Unless otherwise approved by management, such devices shall have full disk encryption with pre-boot authentication.
        4. Devices shall not be used for the long-term storage of any Confidential Information or PII.
        5. All devices shall have proper and appropriate protection mechanisms installed including approved anti-malware/virus software, personal firewalls with unneeded services and ports turned off, and properly configured applications.
        6. Removable media including CD’s, DVD’s, USB flash drives, etc. shall not be used to store Confidential Information or PII.

### **IN-TRANSIT ENCRYPTION**

* + - * 1. In-transit encryption refers to transmission of data between end-points. The intent of these policies is to ensure that Confidential Information or PII transmitted between companies, across physical networks, or wirelessly is secured and encrypted in a fashion that protects student Confidential Information or PII from a breach. <Your Agency Name Here> or their designee shall ensure:
        2. Formal transfer policies, protocols, procedures, and controls are implemented to protect the transfer of information through the use of all types of communication and transmission facilities.
        3. Users follow <Your Agency Name Here> acceptable use policies when transmitting data and take particular care when transmitting or re-transmitting Confidential Information or PII received from non-<Your Agency Name Here> staff.
        4. Strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, etc.) are used to safeguard Confidential Information or PII during transmission over open public networks. Such controls include:
        5. Only accepting trusted keys and certificates, protocols in use only support secure versions or configurations, and encryption strength is appropriate for the encryption methodology in use.
        6. Public networks include but are not limited to the Internet, Wireless technologies, including 802.11, Bluetooth, and cellular technologies.
        7. Confidential Information or PII transmitted in e-mail messages are encrypted. Any Confidential Information or PII transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with <Your Agency Name Here> must be encrypted or transmitted through an encrypted tunnel (VPN) or point-to-point tunneling protocols (PPTP) that include current transport layer security (TLS) implementations.
        8. Wireless (Wi-Fi) transmissions used to access <Your Agency Name Here> computing devices or internal networks must be encrypted using current wireless security standard protocols (e.g. RADIUS, WPS private/public keys or other industry standard mechanisms).
        9. Encryption or an encrypted/secured channel is required when users access <Your Agency Name Here> Confidential Information or PII remotely from a shared network, including connections from a Bluetooth device to an <Your Agency Name Here> PDA or cell phone.
        10. Secure encrypted transfer of documents and Confidential Information or PII over the internet uses current secure file transfer programs such as “SFTP” (FTP over SSH) and secure copy command (SCP).
        11. All non-console administrative access such as browser/web-based management tools are encrypted using SSL based browser technologies using the most current security algorithm.
        12. <Your Agency Name Here> requires a minimum of TLS 1.2 be used for encrypting Web Traffic
        13. <Your Agency Name Here> requires a minimum of 256 Bit AES Encryption per FIPS 140-2 RSA BSAFE be used for Data at Rest Encryption (Backups)
        14. <Your Agency Name Here> requires a minimum of 256 Bit AES Encryption per FIPS 140-2 be used for Disk Encryption
        15. <Your Agency Name Here> requires that Microsoft DEP for encrypting RAM on the Servers be enabled
        16. <Your Agency Name Here> requires a minimum of Cisco AnyConnect using TLSv1.2 with AES256 cipher algorithms for remote Administrator and Developer Access
        17. <Your Agency Name Here> requires a minimum 256 Bit AES FIPS 140-2 for SSH and FTPS
        18. <Your Agency Name Here> requires a minimum 256 Bit AES FIPS 140-2 for Database Encryption
        19. The FIPS 140-2 [validated modules search](https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search) provides access to the official validation information of all cryptographic modules that have been tested and validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-2. The search results list all issued validation certificates that meet the supplied search criteria and provide a link to view more detailed information about each certificate. The Certificate Detail listing provides the detailed module information including algorithm implementation references to the [CAVP algorithm validation](https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation), Security Policies, original certificate images or reference to the consolidated validation lists, and vendor product links if provided.

### **Encryption Key Management**

* + - * 1. Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

### **Secret Key Encryption Keys**

* + - * 1. Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them.

### **Public Key Encryption Keys**

* + - * 1. Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

### **Data Transmission**

* + - * 1. All transmission of sensitive data requires the use of appropriate encryption.  Files can be encrypted before they are transmitted across the network (as an email attachment) for example.  This can be used as an alternative to encrypting the transmission channel.

### **Data Storage Media**

* + - * 1. It is prohibited to store unencrypted sensitive data on any non-network storage device or media, unless the data is encrypted and there is a written exception approved by the agency head or designee.  Prohibited storage media includes storage on desktop computers, laptop computers, PDA's, cell phones, USB drives, thumb drives, memory cards, CD's, DVD's and other USB devices (e.g. media players, cameras, etc.)

### **Additional Controls**

### **Allowed Data Encryption**

* + - * 1. Only modules tested and validated to FIPS 140-1 or FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information shall be used.
        2. Encryption technologies (applications, protocols, and algorithms) must be approved by the Agency Information Security Officer and Agency IT Director.  Other unapproved or proprietary encryption algorithms are not sufficient to meet this standard.  This includes any proprietary encryption that has not been made public and/or has not withstood public scrutiny.

### **Public Key Infrastructure (PKI) Keys**

* + - * 1. The public-private key pairs used by <Your Agency Name Here> –TS public key infrastructure (PKI) are generated on the tamper-resistant smart cards or USB tokens and issued to an individual end user. The private key associated with an end user’s identity certificate, which are only used for digital signatures, will never leave the smart card. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed for recovery purposes. Access to the private keys stored on a <Your Agency Name Here> –TS issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed. State of Kansas Certificate Policy and Certificate Practice Statement will be followed for the issuance of PKI certificates.

### **Hardware Token Storage**

* + - * 1. Hardware tokens storing encryption keys will be treated as sensitive Agency equipment. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user’s computer when not in use.

### **Personal Identification Numbers (PINs), Passwords and Passphrases**

* + - * 1. All PINs, passwords or passphrases used to protect encryption keys must meet agency complexity and length requirements.

### **Database Encryption**

* + - * 1. All keys that are used to encrypt restricted use information in a database must be managed by an approved enterprise Key Management Solution.

### **Loss and Theft**

* + - * 1. The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to Information Security

### **Key Recovery**

* + - * 1. For data of record, where the only access to it is available by decryption, copies of the keys must be burned to a labeled CD and placed in a sealed labeled envelope, or the password for approved software must be written and placed in a sealed labeled envelope.  In either case the envelope shall be presented to the ISO for inspection and the Agency Head for key recovery purposes.  Whenever a password change occurs for data of record the old key/password information must be retrieved, destroyed and replaced with the new key/password information by contacting the Agency ISO and Agency Head.  Appropriate identification will be required for all transactions.

### **Definition Sensitive Data**

* + - * 1. Sensitive data is data which, if compromised with respect to confidentiality, integrity, or availability, could adversely affect Agency interests, the conduct of agency programs, or the privacy to which individuals are entitled.  For example: Social Security numbers, driver’s license or identification card numbers, financial account numbers, and credit or debit card numbers are considered sensitive data.  Other items may also be defined as sensitive in other policies or legislation including PII, FTI, SSA, NDHD, FERPA and HIPAA for example.

### **Audit Controls and Management**

* + - * 1. On-demand documented procedures and evidence of practice should be in place for this operational policy as part of <Your Agency Name Here> operational methodology.
        2. <Your Agency Name Here> shall inventory encrypted devices and validate implementation of encryption products at least annually.
        3. Documentation shall exist for key management procedures.
        4. At-Rest encryption procedures exist and can be demonstrated.
        5. In-Transit encryption procedures exist and can be demonstrated.
        6. Exception logs exist and can be produced for those resources that are excluded from this policy.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

* + - * 1. NONE

# PS – Personnel Security

### **Purpose, Scope & Intent**

### This policy establishes the Information Security Personnel Security Policy, for managing risks for PII Information by ensuring that the agency assesses risk by role and position and screens individuals prior to authorizing access to the information system and performs background checks on individuals with direct access to <Your Agency Name Here> datacenters.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of <Your Agency Name Here> .

### The <Your Agency Name Here> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, data communication and transfer.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### The Information Security Personnel Security Policy seeks to assure integrity and fitness requirements apply to all contractors seeking to perform services on behalf of the <YOUR AGENCY NAME HERE> . In addition, all contractor personnel who will have long term access to <Your Agency Name Here> facilities, sensitive information, or Information Technology Resources, must meet minimum security standards required by regulation. This policy shall not apply to intermittent vendors who access <Your Agency Name Here> facilities on an infrequent, and generally unscheduled basis, and do not require access to sensitive information (i.e. equipment repair, delivery personnel, etc.). These vendors should not be processed under this circular, but must be continuously and attentively escorted, kept under visual surveillance, and work only during normal business hours. Building maintenance, repair and custodial workers may require security checks consisting of fingerprint checks to allow unescorted access to <Your Agency Name Here> space.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# PE - Physical and Environmental Policy

### **Purpose, Scope & Intent**

### This policy establishes the Information Security Physical and Environmental Policy, ensures the agency develops, documents and maintains a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> (<YOUR AGENCY NAME HERE> ). Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <Your Agency Name Here> .

### The <Your Agency Name Here> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, data communication and transfer.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### <Your Agency Name Here> information Security Physical and Environmental Policy protects its information resources through implementation of sound physical, environmental, and administrative security controls designed to reduce the risk of physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and use by unauthorized personnel.

### Where possible, all information resources (including portable information resources) must reside in a protected environment. Physical and administrative security controls must be implemented at each facility to protect against unauthorized personnel access and to protect the physical integrity of <Your Agency Name Here> information resources located at the facility. Such physical and administrative security controls include the following:

1. Physical access controls.
2. Physical protection of information resources.
3. Environmental security.
4. Facility continuity planning.

### **Facility contracts & Data Centers**

### <Your Agency Name Here> shall store or transmit Restricted-Use Information to authorized personnel only.

### <Your Agency Name Here> 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

### <Your Agency Name Here> shall require authorized personnel to authenticate themselves prior to entry to data centers that process, store or transmit Restricted-Use Information.

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

### <Your Agency Name Here> shall log all visitor access to data centers that process, store or transmit Restricted-Use Information.

### 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.

### <Your Agency Name Here> shall ensure sufficient power protection is available for critical information systems to perform an orderly shutdown.

### **Media**

### <Your Agency Name Here> shall restrict physical access to media that store Restricted-Use Information to authorized personnel only.

### 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.

### <Your Agency Name Here> shall ensure appropriate safeguards when media is transported by authorized personnel outside of a controlled area.

### **Secure Purchasing and Acquisition**

### 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.

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

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# PL - Planning

### **Purpose, Scope & Intent**

### This policy establishes the Enterprise Security Planning Policy, for managing risks from inadequate security planning through the establishment of an effective security planning program. The security planning program helps the <Your Agency Name Here> implement security best practices with regard to enterprise security planning, preparation, and strategy.

### The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <YOUR AGENCY NAME HERE> . Any information that is transmitted or stored on <Your Agency Name Here> IT resources (including e-mail, messages and files) is the property of <YOUR AGENCY NAME HERE> .

### The <Your Agency Name Here> information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a security planning capability throughout <Your Agency Name Here> and its business units to help the organization implement security best practices with regard to enterprise security planning, preparation, and strategy.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### <Your Agency Name Here> will have documented security roles and responsibilities. These will be laid out in a in the Rolls and Responsibilities section of this document. Role owners will attest at a minimum annually to understand the policy and validating ownership of their assigned roles and associated duties.

### <Your Agency Name Here> will have a documented security Program/Plan. This will contain a dashboard with a subjective assessment of the agencies security health. It shall also include a roadmap outlining the agencies direction towards continuous improvement.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# PM - Program Management

### **Purpose, Scope & Intent**

### This policy establishes the Security Program Management Policy, for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective System and Information Integrity program. The system and information integrity program helps the <Your Agency Name Here> implement security best practices with regard to system configuration, security, and error handling.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <YOUR AGENCY NAME HERE> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of <YOUR AGENCY NAME HERE> .

### The <Your Agency Name Here> information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a system and information integrity capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, security, and error handling.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### <Your Agency Name Here> will form and manage an information security program for the agency.

### The security program will contain the following:

### Assigned Senior Information Security Officer

### Allotted Information Security Resources

### (POAM) Plan of Action and Milestones

### Information System Inventory

### Information Security Measures of Performance

### Enterprise Security Architecture

### Critical Infrastructure Plan

### Risk management Strategy

### Security Authorization Process

### Mission/Business Process Definitions

### Insider Threat Information

### Information Security Workforce

### Testing, Training and Monitoring

### Contacts with Security Groups and Associations

### Threat Awareness Program

### The program will be reviewed at a minimum quarterly by the (GRC) Governance Risk and Compliance Council

### Information Security Policies will be reviewed at a minimum annually and be updated and communicated as significant changes occur.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# RA - Risk Assessment

### **Purpose, Scope & Intent**

### This policy establishes the Enterprise Risk Management Policy, for managing both the overall broad agency risks, as well risks associated with agency information assets, information leakage, and network vulnerabilities and program/project risks.

### The Risk Management Policy and associated plans, augment <Your Agency Name Here> mission, by proactively identifying threats and vulnerabilities, which can result in negative consequences for the agency.

### The scope of this policy is applicable to all potential risks except those explicitly excluded in the assumptions of the Risk Management Plans. Information Technology (IT) resources owned or operated by <Your Agency Name Here> as well as any information, that is transmitted or stored on <Your Agency Name Here> IT resources (including e-mail, messages and files) is the property of <Your Agency Name Here>

### The <Your Agency Name Here> Security policy serves to be consistent with best practices associated with organizational Security and Information Security management. It is the intention of this policy to establish a Security Risk Management capability throughout <Your Agency Name Here> for identifying, assessing, and managing security risk that may occur across the enterprise environment.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### The following subsections outline the Risk Management standards that constitute <Your Agency Name Here> policy. Each <Your Agency Name Here> business System is then bound to this policy and must develop or adhere to a program plan that demonstrates compliance with the policy related the standards documented.

### All <Your Agency Name Here> business Systems must develop, adopt or adhere to a formal, documented risk assessment procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

### All <Your Agency Name Here> business Systems must categorize information and the information asset in accordance with applicable directives, policies, regulations, standards, and guidance. A NIST Model of Low, Moderate and High will be used. This includes documenting the security categorization results (including supporting rationale) for the system and to ensure the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

### All <Your Agency Name Here> business Systems must conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information asset and the information it processes, stores, or transmits. This includes:

### Documenting the risk assessment results in a Risk Assessment report;

### Reviewing the results;

### Disseminating the results to the <Your Agency Name Here> Leadership Team;

### Updating the risk assessment every year or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system;

### Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by following best practice;

### Scans for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;"

### Analyzes vulnerability scan reports and results from security control assessments;

### Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and

### Shares information obtained from the vulnerability scanning process and security control assessments with peer groups to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

### Scans for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;"

### The organization employs a technical surveillance countermeasures survey at organization defined locations.

### The Policy shall be reviewed at least once every year to ensure relevancy and updated every three years.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# RA - Approval

### **Purpose, Scope & Intent**

### The purpose of this policy is to provide developers, contractors and administrators of <Your Agency Name Here> applications with an understanding of the approval process required for initial development and change requests.

### This policy applies to any and all application and system development.

### In order to help safeguard <Your Agency Name Here> web applications from unauthorized changes, and to ensure that they are consistent with user and management expectations, owners of <Your Agency Name Here> web applications must create and implement an approval process for initial development and on-going change requests. Where possible, this approval process should enforce separation of duties for those associates or contractors who are involved in one or more of the following processes: developing/modifying web applications, approving changes, and/or authorizing deployment into production environments. If separation of duties is not possible due to staffing limitations or availability, <Your Agency Name Here> must employ proper management oversight and approval.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### Create, document, and implement a process of approval for Systems and applications.

### Enforce separation of duties for approval and deployment by implementing one of the following options:

### Deployment to production must be approved by an individual/group who has proper authority and who was not involved in developing or making changes to the application.

### If separation of duties is not possible due to staffing limitations or availability, <Your Agency Name Here> must ensure that proper management oversight is in place to monitor, document and approve all changes.

### The manner in which <Your Agency Name Here> web application development and change requests are documented, approved, and retained is largely up to the discretion of the individual departments.  For example, <Your Agency Name Here> utilizes Redmine as its ticketing system. E-mail, blogs, wikis, or a workflow may also be used for tracking changes and approval, however, <Your Agency Name Here> ’s primary change tracker is Redmine.

### The department should define the roles and responsibilities that form a chain of approval from the client who requested the web application, the functional group who supports and/or “owns” the data, the developers of the web application, the tech support group who will be supporting/maintaining it, etc.

### The approval process should document at a minimum:

### A description of the modification to be approved

### Any important details (e.g. deployment details, modification details)

### Any deviations from the normal process (e.g. deployment details, chain of approval changes)

### The name and position of the approver

### The name and position of the individual/group who made the changes

### The name and position of the individual/group who is responsible for moving the changes to production

### The name and position of the individual/group who authorized the changes to production

### The date and time of approvals

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# CA - Security Assessment and Authorization

### **Purpose, Scope & Intent**

### This policy establishes the Agency Security Assessment and Authorization Policy, for managing risks from inadequate security assessment, authorization, and continuous monitoring of Agency information assets through the establishment of an effective security planning program. The security planning program helps <Your Agency Name Here> implement security best practices with regard to enterprise security assessment, authorization, and continuous monitoring.

### The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <YOUR AGENCY NAME HERE> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IT resources (including e-mail, messages and files) is the property of <YOUR AGENCY NAME HERE> .

### The <AGENCY ACRONYM Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a security assessment and authorization capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to enterprise security assessment, authorization, and continuous monitoring.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### The objective of security assessment and authorization policy is to provide guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls.

### <Your Agency Name Here> has established an integrated agency-wide decision structure for cybersecurity risk management (the Risk Management Framework (RMF) that includes cybersecurity requirements for information technologies will be managed through the principals established in National Institute of Standards and Technology [(NIST) Special Publication (SP) 800-37](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf).

### This plan ensures that <Your Agency Name Here> follows the established guidelines and requirements for security assessment and authorization. The formal System Security Plan is documented separately. The purpose of this document is to consolidate information and provide traceability to security control requirements.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# SC - System and Communications Protection

### **Purpose, Scope & Intent**

### This policy establishes the Enterprise System and Communications Protection Policy, for managing risks from vulnerable system configurations, denial of service, data communication and transfer through the establishment of an effective System and Communications Protection program. The system and communications protection program helps the <Your Agency Name Here> implement security best practices with regard to system configuration, data communication and transfer.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <Your Agency Name Here> .

### It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, data communication and transfer.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### It is <Your Agency Name Here> policy to protect the confidentiality, integrity and availability of information systems, data residing within these systems and the communications among these systems and with systems external to the <Your Agency Name Here> accreditation boundaries.

### System operators, managers, maintainers and providers of <Your Agency Name Here> information & communication systems shall:

### Separate user functionality (including user interface services) from information system management functionality in its systems. Unauthorized and unintended information transfer via shared system resources shall be prevented.

### Protect systems against or limit the effects of denial of service attacks.

### Implement boundary protection. This protection shall address the external boundary as well as key internal boundaries, which shall be identified in the system security plan.

### Logically separate sub networks for publicly accessible system components from internal networks.

### Manage and document interfaces used and their protection capabilities to connect to external networks. Limit the number of the external network connections to assure effective traffic monitoring.

### Terminate <Your Agency Name Here> network connections at the end of the session or after a period of inactivity for remote sessions • Protect the integrity and confidentiality of transmitted and at rest Personally Identifiable Information (PII) and Sensitive Information (SI) with federally compliant encryption.

### Establish and manage cryptographic keys for required cryptography employed within the information system.

### Configure collaborative computing to prohibit remote activation unless an exception has been approved by <Your Agency Name Here> designated leadership.

### For systems employing Public Key Infrastructure (PKI), issue, or obtain from an approved service provider, public key certificates under an appropriate certificate policy.

### Define acceptable and unacceptable mobile code and mobile code technologies. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations.

### Authorize, monitor, and control the use of Voice over Internet Protocol (VoIP) within the information system through established usage restrictions and implementation guidance for VoIP technologies, based on the potential to cause damage to the information system if used maliciously.

### Encrypt all Domain Name System (DNS) services • Configure internal Domain Name System (DNS) servers to: only process name/address resolution requests from internal clients.

### Configure external DNS servers to: only process name/address resolution information requests from external clients.

### Configure <Your Agency Name Here> information systems to request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources for recursive or caching resolver DNS servers.

### Provide fault-tolerant name/address resolution service for all information systems

### Provide mechanisms to protect the authenticity of communications sessions.

### ROLES AND RESPONSIBILITIES The following roles have specific responsibilities pertaining to system and communication protection management. The sections below describe only the responsibilities for these roles as they relate to system and communication protection management. Refer to <Your Agency Name Here> information Security Policy 5000.01, The <Your Agency Name Here> information Security Program, for the full description of the responsibilities for these roles.

### Technology Development Manager, Antarctic Infrastructure & Logistics (AIL) The Technology Development Manager is the responsible official of the <Your Agency Name Here> system and communication protection management program.

### <Your Agency Name Here> information Security Manager (ISM) The <Your Agency Name Here> information Security Manager (ISM) provides oversight of the system and communications protection program and compliance with this policy.

### Coordinates assessment of security controls for system and communications protection.

### Supporting Organizations Supporting organizations assist with the development of system and communications protection procedures and standards. Also ensure system and communications protection is in alignment with guidance from NSF/PLR. Personnel shall provide <Your Agency Name Here> participants with support and guidance in system and communications protection.

### Tenant Organizations Tenant organizations with systems interconnected to the <Your Agency Name Here> enterprise network are responsible for securing their systems in accordance with this policy.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### SC-28(1) Data at rest on Mobile Devices is not encrypted.

# SI - System and Information Integrity

### **Purpose, Scope & Intent**

### This policy establishes the Enterprise System and Information Integrity Policy, for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective System and Information Integrity program. The system and information integrity program helps the <Your Agency Name Here> implement security best practices with regard to system configuration, security, and error handling.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <YOUR AGENCY NAME HERE> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of <YOUR AGENCY NAME HERE> .

### The <Your Agency Name Here> information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a system and information integrity capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, security, and error handling.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### The organization develops, disseminates, and periodically reviews/updates:

### system and information integrity policy and procedures that remain consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

### system and information integrity procedures that are developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

### and provide assurance that the data being accessed or read has neither been tampered with, nor been altered or damaged through a system error, since the time of the last authorized access.

### **APPLICATION DEVELOPMENT & PROCESSING STANDARD**

### Entities shall define and document principles and procedures for secure application development. This will include;

### The methodology used and its major subcomponents to include;

### Project or Idea Initiation

### Business Case Development and Funding Approval

### Requirements Gathering and Analysis

### Application Architecture and Design

### Development

### Documentation

### Testing (Including Security Testing)

### Training and Quality Control

### Deployment

### Support

### 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.

### **SYSTEMS OPERATIONS STANDARD ASSESSMENT OPERATIONS**

### 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.

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

### Entities shall document and implement a Plan of Action and Milestones document for the security issues discovered in Security Assessments and Vulnerability Scanning, assign rankings and establish corrective actions that are reviewed, updated, and approved quarterly by data owner or authorized designee.

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

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

### **INTEGRITY OPERATIONS**

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

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

### Entities shall document and investigate integrity discrepancies.

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

### Configuration Management & System Protection

### <Your Agency Name Here> shall not run information system components, hardware, software, or firmware on unsupported versions

### <Your Agency Name Here> shall build information systems that process, store or transmit Restricted-Use Information from a standard configuration baseline.

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

### <Your Agency Name Here> shall maintain an asset inventory of information systems components and update it as it changes and review it at least annually.

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

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

### <Your Agency Name Here> shall implement boundary protection mechanisms with capability to monitor and control network communications.

### Within the boundary, <Your Agency Name Here> shall create security zones based on data and information system classification.

### <Your Agency Name Here> shall employ malicious code protection mechanisms on systems that contain Restricted-Use Information.

### <Your Agency Name Here> shall configure malicious code protection mechanisms to perform weekly scans of files on information systems.

* + - * 1. Where malicious code protection mechanisms require regular signature or detection engine updates, <Your Agency Name Here> shall employ a documented update mechanism that includes testing and installation of applicable updates.

### **Change Management**

### The agency shall use a Change Control Procedure to promote systems from Test to Production Environments.

### Applications shall implement Event Logging and enable logging when moving applications to production environments.

### Application Event Logs shall be maintained for a minimum of 180 Days

### System Logging will be enabled on all production systems and shall at a minimum track access ID, access time, what was accessed.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# SA - System and Services Acquisition

### **Purpose, Scope & Intent**

### The Agency’s information assets are essential resources in delivering the Agency’s core mission. These assets include information and communications technology equipment (e.g. hardware and operating systems), software used on <Your Agency Name Here> provided computers, multi-user or enterprise applications hosted on <Your Agency Name Here> owned servers and applications and services provided by external Third-Party vendors that store, access, process, or transmit <Your Agency Name Here> data. The purpose of this policy to protect those assets.

### This policy applies to all departments, and members of the Agency community in all locations identified as the owners of assets that create, access, store, process, or transmit data and information. This includes assets purchased, licensed, or contracted by the Agency that are either centrally funded or grant and special account funded whether running in the Agency data center and network, or provided externally by a Third-Party.

### The intent is to ensure employees have a documented reference they can refer to in support the policy.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### It is Agency policy to manage these assets across each phase of their life cycle: plan and acquire; configure and deploy; maintain, support and upgrade; decommission, retire, and dispose of. Each phase must include the approval of the agency Secretary of Commerce, or designee, to ensure the assets conform to standards addressing technology architecture, information security, service delivery, service operation, refresh, disposal, and license management.

### By implementing this policy, the Agency will:

### ensure that appropriate information security standards, practices, and controls are included and applied during all phases of an asset's life cycle,

### ensure conformance with appropriate technology architecture, service delivery, service operation, and license management standards,

### ensure proper removal of data and licenses when an asset is re-purposed, retired, or disposed,

### integrate life cycle management into the asset acquisition or implementation processes and require Secretary of Commerce, or designee, approval for any asset that stores, accesses, processes, or transmits <Your Agency Name Here> data,

### prevent the introduction of new information security risks when an asset is modified, undergoes significant change, is upgraded, or retired,

### ensure information, data, and technology assets are regularly backed up, and critical IT assets are included in an IT disaster recovery plan,

### comply with Federal, State, local laws and regulations, Agency policies, and applicable agreements binding the agency,

### ensure this policy is consistently applied and monitored through the use of a compliance program.

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### **NONE**

# AP AR, DI, DM, IP, SE, TR, UL Privacy

### **Purpose, Scope & Intent**

### This policy establishes the Information Privacy Policy, ensures the agency develops, documents and maintains a privacy policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, while providing the agency employee’s partners, vendors and end users a consistent policy.

### The scope of this policy is applicable to all Information Services (IS) resources owned or operated by the <Your Agency Name Here> . Any information not specifically identified as the property of other parties, that is transmitted or stored on <Your Agency Name Here> IS resources (including e-mail, messages and files) is the property of the <Your Agency Name Here>

### The <Your Agency Name Here> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a system and communications protection capability throughout <Your Agency Name Here> to help the organization implement security best practices with regard to system configuration, data communication and transfer.

### All users (<Your Agency Name Here> employees, contractors, vendors or others) are responsible for adhering to this policy. All Management and IS resources are to implement the policy, controls and compliant procedures to enforce policy.

### **Policy**

### <Your Agency Name Here> serves as the national information systems development and support center for <YOUR AGENCY NAME HERE> . <Your Agency Name Here> helps state and local workforce agencies meet the needs of today’s users by providing intuitive, integrated information technology solutions and exceptional technical support. <Your Agency Name Here> IS committed to protecting privacy and safeguarding the information collected through the <Your Agency Name Here> Applications web-based application.

### For the purpose of this policy, Personally Identifiable Information (PII) means information that can be used to distinguish or trace an individual’s identity, such as their name, Social Security Number, state identification number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, medical, educational, financial, and employment information, etc.

### PII also includes other information that, alone or in combination, would allow a reasonable person in the community, who does not have personal knowledge of the relevant circumstance, to identify the person with reasonable certainty. Additional detail on PII can be found in the Data Classification Policy and Data Classification Procedure.

### This Privacy Policy sets out how <Your Agency Name Here> applications collect and process personal information about a user when the application is used or when a user otherwise does business or contacts <YOUR AGENCY NAME HERE> .

### **What Information is Protected?**

### It is our policy to only collect information required to provide services and to maintain the application. The <Your Agency Name Here> application collects PII when a user registers for an account or uses the <Your Agency Name Here> application. In <YOUR AGENCY NAME HERE> , contact data is collected, including names, addresses, telephone numbers social security numbers, work histories and tests scores. In ServiceLink, this information is collected and information about the user’s WIOA or program eligibility, program enrollments, goals and program outcomes and follow-up results.

### <Your Agency Name Here> asks for and collects information from users in different ways. If a user utilizes Job Match and creates a job seeker or employer account, they provide certain PII such as name, business name, address and telephone numbers and e-mail address. The user may create an electronic resume or job listing to be stored online in <Your Agency Name Here> where basic profile information is collected. While the registration process includes items such as: citizen, gender, race, Social Security number, FEIN, SEIN, and age, this information is only used to fulfill reporting requirements and is not released.

### <Your Agency Name Here> automatically collects IP addresses and application usage information. When users employ some of the application's features, such as creating an account, completing a resume, or reporting client activities, <Your Agency Name Here> collects PII that may include name, age, address, e-mail address, and facts about careers and interests or similar information.

### <Your Agency Name Here> may pass cookies to user’s computers. Cookies are information files that the web browser places on the hard drive of the computer or temporarily in the computer's memory when accessing the <Your Agency Name Here> application. Cookies cannot damage user files nor can they read information from a user's hard drive.

### The <Your Agency Name Here> application collects aggregate log data including such items as the number of job searches performed, or the number of times an individual job order is viewed. This data contains no personal information and is used only as an overall performance indicator for the application. The <Your Agency Name Here> error logging system, however, will collect usernames with any error that occurs as a means to help technical staff understand the error.

### **How Is the Information Utilized?**

### Some of the data that collected is used in the aggregate to allow <Your Agency Name Here> to better understand how the application is used. <Your Agency Name Here> does not disclose information about individual visits or share other private information with outside parties without prior authorization from the individual and will not use this data for any commercial purpose. The principal use of information is for the purposes for which a user specifically provides the information. Information collected is used to create a personal profile or job listing to post in a searchable database on <Your Agency Name Here> servers. Once a user sends contact and other information to an employer or recruiter, <Your Agency Name Here> IS not responsible for the retention, use or privacy practices of that employer or recruiter. The user may choose to restrict the display of PII in the application by selecting the level of disclosure. This way PII or access to all of account information can be limited. The user can also access, amend or delete any part of their account.

### **How Is DATA Secured?**

### To ensure that PII collected in the <Your Agency Name Here> application is protected; <Your Agency Name Here> has implemented security measures that include limiting the people who have physical access to <Your Agency Name Here> database servers, installing electronic security using 256-byte encryption SSL and individual password protection to guard against unauthorized access for all accounts. Only the user or third parties that the user has provided a password can access the user's account. User’s play a valuable part in security as well. After a user has finished using their account, the user should log off and exit the browser so no unauthorized persons can access account information.

### **AJLA Collection and Protection of SSN Data (State of Illinois)**

### This policy statement will serve as written acknowledgement by the undersigned Licensor (“Recipient”) that any and all SSNs disclosed by though <Your Agency Name Here> system will be protected in accordance with the policies set forth herein:

### The Recipient acknowledges that any SSNs disclosed by <Your Agency Name Here> will be utilized solely for the specific purpose(s) and use(s) identified in the pertaining contract, subcontract, grant, sub-grant, or other agreement between <Your Agency Name Here> and the Recipient (“Agreement”). The Recipient affirms that it will not utilize any disclosed SSNs other than for said purpose(s) and use(s) without the prior written consent of <YOUR AGENCY NAME HERE> , and that it will not archive or retain any disclosed SSNs in any manner, form, or format after the termination of the Agreement.

### The Recipient affirms that only the officers and employees of the Recipient who have a need to access disclosed SSNs for the purpose(s) and use(s) identified in the Agreement will have access to disclosed SSNs. The Recipient also affirms that it is responsible for enforcing this restriction of access to disclosed SSNs, and that all of the officers and employees of the Recipient who will have access to disclosed SSNs have been trained to protect the confidentiality of SSNs in accordance with this policy statement. Training shall include instructions on proper handling of disclosed SSNs from receipt through disposal (see Paragraph 7).

### The Recipient acknowledges that all SSNs disclosed by <Your Agency Name Here> are confidential and will be protected from unauthorized use and/or disclosure. Protection from unauthorized use and/or disclosure includes:

### Restricting access to disclosed SSNs to authorized personnel in accordance with Paragraph 2;

### Storing materials, documents, or media containing disclosed SSNs in a place and/or manner physically secure from access by unauthorized persons;

### Maintaining disclosed SSNs reduced to electronic or digital media or formats such as magnetic tapes, hard drives, flash drives, CDs or server-based applications in such a way that unauthorized persons cannot access or obtain disclosed SSNs by any means; and

### Applying security measures to computer systems ensuring that only authorized personnel will have access to disclosed SSNs accessible through said computer systems.

### Per agreement with the State of Illinois, the Recipients affirm that it complies with all applicable laws, regulations, and State and federal legal authorities relating to the protection of disclosed SSNs, including, without limitation:

### Federal regulations codified at [20 CFR 603](https://www.ecfr.gov/cgi-bin/text-idx?SID=770be2390943ff0b8b42ffcba18bddba&mc=true&node=pt20.3.603&rgn=div5#se20.3.603_14) pertaining to recipients of unemployment compensation information;

### The Illinois Data Processing Confidentiality [Act, 30 ILCS 585/0.01 et seq](http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=553&ChapterID=7).;

### Section 1900 of the Illinois Unemployment Insurance [Act, 820 ILCS 405/1900](https://helpdesk.ajla.net/login?back_url=https%3A%2F%2Fhelpdesk.ajla.net%2F); and

### The Recipient affirms that it will not subcontract, sub-grant, or otherwise transfer or assign any of the Recipient’s duties or obligations involving disclosed SSNs under the Agreement without the prior written consent of <YOUR AGENCY NAME HERE> , and/or the approval and/or execution of an appropriate subcontract, sub-grant, or other third-party agreement by <YOUR AGENCY NAME HERE> .

### The Recipient affirms that it will retain records of access to and use of disclosed SSNs for a period of three years following receipt of the SSNs, and will allow on-site inspections by <Your Agency Name Here> to verify SSN security and usage as well as audit access during the three-year period after the receipt of the SSNs. The Recipient also affirms that it will correct any security and/or usage deficiency(ies) identified by <Your Agency Name Here> promptly upon receipt of written notice of said deficiency(ies).

### The Recipient acknowledges that the materials, documents, or media of any type or form that contain SSNs disclosed by <Your Agency Name Here> are the property of and shall be returned to <Your Agency Name Here> upon request. The Recipient also acknowledges that it is responsible for the disposal of said materials, documents, or media upon termination of the Agreement. “Disposal” means the return or delivery of said materials, documents, or media to <YOUR AGENCY NAME HERE> , or the destruction of same, as directed by <YOUR AGENCY NAME HERE> .

### **Exceptions**

# Exceptions must be submitted to the Governance Compliance and Risk Council for review and approval. No exception shall be permitted without the Agency Secretary of XXXXXXXX or their designee’s review and approval.

### **Current Exceptions**

### AR-2 -A new Privacy Impact Assessment needs to be facilitated in alignment of the NIST Privacy controls and will be completed no later than 12/31/2018.

### IP-1, IP-2, IP-3 and IP-4 - The Privacy statements will be updated in the next upcoming release and will update the languages as well as notify users ahead of privacy data collection that their data is being collected and provide a method of contact if the user wish to report concerns, issues or has questions.

### TR-2 – <Your Agency Name Here> IS not a federal agency and therefore does not publish System of Records Notices (SORNs) in the Federal Register. Permanent Exception

**7.Policy Compliance**

This policy shall take effect upon signature of The Director of <Your Agency Name Here> and posted to the Inside <Your Agency Name Here> Fileshare Site. The Policy shall be reviewed at least once every year to ensure relevancy and updated every three years.

Any violation of these policies and guidelines may result in disciplinary action, up to and including dismissal, and the possibility of civil penalties, and/or criminal prosecution. <Your Agency Name Here> will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

**8.POLICY AUTHORITY**

This policy has been issued under the authority of the <Your Agency Name Here> Secretary of XXXXXXXX and the <Your Agency Name Here> information Security Officer. Pending Approval from the Kansas Secretary of Commerce.

1. **DOCUMENT CONTROL**

| **Version #** | **Implemented By** | **Revision Date** | **Reason** |
| --- | --- | --- | --- |
| 1.0 | Mark Abraham - ISO | 6/28/2018 | Initial Policy |
| 1.2 |  |  |  |
| 1.3 |  |  |  |
| 1.4 |  |  |  |
| 2.0 |  |  |  |
|  |  |  |  |
|  |  |  |  |

**<Your Agency Name Here> - Technical Support**

**EMPLOYEE AGREEMENT FORM**

**ELECTRONIC COMMUNICATION SYSTEMS**

1. **GENERAL**

As an employee, agent, associate, representative, intern, contractor, temporary employee, assignee, or other designee (hereinafter referred to collectively as “Employee” strictly for the purposes of this agreement form) of the <Your Agency Name Here> (hereinafter referred to as “<Your Agency Name Here> ) you have or may be provided access to various electronic communication systems including, but not limited to, telephone voicemail, Email, and the Internet. These systems are provided to you to assist in the conduct of <Your Agency Name Here> ’s business. This agreement form is based upon the <Your Agency Name Here> Acceptable Use of Information Technology Resources. Employees are specifically directed to read the following <Your Agency Name Here> Policies.

* Data Classification Policy
* Remote Access Policy
* Telecommuting Policy – as applicable
* Mobile Device Policy & User Agreement – as applicable

1. **NO PRIVACY RIGHTS IN ELECTRONIC COMUNICATION SYSTEMS**

Voicemail, E-mail, access to the Internet and the information or communications sent or stored on them are and remain at all times the property of <YOUR AGENCY NAME HERE> . As such, you do not have any right to information or communications sent or stored on <Your Agency Name Here> IT resources. <Your Agency Name Here> reserves the right to monitor, access, retrieve, read, and/or distribute, for official purposes, any information or communications sent or stored on IT resources, and it in fact does so as it determines is necessary. You should be aware that, even when information or communications on such IT resources are deleted, it may be possible for <Your Agency Name Here> to retrieve such information or communications and it in fact does so as it determines is necessary. You should also be aware that your use of a password may not prevent other individuals from accessing your IT resources nor does it prevent <Your Agency Name Here> from accessing them. Passwords are strictly for security purposes; passwords are not for the protection of privacy. This applies regardless of where you use <Your Agency Name Here> IT resources; whether from a remote or local access.

1. **AUTHORIZED USERS**

Employees may access only those electronic communication systems that the Employee has been expressly granted permission by <Your Agency Name Here> to access. Unauthorized accessing, review, duplication, dissemination, removal, damage, or alteration of files, passwords, digital certificates, computer systems or programs, voicemail messages, E-mail messages, Internet communications, information, or systems, or other such property of <YOUR AGENCY NAME HERE> , or improper use of information obtained by such unauthorized means, constitutes grounds for disciplinary action, up to and including dismissal, and the possibility of a criminal complaint being filed.

1. **IMPROPER CONTENT**

Each Employee is responsible for the content of all text, audio, or images that they place, send, retrieve, or view over any electronic communication systems. All messages communicated on such systems should have the Employee’s name attached; messages may not be transmitted using another Employee’s name or under an assumed name. Each Employee is responsible for ensuring that he or she uses such systems in an effective, ethical, and lawful manner. Your use of electronic communication systems shall not include content that might be considered offensive or disruptive to any Employee. Offensive content, whether text or image, includes, but is not limited to, material of a sexual nature including comments, jokes, or images; racial slurs; defamatory materials; threats or insults; or any other matter that might offend a person on the basis of his or her age, disability, gender, race, religion, national origin, ancestry, political affiliation, military or veteran status, or any other classification protected by federal, state, or local law. The determination of the Secretary of Revenue as to what constitutes offensive or disruptive content is final. Employees may neither send nor receive unauthorized copyrighted materials. Violation of this policy constitutes grounds for disciplinary action, up to and including dismissal, and the possibility of a criminal complaint being filed.

1. **CONFIDENTIALITY**

Disclosure of confidential information (e.g., taxpayer information, driver’s license information, etc.) via electronic communication systems is strictly prohibited unless required in the lawful performance of assigned duties. Violation of this policy constitutes grounds for disciplinary action, up to and including dismissal, and the possibility of a criminal complaint being filed.

1. **SOLICITATION**

Use of electronic communication systems to solicit for religious, personal, business, charitable, union-organizing (unless authorized by state law), or political purposes is prohibited. Officially sanctioned state charities are exempted under this Policy. Violation of this policy constitutes grounds for disciplinary action, up to and including dismissal, and the possibility of a criminal complaint being filed.

1. **PERSONAL USE OF ELECTRONIC COMMUNCATION SYSTEMS**

Use of IT resources should be for official <Your Agency Name Here> uses only. Limited appropriate personal use is permitted. The determination of the IT Director of <Your Agency Name Here> as to what constitutes limited appropriate personal use shall be final, but in no event shall it include any use contrary to this agreement form and <Your Agency Name Here> Policy. Violation of this policy constitutes grounds for disciplinary action, up to and including dismissal, and the possibility of a criminal complaint being filed.

1. **DISCIPLINE FOR IMPROPER USE OF ELECTRONIC COMMUNICATION SYSTEMS**

Improper use of IT resources subjects the offending Employee to discipline up to and including dismissal, and the possibility of a criminal complaint being filed. Past breaches of any policy respecting an Employee’s use of IT resources are not a bar to discipline for present or future breaches. In other words, the fact that you were not disciplined for breaches of policy in the past does not mean you will be excused or immune from discipline now or in the future.

1. **EMPLOYEE CONSENT**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, have read the preceding statement, understand it, and agree thereto. Additionally, I have read all <Your Agency Name Here> Policy and Procedures, and agree thereto.

At the time of signing this agreement, I have asked any questions that I have concerning this policy and agreement form, and such have been answered to my satisfaction by my supervisor and/or <Your Agency Name Here> Office of Personnel Services.

I understand that any violation of these policies and guidelines may result in disciplinary action, up to and including dismissal, and the possibility of a criminal complaint being filed.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 Employee Printed Name

**APPENDIX A AU 2- List of Auditable Events**

Configure information systems to audit for the following events:

The following events shall be identified within server audit logs:

(1) Server startup and shutdown

(2) Loading and unloading of services

(3) Installation and removal of software

(4) System alerts and error messages

(5) User logon and logoff

(6) System administration activities

(7) Accesses to sensitive information, files, and systems

(8) Account creation, modification, or deletion

(9) Modifications of privileges and access controls

(10) Additional security-related events, as required by the SO or to support the nature of the supported business and applications

The following events shall be identified within application and database audit logs:

(1) Modifications to the application

(2) Application alerts and error messages

(3) User logon and logoff

(4) System administration activities

(5) Accesses to information and files

(6) Account creation, modification, or deletion

(7) Modifications of privileges and access controls

The following events shall be identified within network device (e.g., router, firewall, switch, wireless access point) audit logs:

(1) Device startup and shutdown

(2) Administrator logon and logoff

(3) Configuration changes

(4) Account creation, modification, or deletion

(5) Modifications of privileges and access controls

(6) System alerts and error messages