Policy Title and #	CIO-106: Enterprise Privacy Policy				
Effective Date:	08/17/2018	Revision Date:	-	Review Date:	08/05/2020

POLICY STATEMENT:
This policy provides a structured set of principles for protecting privacy and serves as a roadmap for agencies to use in identifying and implementing privacy principles for the entire life cycle of Personal Information (PI), whether in paper or electronic form.

DEFINITIONS:
Personal Information: Personal Information (PI) is defined in KRS 61.931(6)

POLICY:
The following provides a structured set of privacy controls, based on NIST (National Institute of Standards and Technology) best practices, that assist agencies' compliance with applicable federal laws, Executive Orders, directives, instructions, regulations, policies, standards, guidance, and agency-specific issuances;

AP -Authority and Purpose

- AP-1 Authority to Collect: The agency must determine and document the legal authority that permits the collection, use, maintenance, and sharing of PI, either generally or in support of a specific program or information system need.
- AP-2 Purpose Specification: The agency must describe the purpose(s) for which PI is collected, used, maintained, and shared in its privacy notices.

AR- Accountability, Audit and Risk Management

- AR-1 Governance and Privacy Program: The agency must:
    a. Appoint an Agency Privacy Officer accountable for developing, implementing, and maintaining an agency-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PI by programs and information systems;
    b. Monitor all applicable privacy laws (federal and/or state), and policy for changes that affect the privacy program;
    c. Allocate budget, staff and other sufficient resources to implement and operate the agency-wide privacy program;
    d. Develop a strategic agency privacy plan for implementing applicable privacy controls, policies, and procedures;
    e. Develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PI; and
    f. Update the privacy plan, policies, and procedures every two years.

- AR-2 Privacy Impact and Risk Assessment: The agency must:
    a. Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PI; and
    b. Conduct Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, policy, or any existing agency policies and procedures.

- AR-3 Privacy Requirements for Contractors and Service Providers: The agency must:
    a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. Include applicable privacy requirements in contracts and other acquisition-related documents.

- AR-4 Privacy Monitoring and Auditing: The agency must monitor and audit privacy controls and internal privacy policy every two years to ensure effective implementation.
- AR-5 Privacy Awareness and Training: The agency must:
  a. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
  b. Administer basic privacy training at least annually and target role-based privacy training for personnel having responsibility for PI and/or for activities that involve PI.
  c. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements.

- AR-6 Privacy Reporting: The agency develops, disseminates, and updates reports to the Commonwealth Office of Technology (COT), Office of Chief Information Officer as appropriate, to demonstrate accountability with specific and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

- AR-7 Privacy-Enhanced System Design and Development: The agency must design information systems to support privacy by automating privacy controls.

- AR-8 Accounting of Disclosures: The agency must:
  a. Keep an accurate accounting of disclosures of information held under its control, including:
     1) Date, nature, and purpose of each disclosure of a record; and
     2) Name and address of the person or agency to which disclosure was made;
  b. Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer, for systems that require compliance with the Privacy Act of 1974; for Commonwealth systems, retain the accounting of disclosures for five years or according to the agency's record retention policy whichever is longer; and
  c. Makes the accounting of disclosures available to the person named in the record upon appropriate request.

DI Data Quality and Integrity

- DI-1 Data Quality: The agency must:
  a. Confirm, to the greatest extent practicable, upon collection or creation of PI, the accuracy, relevance, timeliness, and completeness of that information.
  b. Collect PI directly from the individual to the greatest extent practicable;
  c. Check for, and correct as necessary, any inaccurate or outdated PI used by its agency systems; and
  d. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

- DI-2 Data Integrity and Data Integrity Board: The agency must:
  a. Document processes to ensure the integrity of PI through existing security controls; and
  b. Establish a Data Integrity Board, when appropriate, and as needed, to comply with requirements for oversight of agency computer Matching Agreements, required for Federal systems, and to ensure that those agreements comply with the computer matching provisions of the Federal Privacy Act of 1974.

DM Data Minimization and Retention

- DM-1 Minimization of PI: The agency must:
  a. Identify the minimum PI elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
  b. Limit the collection and retention of PI to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent, if consent is required; and
  c. Conduct an initial evaluation of PI holdings, establish, and follow a schedule for regularly review of these holdings every two years or, if the agency must comply with Federal Privacy Act requirements, annually, to ensure that only PI identified in the notice is collected and retained, and that the PI continues to be necessary to accomplish the legally authorized purpose.

- DM-2 Data Retention and Disposal: The agency must:
  a. Retain each collection of PI for the time period required to fulfill the purpose(s) identified in the notice or as required by law;
  b. Dispose of, destroy, erase, and/or anonymize the PI, regardless of the method of storage, in accordance with the agency's record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
  c. Use agency defined security methodology to ensure secure deletion or destruction of PI including original copies and archived records.

- DM-3 Minimization of PI used in Testing, Training, and Research: The agency must:
  a. Develop policies and procedures that minimize the use of PI for testing, training, and research; and
  b. Implement policies and procedures to protect PI used for testing, training, and research.

IP Individual Participation and Redress

- IP-1 Consent: The agency must:
  a. Provide a means, where feasible and appropriate, or as required by statute or regulation, for individuals to authorize the collection, use, maintaining, and sharing of PI prior to its collection;
  b. Provide appropriate means for individuals to understand the consequences of the decision to approve or decline the authorization of the collection, use, dissemination, and retention of PI;
  c. Obtain consent, where feasible and appropriate, or as required by statute or regulation, from individuals prior to any new uses or disclosure of previously collected PI; and
  d. Ensure that individuals are aware of and, where feasible, or as required by statute or regulation, consent to all uses of PI not initially described in the public notice that was in effect at the time the agency collected the PI.

- IP-2 Individual Access: The agency must:
  a. Provide individuals the ability to have access to their PI maintained in its records;
  b. Publish rules and regulations governing how individuals may request access to records maintained in a system subject to the Privacy Act of 1974; or in the agency's records
  c. Publish access procedures in a location readily available to individuals that provide their PI to the agency; and
  d. Adhere to Privacy Act requirements, if necessary, and agency policies and guidance, for the proper processing of individual access requests.

- IP-3 Redress: The agency must:
    a. Provide a process for individuals to have inaccurate PI maintained by the agency corrected or amended, as appropriate; and
    b. Establish a process for disseminating corrections or amendments of the PI to other authorized users of the PI, such as external information-sharing partners and, where feasible and appropriate, notify affected individuals that their information has been corrected or amended.

- IP-4 Complaint Management: The agency must implement a process for receiving and responding to complaints, concerns, or questions for individuals about agency privacy practices.

SE- Security

- SE-1 Inventory of PI: The agency must:
    a. Establish, maintain, and update an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PI every two years; and
    b. b. Provide each update of the PI inventory to COT, the Office of the CIO to support the establishment of information privacy and security requirements for all new or modified information systems containing PI every two years.

- SE-2 Privacy Incident Response: The agency must:
    a. Develop, and implement a Privacy Incident Response Plan; and
    b. Provide an organized and effective response to privacy incidents in accordance with the agency's Privacy Incident Response Plan.

Transparency

- TR-1 Privacy Notice: The agency must:
    a. Provide effective notice to the public and to individuals regarding; (i) its activities that impact privacy, including its collection use, sharing, safeguarding, maintenance, and disposal of PI; (ii) authority for collecting PI; (iii) the choices, if any, individuals may have regarding how the agency uses PI and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PI amended or corrected if necessary;
    b. Describe, (i) the PI the agency collects and the purpose(s) for which it collects that information; (ii) how the agency uses PI internally; (iii) whether the agency shares PI with external entities, the categories of those entities, and the purposes of such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PI and how to exercise any such consent; (v) how individuals may obtain access to PI; and (vi) how the PI will be protected; and
    c. Revise its public notices to reflect changes in practice or policy that affect PI or changes in its activities that impact privacy, before, or as soon as practicable, after the change.

- TR-2 System of Records Notices and Privacy Act Statements: The agency must: Include privacy statements on its forms that collect PI (federally regulated agency's notice must comply with the Privacy Act), or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

- TR-3 Dissemination of Privacy Program Information: The agency must:
    a. Ensure that the public has access to information about its privacy activities and the public is able to communicate with the agency's Privacy Officer; and
    b. Ensure that its privacy practices are publicly available through agency websites or other publicly available means.

UL-Use Limitation

- UL-1 Internal Use: The agency must use PI internally only for the authorized purpose(s) identified in public notices or for agencies subject to federal regulation, the Privacy Act.

- UL-2 Information Sharing with Third Parties: The agency must:
  a. Share PI externally, only for the authorized purposes as described in the agency's privacy notice(s), or, if applicable, according to the Privacy Act, for a purpose that is compatible with those purposes, or for a purpose authorized by statute or regulation;
  b. Where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Service Level Agreements, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PI covered and specifically enumerate the purposes for which the PI may be used;
  c. Monitor, audit, and train its staff on the authorized sharing of PI with third parties and on the consequences of unauthorized use or sharing of PI; and evaluate any proposed new instances of sharing PI with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

POLICY MAINTENANCE:
The Commonwealth Office of Technology (COT), Office of the Chief Information Officer has the responsibility for maintaining this policy. Commonwealth agencies may choose to add to this policy as appropriate to enforce standards that are more restrictive. Therefore, staff members are to refer to their agency's internal policy, which may have additional information or clarification of this enterprise policy.

AUTHORITY:
KRS 42.726 authorizes the COT to develop policies that support and promote the effective application of information technology within the executive branch of government, as well as information technology directions, standards, and necessary management processes to assure full compliance with those policies.

APPLICABILITY:
This policy is to be adhered to by all Executive Branch agencies, and non-Executive Branch agencies, utilizing COT to manage infrastructure and services, including employees, contractors, consultants, temporaries, volunteers and other workers within state government that install, operate, or maintain production of software applications hosted on infrastructure controlled by COT. This policy requires initial determination, by the agency, of applicability of the Privacy Act of 1974, to the data collected, held or shared by the agency.

RESPONSIBILITY FOR COMPLIANCE:
Each agency is responsible for assuring that appropriate staff within their authority are made aware of the provisions of this policy, that compliance by the staff is expected, and that unauthorized and/or neglectful actions concerning this policy may result in disciplinary action, up to, and including dismissal. It is each Executive Cabinet's responsibility to enforce and manage the application of this policy.

Non-compliance with this policy may result in additional shared service charges to the Agency for COT's remediation efforts pertaining to this policy.

REVIEW CYCLE:
This policy will be reviewed at least every two years.

REFERENCES:
Helpful references can be found on the Enterprise IT Policies webpage.