**Information Privacy Policy Sample**

# Purpose

# The purpose of this Information (Data) Privacy Policy is to establish guidelines for protecting the privacy of individuals' personal information within [Agency]. This policy ensures compliance with applicable privacy laws, regulations, and standards, and promotes best practices for data privacy and protection as required by the Virginia Government Data Collection and Dissemination Practices Act, or Va. Code §§ 2.2-3800 et seq. (the “GDCDPA”).

# Scope

This policy applies to all employees, contractors, and third-party agents who handle, manage, or use personal information owned by or entrusted to [Agency].

# Definitions

| **Term** | **Definition** |
| --- | --- |
| **Personal Information[[1]](#footnote-2)** | All information that 1. Describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or
2. Affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution.

"Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information. |
| **Data Subject[[2]](#footnote-3)** | An individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system |
| **Proper purpose[[3]](#footnote-4)** | The sharing or dissemination of data or information among and between agencies in order to 1. Streamline administrative processes to improve the efficiency and efficacy of services, access to services, eligibility determinations for services, and service delivery
2. Reduce paperwork and administrative burdens on applicants for and recipients of public services
3. Improve the efficiency and efficacy of the management of public programs
4. Prevent fraud and improve auditing capabilities
5. Conduct outcomes-related research
6. Develop quantifiable data to aid in policy development and decision making to promote the most efficient and effective use of resources
7. Perform data analytics regarding any of the purposes set forth in this definition.
 |
| **Purge[[4]](#footnote-5)** | To obliterate information completely from the transient, permanent, or archival records of an agency. |
| **Processing** | Any operation performed on personal information, including collection, storage, use, disclosure, and deletion. |
| **Data Owner** | The person or entity responsible for the overall data governance of a dataset, typically a senior leader within the organization. |
| **Data User** | Any individual who interacts with data for analysis, reporting, or operational purposes. |
| **Data Custodian** | IT personnel responsible for the technical environment and security where data is stored, processed, and transmitted. |
| **ISO** | The person responsible for developing and managing the agency’s information security program. |

# Roles and Responsibilities

| **Role** | **Responsibility** |
| --- | --- |
| **Agency Data Privacy Officer (DPO)** – *if available* | * Develop and implement data privacy policies and procedures for [agency].
* Ensure agency information and processes are compliant with relevant privacy laws, regulations, and standards.
* Conduct regular privacy risk assessments and audits of agency systems and agency’s third-party suppliers.
* Serve as the point of contact for data sharing requests regarding privacy concerns and rights.
* Handle agency data breach notifications and incident responses.
* Provide data privacy training and awareness programs to agency personnel.
* Report on the agency’s data privacy posture to senior management and relevant stakeholders.
* Monitor agency data processing activities and ensure proper documentation and reporting.
 |
| **Chief Information Officer (CIO)** | * Oversee the agency’s information technology strategy, including data privacy measures.
* Ensure that privacy considerations are integrated into the agency’s IT systems and processes.
* Allocate agency resources for data privacy initiatives and technologies.
* Support the DPO in implementing and maintaining data privacy controls for the agency.
 |
| **Agency Department Heads and Managers** | * Ensure that their teams comply with applicable data privacy policies and procedures.
* Identify and address privacy risks within their departments.
* Support the DPO and data owners in implementing privacy controls.
* Promote a culture of data privacy and protection within their teams.
 |
| **Data Owner** | * Determine the regulations and sections of Virginia Code that apply to the personal information within their purview.
* Ensure agency employee’s compliance with data privacy principles and policies.
* Approve access to personal information and determine data classification levels.
* Maintain records of agency data processing activities.
* Respond to data sharing requests in a timely manner.
* Work with the DPO to address privacy risks and issues.
 |
| **Data User** | * Adhere to agency data privacy policies and procedures.
* Protect personal information and report any breaches or suspicious activities to the DPO or ISO.
* Participate in data privacy training and awareness programs.
* Use personal information responsibly and ethically in accordance with agency guidelines.
 |
| **Third-Party Vendors and Service Providers** | * Comply with the contracting agency’s data privacy policies and contractual obligations.
* Implement appropriate data protection measures.
* Report any data breaches or incidents to the agency ISO or vendor’s agency point of contact immediately.
* Assist the agency in audits and assessments as required.
 |
| **Data Custodians** | * Implement and maintain technical safeguards to protect personal information in accordance with applicable law and regulation.
* Manage data storage, backup, and recovery procedures.
* Ensure that data is securely stored, transmitted, and disposed of according to policy.
* Execute data destruction processes as authorized by data owners.
* Monitor and control access to personal information.
* Report any privacy incidents to the DPO or ISO immediately.
 |
| **Legal Team/OAG** | * Interpret and provide guidance on privacy laws, regulations, and standards.
* Assist in developing and updating data privacy policies and procedures.
* Conduct legal reviews of data processing agreements.
* Support the DPO in ensuring regulatory compliance.
* Partner with agencies on the legal aspects of data breach responses and notifications.
 |

# Policy[[5]](#footnote-6)

All [AGENCY] employees must adhere to the Virginia Government Data Collection and Dissemination Practices Act (or “GDCDPA”), pertaining to data privacy as referenced above. The purpose of the Act is to require adherence to the following key principles:

Principles[[6]](#footnote-7)

1. There shall be no personal information system whose existence is secret.
2. Information shall not be collected unless the need for it has been clearly established in advance.
3. Information shall be appropriate and relevant to the purpose for which it has been collected.
4. Information shall not be obtained by fraudulent or unfair means.
5. Information shall not be used unless it is accurate and current.
6. There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.
7. There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete, or irrelevant information.
8. Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse.
9. There shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used or disseminated for another purpose unless such use or dissemination is authorized or required by law.
10. The Commonwealth or any agency or political subdivision thereof shall not collect personal information except as explicitly or implicitly authorized by law.

## Data Collection and Sharing[[7]](#footnote-8)

Any agency[[8]](#footnote-9) maintaining an information system that includes personal information shall:

1. Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency.
2. Collect information to the greatest extent feasible from the data subject directly, or through the sharing of data with other agencies, in order to accomplish a proper purpose of the agency.
3. Establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls.
4. Maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to ensure fairness in determinations relating to a data subject.
5. Make no dissemination to another system without
	1. Specifying requirements for security and usage including limitations on access thereto, and
	2. Receiving reasonable assurances that those requirements and limitations will be observed.

NOTE: This subdivision shall not apply, however, to a dissemination made by an agency to an agency in another state, district or territory of the United States where the personal information is requested by the agency of such other state, district or territory in connection with the application of the data subject therein for a service, privilege or right under the laws thereof, nor shall this apply to information transmitted to family advocacy representatives of the United States Armed Forces in accordance with subsection N of § 63.2-1503;

1. Maintain a list of all persons or organizations having regular access to personal information in the information system.
2. Maintain for a period of three years or until such time as the personal information is purged, whichever is shorter, a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority but excluding access by the personnel of the agency wherein data is put to service for the purpose for which it is obtained.
3. Take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, about all the requirements of this chapter, the rules and procedures, including penalties for noncompliance, of the agency designed to assure compliance with such requirements.
4. Establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security.
5. Collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects that is maintained, used, or disseminated in or by any information system operated by any agency unless authorized explicitly by statute or ordinance. Nothing in this subdivision shall be construed to allow an agency to disseminate to federal government authorities’ information concerning the religious beliefs and affiliations of data subjects for the purpose of compiling a list, registry, or database of individuals based on religious affiliation, national origin, or ethnicity, unless such dissemination is specifically required by state or federal law.

## Regulatory Compliance

* In addition to the requirements of the Government Data Collection and Dissemination Practices Act, Data Owners must ensure compliance with legal, regulatory, and organizational requirements which may include FERPA, CJIS, HIPAA and other applicable laws and regulations.

## Data Privacy Breach Response

In the event of a data breach, [Agency] must follow its agency-specific incident response plan, which must include the following minimum steps:

### Detection and Reporting

* Employees and contractors must report any suspected data breaches to the ISO immediately.
* The ISO must assess the breach and determine its scope and impact.

### Containment and Recovery

* The ISO must take immediate steps to contain the breach and prevent further unauthorized access or damage.
* Recover any lost data and restore systems to normal operation.

### Notification:

* Notify affected data subjects and relevant regulatory authorities as required by § 18.2-186.6. of the Code of Virginia’s “Breach of personal information notification” law and any other applicable laws.
* Provide information on the nature of the breach, the potential impact, and steps taken to mitigate the risk.

### Investigation and Remediation:

* Conduct a thorough investigation to determine the cause of the breach.
* Implement corrective actions to prevent future breaches.

## Compliance and Monitoring

## The DPO or Data Owner must conduct regular audits and assessments to ensure compliance with data privacy policies.

## The DPO or Data Owner must monitor data processing activities to detect and address privacy risks.

## The Data Users must report non-compliance or privacy incidents to the DPO or Data Owner for further action.

## Training and Support

* The DPO or Data Owner must ensure all employees are trained on data privacy policies, principles, and best practices including handling personal information and regulatory compliance as required by ITRM Standard SEC527-1.1
* The DPO or Data Owner must promote a culture of privacy awareness within the organization.

## Policy Review

This Policy will be reviewed and updated annually from the approval date in the version history of this policy, or more frequently if appropriate. Any staff members who wish to make any comments about the Policy may forward their suggestions to [AGENCY Contact].

## Related Policies

|  |
| --- |
| **[AGENCY] Policies, Standards and Procedures** |
| Data Governance Policy |
| Data Quality Policy |
| Metadata Management Policy |
| Data Security Policy |
| Data Retention Policy |
| Data Stewardship Policy |

The [Agency] adheres to all Commonwealth Information Technology Resource Management (ITRM) policies and standards for security and architecture, which are available at the following link: [Policies, Standards & Guidelines | Virginia IT Agency](https://www.vita.virginia.gov/policy--governance/policies-standards--guidelines/).

|  |  |
| --- | --- |
|  | **VITA Related Policies** |
| IT Information Security Policy - SEC519 |
| Information Security Standard - SEC530 |
| IT Risk Management Standard - SEC520 |

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Revision Date** | **Description of Change** | **Author** |
| V1 | 6/202024 | Initial Draft | Chris Burroughs |
| V2 | 7/17/2024 | Added OAG requested changes | Chris Burroughs |
|  |  |  |  |

1. This definition is provided by 2.2-3800 Code of Virginia “Government Data Collection and Dissemination Practices Act” [↑](#footnote-ref-2)
2. This definition is provided by 2.2-3800 Code of Virginia “Government Data Collection and Dissemination Practices Act” [↑](#footnote-ref-3)
3. This definition is provided by 2.2-3800 Code of Virginia “Government Data Collection and Dissemination Practices Act” [↑](#footnote-ref-4)
4. This definition is provided by 2.2-3800 Code of Virginia “Government Data Collection and Dissemination Practices Act” [↑](#footnote-ref-5)
5. For exclusions, website privacy policies, and other agency-specific information, please see § 2.2-3800 Code of Virginia “Government Data Collection and Dissemination Practices Act” [↑](#footnote-ref-6)
6. The key principles provided by § 2.2-3800 Code of Virginia “Government Data Collection and Dissemination Practices Act” [↑](#footnote-ref-7)
7. The Data Collection and Sharing requirements are provided by § 2.2-3800 Code of Virginia “Government Data Collection and Dissemination Practices Act” [↑](#footnote-ref-8)
8. Per the GDCPA, "Agency" means any agency, authority, board, department, division, commission, institution, bureau, or like governmental entity of the Commonwealth or of any unit of local government including counties, cities, towns, regional governments, and the departments thereof, and includes constitutional officers, except as otherwise expressly provided by law. "Agency" shall also include any entity, whether public or private, with which any of the foregoing has entered into a contractual relationship for the operation of a system of personal information to accomplish an agency function. Any such entity included in this definition by reason of a contractual relationship shall only be deemed an agency as relates to services performed pursuant to that contractual relationship, provided that if any such entity is a consumer reporting agency, it shall be deemed to have satisfied all of the requirements of this chapter if it fully complies with the requirements of the Federal Fair Credit Reporting Act as applicable to services performed pursuant to such contractual relationship. [↑](#footnote-ref-9)