Data Policy Template

{This template is to serve as a starting point for agencies to leverage when building a policy serving W.S. 9-21-101. It is offered as a technical starting point only. Agencies are free to use this template in whole or in part and are encouraged to seek legal counsel for final compliance}

All purple highlighted text is intended as instructional and should be removed prior to adoption.
All yellow highlighted text is intended to denote text to be replaced by the Agency.
All green highlighted text serves as suggestions or examples. Keeping in mind, the entirety of this template is optional and at the discretion of the authoring agency.}

[Agency] Policy Header

Contents Agency will need to adjust this as they adjust the policy. Alternately, the Agency can delete this table completely

1. Purpose

This policy describes how data shall be collected, accessed, secured, and used to meet Agency and State data protection standards as well as [legislative requirements and regulatory requirements]. This data protection policy ensures [Agency]:

Agency may list specific aspects covered in this policy. Examples include:

- Complies with data protection law and follows best practices
- Protects the rights of staff, customers, and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

2. Scope

This policy applies to:

- All staff and volunteers of [Agency]
- All contractors, suppliers and other people working on behalf of [Agency]

This can include:

- Names of individuals (although unusual)
- Positions by title

3. Definitions

Agency may choose to include specific terms here; being careful not to create a derivative re-definition from other policies/regulations.

4. Data Collection

This section is to describe how data are collected. It should be broad enough to cover all data collection for all agency systems but specific enough to be actionable. It may include items such as: how collection(s) happen, sources, the authority to collect, protections, reference to other regulations, or which positions within the agency serve as the data stewards.

5. Data Access

This section is to describe how access to data is determined. It may include items such as: who (by role) has access, the levels of access, who or by what process access is determined, how data are grouped for varying access.

Only employees with a business necessity shall be granted access to data. Data shall not be shared informally. When access to confidential information is required, employees shall request it from their manager. [Agency] will provide training to all employees to help them understand their responsibilities

when handling data. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

This area is intended for the Agency to list below any specific rules they have for the access, security, and use of data Examples include:

• Strong passwords must be used and they should never be shared.

• Personal data should not be disclosed to unauthorized people, either within the [the Agency] or externally.

• Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

• Employees should request help from their line-supervisor or Manager if they are unsure about any aspect of data protection.

6. Data Security

This section is to describe security requirements. The policy may include items such as requirements for: physical security, logical security, passwords, applicable regulations (State, Federal, or local), encryption, off-shore transmissions, or employee training.

When working with private data, employees should ensure the screens of their computers are locked when left unattended. It should never be sent in clear text (e.g. email). Data must be encrypted before being transferred electronically. Managers and supervisors can explain how to send data to authorized external contacts. Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Agency may choose to list specific risks mitigated by this policy. Examples include:
This policy helps to protect [Agency] from some data security risks, including:

• Breaches of confidentiality: information being given out inappropriately.

• Failing to offer choice. All individuals should be free to choose how the [the Agency] uses data relating to them.

• Reputational damage. The [Agency] could suffer if bad actors successfully gained access to sensitive data.

7. Data Use

This section is to describe how the data are allowed to be used. The policy may include items such as retention period, update frequency, governance, sharing restrictions, or lineage.

Everyone who works for or with [Agency] has some responsibility for ensuring data is collected, stored, and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Agency may choose to list specific roles

in the policy. Some agencies choose to list responsibilities in a separate procedural document for ease of maintainability. Examples include:

- The Governing Board is ultimately responsible for ensuring that [Agency] meets its legal obligations.
- The Executive Management Team is responsible for:
  - Keeping the Governing Board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- The Systems Manager is responsible for:
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data [Agency] holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the [the Agency]'s sensitive data.
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services, the [the Agency] is considering using to store or process data. For instance, cloud computing services.
- The Communication Officer is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

8. Data Inventory

For each unique system created for or by [Agency], an inventory of all data elements required, collected and stored shall be maintained. The inventory shall include element name, description, data classification level, and data steward (by role) responsible for it and any other agency desired metadata fields. The inventory shall be kept current to coincide with system changes. The

inventory should not have any data values included but may include example data or range definitions. It shall reside in a common, shared location [location specified here].

9. Authorization and Authentication

Access to data shall be given to only those who have a business need to access it. Regular review of authorization shall occur annually or as major updates occur. Authentication to systems will be set and maintained at a level commensurate with the sensitivity level of the data within.

10. Compliance Standards

Agency may choose to list specific regulations or statutes the policy satisfies Examples include:

Example 1:

Wyoming Statute 9-21-101 requires the following aspects be included in policy:

(i) An inventory and description of all data required of, collected or stored by an agency;

(ii) Authorization and authentication mechanisms for accessing the data;

(iii) Administrative, physical and logical security safeguards, including employee training and data encryption;

(iv) Privacy and security compliance standards;

(v) Processes for identification of and response to data security incidents, including breach notification and mitigation procedures;

(vi) In accordance with existing law, processes for the destruction and communication of data.

Example 2:

[HIPAA Regulation X] describes how organizations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. [LAW] is underpinned by seven important principles, that data:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant, and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.

11. Data Security Incident Process

Most agencies have a separate breach policy and a recommendation for this policy is to merely reference it by name/number.

[Agency] shall follow [Agency Data Breach policy X]

12. Data Destruction

[Agency] will only dispose of data and records in accordance with the requirements of the state and federal government legislative instruments, including State Policy 09400-P221 [list other statutes and policies]. The destruction of data may be registered in the approved process and will be managed centrally through the [Role] who will maintain a register of such. Data must not be destroyed if it is, or may be, the subject of a subpoena, or other formal request for access or relate to any ongoing action such as an appeal, regardless of whether the minimum statutory retention period has expired.

13. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely should be directed to the Manager or supervisor. When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be evaluated regularly, in line with the [Agency]'s standard backup procedures.

• Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

• All servers and computers containing data should be protected by approved security software and a firewall.

The agency may have revision and/ or review dates as a footer to the policy.
[Version Change Description] [Date] [Author]