Data Security and Access Policy Development Packet

Data security and access is making sure that data are protected from unauthorized access and defining who may access the data. To protect and safeguard Part C and Part B 619 data, programs should develop and implement policies that address how these data are secured (i.e., making sure that data are protected from unauthorized access) and who may access the data. These policies guard data from loss, corruption, breach, and other compromises such as unintended access. Please see the DaSy Data Governance and Management Toolkit for more information on Data Security and Access Policies and other data governance policies.

How to Use This Packet

1. Review and Complete the Considerations Worksheet for Data Security and Access Policy

The considerations include questions about general policy implementation and the procedures associated with work covered by this policy. A team knowledgeable about this content and the procedures should convene to discuss these considerations. The team assembled should, include but not necessarily be limited to relevant and knowledgeable Part C or Part B 619 staff. (Others might include, IT, broader data governance committee members, etc.)

Each lettered consideration in this worksheet references a corresponding number in the Data Security and Access Policy Template. Consideration-specific notes should be captured on this worksheet and be used to refine the applicable section of the Data Security and Access Policy Template. After reflection and discussion by the team, a Part C or Part B 619 program may opt to exclude consideration content in their final policy.

1. Use Responses to the Considerations to Complete the Data Security and Access Policy Template

The Data Security and Access Policy Template is a fully modifiable document so that the resulting policy can be adapted to align with other states policies. Where appropriate, some basic content is included in the template; however, the content can and should be edited, added to, or deleted so the resulting policy accurately reflects the Part C or Part B data governance in this area. It may also be helpful to add links to policies referenced within the template.

The Data Security and Access Policy Template has 12 sections and there are one or more considerations that relate to each section. Sections vary in their depth and complexity, but all are important to fully describe the policy and the data governance and procedures covered by the policy. Each numbered section in this template references a corresponding letter in the Considerations Worksheet for Data Security and Access Policy. Once the policy is completed, there is no need to keep the lettered cross references to the associated considerations.

If you have questions about or would like assistance with this work, please contact: DaSy‑Center@sri.com

Considerations Worksheet for Data Security and Access Policy

| Considerations Worksheet for Data Security and Access Policy  |
| --- |
| *Considerations* | *Template Section* | *Notes/Status* | *Draft Language* |
| 1. Which, if any, federal laws/regulations (IDEA and FERPA) related to data security and access apply to the Part C or Part B 619 program?
 | 1.1 | *See policy template for draft language.*  |  |
| 1. What, if any, additional state agency policies related to data security and access apply to the Part C or Part B 619 program?
 | 1.2 |  |  |
| 1. What specific Part C or Part B 619 policies or procedures, if any, exist and apply to data security and access?
 | 1.3 |  |  |
| 1. When did/does this policy take effect?
 | 2 |  |  |
| 1. Which Part C or Part B 619 role should be contacted for more information on this policy?
 | 3 |  |  |
| 1. How frequently will this policy be reviewed and, if needed, updated?
 | 4.1 |  |  |
| 1. What mechanisms will be used to collect user and other stakeholder input for consideration in the review and possible revisions to this policy?
 | 4.2 |  |  |
| 1. Where can the public access this policy?
 | 5.1 |  |  |
| 1. How will interested members of the public be informed of this policy?
 | 5.2 |  |  |
| 1. What parties (including participating agencies) will be required to follow this policy?
 | 6 |  |  |
| 1. What is the purpose of the Data Security and Access Policy?
 | 7 | *See policy template for draft language.* |  |
| 1. What is the definition of data security and access?
 | 8 | *See policy template for draft language.* |  |
| 1. What data systems and data reported from these systems are covered by this Data Security and Access Policy?
 | 9 |  |  |
| 1. Which role is responsible for establishing and managing policies and procedures related to this policy?
 | 10.1 |  |  |
| 1. Which role is responsible for monitoring adherence to this policy?
 | 10.2 |  |  |
| 1. Which role is responsible for addressing questions regarding this policy?
 | 10.3 |  |  |
| 1. Which role is responsible for securing or providing training and technical assistance on data security and access?
 | 10.4 |  |  |
| 1. Which role is responsible for addressing failures to adhere to this policy?
 | 10.5 |  |  |
| 1. Which role is responsible for receiving reports of violations of this policy within the agency?
 | 10.6 |  |  |
| 1. Which role is responsible for ensuring the protection and security of data, including security measure, type, and testing and revision schedule?
 | 11.1.1 |  |  |
| 1. Which role is responsible for maintaining a list of all computer equipment and devices that access and store PII?
 | 11.1.2 |  |  |
| 1. Which role is responsible for assessing and auditing the system to identify any potential security risks to the system?
 | 11.1.3 |  |  |
| 1. Which role is responsible for identifying and managing permissions and restrictions for access to data?
 | 11.2.1 |  |  |
| 1. Which role is responsible for responding to internal and external requests for data system access?
 | 11.2.2 |  |  |
| 1. Which role is responsible for ensuring that staff and external requestors have access to the minimum amount of data needed to complete his/her job?
 | 11.2.3 |  |  |
| 1. Which role is responsible for determining that data sharing agreements are in place to ensure that protected data is guarded from unauthorized disclosure?
 | 11.2.4 |  |  |
| 1. Which role is responsible for trainings to support data security and access?
 | 12.1 |  |  |
| 1. Which role is responsible for documentation to support data security and access?
 | 12.2 |  |  |
| 1. Which role is responsible for collecting user input to support data security and access?
 | 12.3 |  |  |

Data Security and Access Policy Template for
NAME OF PART C/PART B 619 PROGRAM

1. Requirements
	1. NAME OF STATE is federally required to collect and report PART C OR PART B 619 data and collects such data through data systems noted below in section 9, Policy Application. The federal requirements (statutes/regulations/rules/policies) that apply to data security and access are IDEA and FERPA regulations: (a)

Part C at 34 CFR 303.414 (a) and (b) and 300.415

Part B at 34 CFR 300.622(a) and (b) and 300.623

FERPA at 34 CFR 99.30 and 99.31

* 1. The state requirements (statutes/regulations/rules/policies) that apply to data security and access are: (b)

*(insert relevant state requirement)*

*(insert relevant state requirement)*

* 1. The PART C OR PART B 619 policies or procedures that apply to data security and access are: (c)

*(insert relevant Part C or Part B 619 policy/procedure)*

*(insert relevant Part C or Part B 619 policy/procedure)*

1. Effective Policy Date

*(insert date)* (d)

1. Point of Contact

*(insert Part C or Part B 619 role or other contact as applicable)* (e)

1. Revisions

4.1 The Data Security and Access Policy will be reviewed and updated as needed/or *(insert frequency).* (f)

4.2 PART C OR PART B 619 will collect users and other stakeholders’ input through the following mechanisms to review and revise data security and access policies and procedures. *(insert mechanisms)* (g)

4.3 Below is a listing of all policy revisions completed to date: *(insert version number, date, and associated notes)*

1. Access

5.1 The Data Security and Access Policy will be available to the public at *(insert URL).* (h)

5.2 Interested members of the public will be informed by *(insert mechanisms).* (i)

1. Relevant Parties

This policy applies to *(insert name of programs and/or agencies)* that collect, maintain, use, manage, operate, or are otherwise active in or with PART C OR PART B 619 program data regardless of format. (j)

1. Purpose

The purpose of this Data Security and Access Policy is to establish authority and a process for protecting and safeguarding PART C OR PART B 619 PII and other important data within the data system supporting the PART C/PART B 619 PROGRAM NAME. (k)

1. Definition

*Data security* refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases, and websites. Data security also protects data from corruption occurring during the writing, reading, transmission, or processing of data resulting in unintended changes to the original data. Data security is the main priority for organizations of every size and type.

*Access,* in the context of security, is the privilege or assigned permission to use computer data or resources in some manner. Access may restrict the use and distribution of information, settings, and the general use of a data system.

*Personally identifiable information (PII)* as defined by FERPA regulations at 34 CFR 99.3 includes information that can be used to distinguish or trace an individual’s identity either [directly](https://studentprivacy.ed.gov/glossary#glossary-node-210) or [indirectly](https://studentprivacy.ed.gov/glossary#glossary-node-227) through linkages with other information (e.g., name, address, student ID, birthdate, social security number).(l)

1. Policy Application

The following PART C/PART B 619 PROGRAM NAME data systems are covered by this Data Security and Access Policy. (m)

| Data System | Description |
| --- | --- |
| *(data system name)* | *(description)* |
| *(data system name)* | *(description)* |
| *(data system name)* | *(description)* |
| *(insert data systems as needed)* | *(description)* |

1. Responsibilities

The table below outlines the specific responsibilities and roles related to data security and access.

| Responsibilities | Data System | Role Responsible (by data system) |
| --- | --- | --- |
| 10.1 Establish and manage procedures related to this policy. (n) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.2 Monitor adherence to this policy. (o) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.3 Address questions regarding this policy. (p) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.4 Secure or provide training and technical assistance on data requests. (q) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.5 Address failures to adhere to this policy. (r) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.6 Receive reports of violations of this policy within the agency. (s) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| *(insert other responsibilities as needed)* | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |

1. Procedures

The table below includes the procedures used to support this Data Security and Access Policy.

| Procedures | Role Responsible |
| --- | --- |
| 11.1 Data Security |  |
| 11.1.1 Ensure protection and security of data. This may include: (t)* the role responsible for implementing the security measure
* the type of security measure
* how often the measure is revised or updated
* how often the measure is tested
 | *(role responsible and security measure)**(role responsible and security measure)**(role responsible and security measure)* |
| 11.1.2 Maintain a list of all computer equipment and devices with access to or storage of PII. This may include: (u)* staff assignment
* equipment location
* inventory update frequency

(See *Data Breach Response Policy* for loss or theft of equipment.) | *(role responsible)**(role responsible)* |
| 11.1.3 Assess and audit the system in order to identify any potential security risks to the system. (v) | *(role responsible)**(role responsible)* |
| 11.2 Data Access |  |
| 11.2.1 Identify and manage permissions and restrictions for access to data. (w) | *(role responsible)**(role responsible)* |
| 11.2.2 Respond to internal and external requests for data system access. (x) | *(role responsible)**(role responsible)* |
| 11.2.3 Ensure that staff and approved external requestors have access to the minimum amount of data needed to complete his/her job. (y) | *(role responsible)**(role responsible)* |
| 11.2.4 Determine that data sharing agreements or other appropriate procedures are in place to ensure that protected data is guarded from unauthorized disclosure. (z) | *(role responsible)**(role responsible)* |
| *(insert additional responsibilities as needed)* | *(role responsible)**(role responsible)* |

1. Responsibilities for Supporting Data Security and Access Policy

The table below includes the roles responsible for the tools and supports for this Data Security and Access Policy.

| Tool/Support  | Role Responsible  | Location  |
| --- | --- | --- |
| 12.1 Training(s) that support this policy. (aa) *(Training 1 name and description)* *(Training 2 name and description)* *(Include all trainings)*  | *(role responsible)* *(role responsible)*  | *(insert URL training location)*  |
| 12.2 Documentation that supports this policy. (bb) *(Document 1 name and description)* *(Document 2 name and description)* *(Include all documents, including any applicable forms or reports)*  | *(role responsible)* *(role responsible)*  | *(insert URL or document location)*  |
| 12.3 User input that is collected and used to support this policy. (cc) *(User input 1 description of input)* *(User input 2 description of input)* *(Include all user inputs)*  | *(role responsible)* *(role responsible)*  | *(insert URL or location with applicable content)*  |
| *(insert additional tools/supports as needed)* | *(role responsible)* | *(insert URL or location with applicable content)*  |