DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

Data Security and Access

Overview

Part C and Part B 619 programs collect and maintain large amounts of data, including **personally identifiable information (PII)**, on the children and families they serve. To protect and safeguard Part C and Part B 619 **PII** and other important 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. Securing data and limiting access guard data from loss, corruption, breach, and other compromises such as unintended access.

Policies supporting *data security* outline the purpose and requirements of data protection and the roles and responsibilities needed to maintain secure Part C and Part B 619 data. Data security encompasses the technical processes and actions associated with preserving data existence and **integrity**.

> ***Definition***
> Data Security: 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. Data security is the main priority for organizations of every size and type.
> **Access:** 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.
> Source: **Techopedia**

Policies supporting *data access* establish processes for managing access to Part C and Part B 619 data. These are the technical approaches to limiting data access, including differentiated access, to all those with a legitimate need for the data—in some cases other data systems—based on agency, role, established agreements, and the like. Policies should describe procedures in detail and, where applicable, refer to federal and state laws and regulations.

Whether Part C and Part B 619 programs are considering developing new data security and access policies or are revisiting existing policies, it is important to review **relevant federal and state agency regulations** related to data security and access.

Part C and Part B 619 programs operate within the state agency in which they are housed. Thus, the structure and content of any **data governance** *already within an agency* is of particular importance. Before developing a data security and access policy, Part C and Part B 619 programs should review any policies regarding data security and access developed by the agency in which their program resides. Existing policies might need to be updated with specific references or provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language for this purpose.

Where no policy on data security and access exist or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new data security and access policies.

The *DaSy Data System Framework* defines both data security and access and emphasizes the importance of both in the **Data Governance** and **Management** section, Quality Indicator **DG6**, **DG7**, and **DG8**.

Considerations

Use the questions below to discuss, consider, and develop a comprehensive data security and access policy. Where appropriate, procedures and operational manuals that detail specific actions supporting implementation of this policy should be created.

1. Data Security and Access Policy: General Provisions

a. What federal laws/regulations (e.g., IDEA/**FERPA**) related to data security and access apply to the Part C or Part B 619 program?

b. Are there additional state agency policies related to security and data access that apply to your Part C or Part B 619 program? If yes, what are they?

c. What specific Part C or Part B 619 data security and access policies or procedures, if any, exist and apply?

d. What established data sharing agreements, if any, pertain to support data access and data security?

e. Which participating agencies, if any, will be required to follow this policy and under what mechanisms (e.g., contracts, subgrants, or interagency agreements)?

f. Which role, within what agency/program should be contacted with questions about this policy?

g. Which role, within what agency/program is responsible for ensuring adherence to this policy?

h. Which role, within what agency/program is responsible for monitoring adherence to this policy, and how will the monitoring be conducted?

i. Which role, within what agency/program is responsible for managing the implementation of this policy including provision of training and technical assistance?

j. What consequences, if any, will apply when this policy is not followed?

k. How often will this policy be reviewed for necessary revisions?

l. How will the public be informed about this policy? Where will it be posted on the state's website?

2. Data Security and Access Policy: Security

a. What technical security measures (e.g., firewalls, secure laptops, password, **management**, etc.) will be used to secure the Part C or Part B 619 data?

b. What nontechnical security measures will be used to increase data security? For example:

   i. Data access and sharing restrictions

   ii. Regular staff trainings

iii. Ensuring correct access and administrative rights are granted for staff and authorized data **users**

c. Under what circumstances should a security assessment or audit be conducted and security risks be evaluated? Which role, within what agency/program conducts the security assessment?

d. Does the organization maintain a current inventory of all computer equipment, **software**, and data files associated with Part C or Part B 619 data? Where is this located?

e. Have data records been classified in accordance with the level of risk for **disclosure** of **PII**?

3. Data Security and Access Policy: Access

a. How are **users** approved for and assigned access? How and when is this access terminated?

b. What methods are used to restrict authorized **users'** access to the minimum amount of data needed to complete their job duties?

c. Which role, within what agency/program is responsible for maintaining system access controls in coordination with the **IT team**?

d. What privacy, confidentiality, and data protection trainings exist for individuals with access to data?

e. What policies are in place to guide decisions about data exchanges and reporting, including sharing data (either in the form of individual records containing **PII** or as de-identified aggregate reports) with educational institutions, researchers, policymakers, parents, third-party contractors, and the like?

f. What sharing agreements or other appropriate procedures are in place to ensure that protected data are guarded from unauthorized **disclosure**, once the **users** are provided access?

g. Where are the records maintained that document the access and denial requests for data? Which role, within what agency/program oversees the maintenance of these records?

When analyzing the privacy and confidentiality requirements for children with disabilities, it is critical to begin by examining the IDEA requirements first. If you or members of your staff have questions, please contact your **State Lead** in OSERS Office of Special Education Program's (OSEP) Monitoring and State Improvement Planning Division.

Data Security and Access Policy Template

Use, and modify as needed, the template linked below for developing a data security and access policy. Select the highlighted text and replace with your state/program information. We recommend that you consult with relevant staff and **stakeholders** when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Data Governance Data Security and Access Policy

This page intentionally left blank

Data Security and Access Policy Template

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Security and Access Policy

NAME OF PART C/PART B 619 PROGRAM

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.

DEFINITIONS

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

AUTHORITY

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 in the table below. The following federal (AND POTENTIALLY NAME OF STATE) requirements (statutes/regulations/rules/policies) apply to data security and access:

Federal regulations are IDEA regulations for Part C at 34 CFR 303.414(a) and (b) and Part B at 34 CFR 300.622(a)

The NAME OF STATE statute, regulations, and current policies that address data security and access are:

- RELEVANT STATE STATUTE
- RELEVANT STATE REGULATIONS/RULES
- RELEVANT STATE POLICIES

RESPONSIBILITY

It is the responsibility of AGENCY, PROGRAM, ROLE, ETC. overseeing the data for the PART C/PART B 619 PROGRAM NAME to establish and carry out those processes associated with data security and access to PART C/PART B 619 PROGRAM data systems. The following PART C/PART B 619 PROGRAM NAME data systems are covered by this data security and access policy.

PART C/PART B 619 PROGRAM NAME Data System(s)

1. *(insert name of data system)*
2. *(insert name of data system)*
3. *(insert name of data system)*
4. *(insert name of data system)*
5. *(insert name of data system)*
6. *(insert name of data system)*

AGENCY, PROGRAM, ROLE, ETC. is responsible for ensuring adherence to this policy in PART C/PART B 619 PROGRAM data systems. Further, AGENCY, PROGRAM, ROLE, ETC. is responsible for monitoring adherence to these processes, identifying the timing and method for such monitoring to occur.

This policy will be reviewed ANNUALLY, BI-ANNUALLY, AS NEEDED by AGENCY, PROGRAM, ROLE, ETC. and they will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC. and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy.

AGENCY, PROGRAM, ROLE, ETC. is responsible for monitoring adherence to this policy through REVIEW OF DATA QUALITY REPORTS, REVIEW OF DATA QUALITY ISSUES REPORTED, ETC. Any questions data quality will be addressed by AGENCY, PROGRAM, ROLE, ETC. AGENCY, PROGRAM, ROLE, ETC. who will also secure or provide training and technical assistance on data quality when requested. This policy will be reviewed ANNUALLY, BI-ANNUALLY, AS NEEDED by AGENCY, PROGRAM, ROLE, ETC. and they will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC. and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy.

The public will be informed about this policy through AGENCY WEBSITE, MANUAL, ETC..

APPLICABILITY

This policy applies to those who collect, maintain, use, manage, operate, or are otherwise active in the control of data regardless of format. This includes staff from NAME OF LOCAL PROGRAMS/AGENCIES directly associated with NAME OF PARTICIPATING AGENCY(IES). All local programs, agencies, contractors, and staff identified in this policy must adhere to this policy. These entities and the mechanism (regulation/contract/interagency agreement) that make this policy applicable to each program/agency are listed in the table below.

Entities Covered by Policy	Mechanism
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*

Entities Covered by Policy	Mechanism
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*

SECURITY OF DATA

The table below describes the technical security measures used by the PART C/PART B 619 PROGRAM DATA SYSTEM to ensure protection and security of PART C/PART B 619 PROGRAM data including the type of security measure, the entity responsible for implementing the security measure, how often the measure is revised or updated, and how often the measure is tested.

Security Measure	Responsible Entity for This Security Measure	How Often Reviewed/Updated?	How Often Tested (if applicable)
EXAMPLE: Anti-virus Software	*Information Technology*	• *Updates pushed out weekly* • *Yearly License*	*Monthly*

In addition to the above measures, several nontechnical security measures are used to increase data security, including:

- Equipment inventories – a list of all computer equipment and devices which access or store PII can be found INSERT LOCATION. This inventory is updated TIMEFRAME by AGENCY, PROGRAM, ROLE, ETC.. Any loss or theft of equipment should be reported immediately to AGENCY, PROGRAM, ROLE, ETC. and data breach response actions shall be instituted, if applicable (see Data Breach Response policy).
- Security assessments – assessments and audits need to be conducted by AGENCY, PROGRAM, ROLE, ETC. on a TIMEFRAME in order to identify any potential security risks to the system.
- Trainings on confidentiality, data access, and data sharing restrictions for both new staff and refresher trainings conducted by AGENCY, PROGRAM, ROLE, ETC..
- OTHER MEASURES (LEVEL OF RISK CLASSIFICATION FOR DATA, ETC.)

DATA ACCESS

Permissions and restrictions for access to PART C/PART B 619 PROGRAM DATA are managed by AGENCY, PROGRAM, ROLE, ETC.. AGENCY, PROGRAM, ROLE, ETC. will be responsible for:

- Responding to requests for data system access (see below)
- Responding to access requests within TIMEFRAME from receiving the EMAIL, REQUEST FORM, ETC..
- Ensuring that staff have access to the minimum amount of data needed to complete his/her job duties through user roles or other mechanism

- Identifying various levels of access to restrict authorized users' access

Identified sharing agreements or other appropriate procedures for all PART C/PART B 619 PROGRAM DATA are in place to ensure that protected data is are guarded from unauthorized disclosure.

- LIST OTHER RESPONSIBILITIES
- Staff Training for privacy, confidentiality, and data protection issues are the responsibility of AGENCY, PROGRAM, ROLE, ETC. and are offered INSERT TIMEFRAME.

Steps To Request Data System Access

The following steps are required to request access to the PART C/PART B 619 PROGRAM DATA SYSTEM:

1. Access requests are made to AGENCY, PROGRAM, ROLE, ETC. via EMAIL, REQUEST FORM, ETC. and are to contain the following information, NAME, TITLE/ROLE, EMAIL, PHONE NUMBER, SUPERVISOR NAME, SUPERVISOR CONTACT INFORMATION, SUPERVISOR APPROVAL, REASON FOR ACCESS, ETC..
2. AGENCY, PROGRAM, ROLE, ETC. confirms supervisor approval via EMAIL, REQUEST FORM, ETC..
3. AGENCY, PROGRAM, ROLE, ETC. determines the level of access/permission needed based on staff role and data access needs as outlined in EMAIL, REQUEST FORM, ETC..
4. Notification of approval or denial will be sent by AGENCY, PROGRAM, ROLE, ETC. via EMAIL, REQUEST FORM, ETC.. Denials of access should be accompanied by the reason(s) for denial. Access requests and resulting permissions/denials are located LOCATION WHERE ACCESS REQUESTS ARE STORED and are maintained by AGENCY, PROGRAM, ROLE, ETC..

NOTE: Requests for access to PART C/PART B 619 PROGRAM DATA by others not covered by this data security and access policy are addressed in the PART C/PART B 619 PROGRAM data request policy.