

# 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)* |
| 1. *(insert name of data system)* |
| 1. *(insert name of data system)* |
| 1. *(insert name of data system)* |
| 1. *(insert name of data system)* |
| 1. *(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 SECURITY REPORTS, REVIEW OF DATA SECURITY ISSUES REPORTED, ETC. Any questions about data security will be addressed by AGENCY, PROGRAM, ROLE, ETC. AGENCY, PROGRAM, ROLE, ETC. who will also secure or provide training and technical assistance on data security 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)* |
| *(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.