Data Breach Response Policy Development Packet

Data breaches are not the concern of just information technology (IT) staff; they are the concern of everyone who has access to and handles Part C or Part B 619 data. A data breach response policy establishes a set of procedures to be followed in the event of a data breach: how and when the breach should be reported to authorities; how and when to inform the public, especially those at risk because of the data breach; recommendations to the public to reduce the post-breach risk; sanctions the agency might consider if warranted; and strategies to minimize future risk of a breach. Please see the DaSy Data Governance and Management Toolkit for more information on Data Breach Response Policies and other data governance policies.

How to Use This Packet

1. *Review and Complete the Considerations Worksheet for Data Breach Response 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 Breach Response Policy Template. Consideration-specific notes should be captured on this worksheet and be used to refine the applicable section of the Data Breach Response 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 Breach Response Policy Template*

The Data Breach Response 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 Breach Response 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 Breach Response 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 Breach Response Policy

| Considerations Worksheet for Data Breach Response Policy  |
| --- |
| *Considerations* | *Template Section* | *Notes/Status* | *Draft Language* |
| 1. Which, if any, federal laws/regulations (IDEA and FERPA) related to data breach apply to the Part C or Part B 619 program?
 | 1.1 | *See policy template for draft language.*  |  |
| 1. What, if any, state agency policies related to data breach 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 breaches?
 | 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 Breach Policy?
 | 7 | *See policy template for draft language.* |  |
| 1. What is the definition of data breach?
 | 8 | *See policy template for draft language.* |  |
| 1. What data systems and data reported from these systems are covered by this Data Breach Policy?
 | 9.1 |  |  |
| 1. What data elements are specifically excluded from this policy?
 | 9.2 |  |  |
| 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 breaches?
 | 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 reporting a data breach or a potential data breach?
 | 11.1 |  |  |
| 1. Which roles are responsible for confirming and/or stopping a data breach?
 | 11.2 |  |  |
| 1. Which role is responsible for convening the Data Breach Response Team to consider options for informing individuals potentially at risk and, if warranted, the public at large?
 | 11.3 |  |  |
| 1. Which role is responsible for determining when and how individuals potentially at risk are to be informed?
 | 11.4 |  |  |
| 1. Which role is responsible for determining what, if any, sanctions or consequences are to be levied on those responsible for the data breach?
 | 11.5 |  |  |
| 1. Which role is responsible for reviewing the data breach and determining what and when procedures shall be taken to prevent or minimize the risk of similar data breaches in the future?
 | 11.6 |  |  |
| 1. Which role is responsible for trainings to support data breach response?
 | 12.1 |  |  |
| 1. Which role is responsible for documentation to support data breach response?
 | 12.2 |  |  |
| 1. Which role is responsible for collecting user input to support data breach response?
 | 12.3 |  |  |

Data Breach Response 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 collect such data through data systems noted below in section 9, Policy Application. All reasonable efforts are required to secure and protect the integrity and confidentiality of certain information the agency possesses. In the event of a data breach, the established requirements below are to be followed. (a)
	2. The state requirements (statutes/regulations/rules/policies) that apply to data breach 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 breach 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 Breach Response 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 breach response 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 Breach Response 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 NAME OF PROGRAMS AND/OR AGENCIES, staff, vendors, and contractors that collect, maintain, manage, operate, or are otherwise active in the control of NAME OF DATA TYPE(S) that if breached would trigger a notification. This may include staff from NAME OF LOCAL PROGRAMS. If such local programs are named, all such programs must adhere to this policy including actions listed below in response to a data breach. (j)

1. Purpose

The purpose of this Data Breach Response Policy is to establish authority and procedures for responding to any PART C/PART B 619 PROGRAM NAME data breach that may occur, notwithstanding the reasonable efforts to prevent such a breach. (k)

1. Definition

*Data breach* is “any instance of an unauthorized release of or access to personally identifiable information (PII) or other information not suitable for public release” that the PART C/PART B 619 PROGRAM NAME collects, maintains, manages, operates control over, and/or otherwise oversees.[[1]](#footnote-2) A data breach may include the following:

* A hack or breach of security designed to protect such data
* Potential or actual violation of other federal or state data law/statute/regulation/rule/policy
* Theft or loss of hardware and/or software designed to house and protect data
* Unauthorized duplication of data
* Unauthorized dissemination
* Unauthorized data viewing
* Accidental release of data
* Accidental (unsecured) access to data

*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

9.1 This Data Breach Response Policy applies to and includes the Part C/Part B 619 data elements and/or categories noted below, housed in the data systems noted below, which are collected, maintained, managed, operated, or otherwise controlled by PART C/PART B 619 PROGRAM NAME, within AGENCY NAME(S). (m)

| Data Elements/Categories | Data System | Data System Location |
| --- | --- | --- |
| *(data element**/category)* | *(data system name)* | *(location)* |
| *(data element/category)* | *(data system name)* | *(location)* |
| *(data element/category)* | *(data system name)* | *(location)* |
| *(insert data elements/categories as needed)* | *(data system name)* | *(location)* |

* + 1. This Data Breach Response Policy also specifically excludes the PART C/PART B 619 data elements noted below: (n)

| Data Elements/Categories | Data System |
| --- | --- |
| *(data element/category)* | *(data system name)* |
| *(data element/category)* | *(data system name)* |
| *(data element/category)* | *(data system name)* |
| *(insert data elements/categories as needed)*  | *(data system name)* |

1. Responsibilities

The table below outlines the specific responsibilities and roles related to data breach response.

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

| Procedures  | Role Responsible  |
| --- | --- |
| 11.1 Report a data breach or potential data breach immediately. (u) | *All covered by this policy* |
| 11.2 Confirm data breach. If confirmed, take all necessary actions to stop breach. (v) | *(role responsible)* *(role responsible)*  |
| 11.3 Convene GROUP, COMMITTEE, ETC. as soon as possible to consider all options of informing both individuals potentially at risk based on the breached data and, if warranted, the public at large. (w) | *(role responsible)* *(role responsible)*  |
| 11.4 Determine when and how individuals potentially at risk based on the breached data and/or the public at large are to be informed. (x)  | *(role responsible)* *(role responsible)*  |
| 11.5 Consider and determine what, if any, sanctions or consequences are to be levied on those responsible for the data breach including but not limited to discussing the circumstances, formal reprimand, administrative leave, dismissal, criminal charges, etc. (y) | *(role responsible)* *(role responsible)*  |
| 11.6 Review the data breach and determine what and when procedures shall be taken to prevent or minimize risk of similar data breaches in the future. (z) | *(role responsible)* *(role responsible)*  |
| *(insert additional procedures as needed)* | *(role responsible)*  |

1. Responsibilities for Supporting Data Breach Response Policy

The table below includes the roles responsible for the tools and supports for this Data Breach Response 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) (insert all* training(s)  | *(role responsible)* *(role responsible)*  | *(URL training location)*  |
| 12.2 Documentation that supports this policy. (bb) *(Document 1 name and description) (Document 2 name and description) (insert all documents, including any applicable forms or reports)*  | *(role responsible)* *(role responsible)*  | *(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) (insert all user inputs)*  | *(role responsible)* *(role responsible)*  | *(URL or location with applicable content)*  |
| *(insert additional tools/supports as needed)* | *(role responsible)* | *(URL or location with applicable content)*  |

1. <http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf> [↑](#footnote-ref-2)