Data Breach Response Policy for  
NAME OF PART C/PART B 619 PROGRAM

# PURPOSE

The purpose of this data breach policy is to establish authority and a framework for responding to any data breach that may occur, notwithstanding the reasonable efforts to prevent such a breach.

# BUSINESS CASE

Federal (AND POTENTIALLY NAME OF STATE) laws require reasonable efforts to secure and protect certain information that the agency possesses, thereby protecting the integrity and confidentiality of any such maintained information. (1a)

# DEFINITIONS

For purposes of this policy, a 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-1)

A data breach may occur from but is not limited to unauthorized data copying, unauthorized dissemination, system hacking, unauthorized data viewing, loss of physical data (e.g., loss of laptop computer, flash drive), accidental release of data, and accidental (unsecured) access to data. (3)

# SCOPE

1. Various federal (AND POTENTIALLY NAME OF STATE) laws (statutes/regulations/rules/ policies) apply to security and breach situations depending on the data to be protected. (2) The NAME OF STATE statutes that address a breach of information security are
   * 1. RELEVANT STATUTE 1
     2. RELEVANT STATUTE 2
     3. RELEVANT STATUTE 3
2. This data breach response policy applies and includes these NAME OF DATA TYPE(S), which are collected, maintained, managed, operated, or otherwise controlled by PART C/PART B 619 PROGRAM NAME, WITHIN AGENCY NAME(S). (1b)
3. This data breach response policy also specifically excludes
   * 1. NAME OF DATA TYPE 1
     2. NAME OF DATA TYPE 2
     3. NAME OF DATA TYPE 3
     4. NAME OF DATA TYPE 4
4. This data breach response policy applies to WHO IS COVERED BY POLICY – STAFF, PARTICIPATING AGENCIES, VENDORS, CONTRACTORS, ETC., that collect, maintain, manage, operate, or are otherwise active in the control of NAME OF DATA TYPE(S) that if breached would trigger notification. This may include staff from NAME OF LOCAL PROGRAMS directly associated with NAME OF PARTICIPATING AGENCY(IES). If such local programs are named, all such programs must adhere to this policy including actions listed below in response to a data breach. (1d, 1e)

# RESPONSIBILITY

1. Anyone observing what appears to be a data breach, including a breach of security designed to protect such data, potential or actual violation of other federal or state data law/statute/regulation/rule/policy, theft of hardware and/or software designed to house and protect data, unauthorized duplication of data, or any action placing the state or state resources at risk pursuant to this data breach policy, must immediately report the incident to an appropriate-level supervisor, manager, or security officer within their organization.
2. ROLE, GROUP, COMMITTEE, ETC is responsible for informing and ensuring that staff follow the intent of this policy and adhere to all related procedures including the provision of training and technical assistance. ROLE, GROUP, COMMITTEE, ETC. is responsible for investigating and confirming any data breach. ROLE, GROUP, COMMITTEE, ETC. are charged with carrying out the actions within this data breach response policy. ROLE, GROUP, COMMITTEE, ETC. is responsible for monitoring adherence to this policy and will document such monitoring by INSERT MONITORING PROCEDURE. (2a, 2b, 2c, 2d)

# IMMEDIATE ACTIONS

In the event of a data breach, all the following actions shall be considered and those deemed applicable by ROLE, GROUP, COMMITTEE, ETC. shall be implemented:

1. As it is the responsibility of anyone COVERED BY THIS POLICY: STAFF, PARTICIPATING AGENCIES, VENDORS, CONTRACTORS, ETC., to report a data breach or potential data breach, and when such breach has been confirmed, ROLE, GROUP, COMMITTEE, ETC. shall report such breach to ROLE, GROUP, COMMITTEE, ETC., including all appropriate agency heads and the AGENCY DIRECTOR. (2a, 3a)
2. Any confirmed breach shall be reported immediately. (3b)
3. GROUP, COMMITTEE, ETC. shall convene 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. (3c, 3d)
4. When individuals potentially at risk based on the breached data and/or the public at large are to be informed, ROLE, GROUP, COMMITTEE, ETC. and AGENCY DIRECTOR shall determine when and how such notification shall occur. (3d, 3e, 3f, 3g)

# POST BREACH ACTIONS

After any notifications have occurred, ROLE, GROUP, COMMITTEE, ETC. shall consider and may implement any of the following post breach actions:

1. ROLE, GROUP, COMMITTEE, ETC. and AGENCY DIRECTOR shall 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. (4a)
2. ROLE, GROUP, COMMITTEE, ETC. shall 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. (4c)
3. An agency that has a security policy in place and maintains a breach response policy and procedures consistent with the requirements of NAME OF RELEVANT STATUTE(S) shall be in compliance with the requirements of this policy. (4b)

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