

Data Security Policy

References

- Effective Date: 2/3/2023
- Approved By: P20 WIN Data Governing Board

Policy Purpose

The purpose of this policy is to outline the P20 WIN data security process. The establishment of a data security policy and process will help ensure that data requestors can prepare adequately to request data, that agencies can make informed decisions for the release of data, and that data are securely transmitted, stored, and released in compliance with all applicable state laws, policies, and regulations throughout the P20 WIN information lifecycle.

Policy Statement

To fulfill the mission of P20 WIN to inform policy and practice, agencies must be able to ensure that data will be shared securely throughout the data sharing process. Data security involves people, process and technology – and involves legal, technical, procedural and physical measures to ensure security.

To set clear expectations, P20 WIN agencies will describe the critical components of data security for anyone requesting data. Requirements for data requestors will be communicated clearly and transparently to facilitate the request process.

Related Documents

Data Security Working Group Memo

Relevant federal laws:

[Privacy Act of 1974 - 5 U.S.C. 552a](#)

[Federal Educational Rights and Privacy Act \(FERPA\)](#)

[Section 303 of the Social Security Act - 20 U.S.C. 603](#)

Relevant state laws:

[Connecticut Freedom of Information Act](#)

[Connecticut Personal Data Act \(CTDPA\)](#)

Data Security Process

References

- Effective Date: 2/3/2023
- Approved By: P20 WIN Data Governing Board

Purpose

The purpose of this process is to document the steps to ensure that data shared through P20 WIN requests is securely transmitted, stored, and released.

Applicability

This process applies to all P20 WIN Participating Agencies and all P20 WIN data requestors.

Definitions

Data Requestor: Any person, entity or organization that submits a data request through P20 WIN for data from two or more Participating Agencies for legitimate state purposes.

Data Security Questionnaire: A questionnaire used to capture the capability of requestors to safeguard data in a secure environment, confirm their understanding of relevant data privacy and security laws and regulations, and agree to strict protocols regarding how the data are used.

Data Security Plan: A written plan to capture the capability of requestors to safeguard data in a secure environment, confirm their understanding of relevant data privacy and security laws and regulations, and agree to strict protocols regarding how the data are used.

Participating Agency: Any entity that has executed an enterprise memorandum of understanding for participation in the P20 WIN and has been approved for participation pursuant to the terms of that agreement.

Implementation

The following steps describe the process to be used collecting and reviewing security questionnaires and plans submitted by data requestors. The standard process is designed to cover most scenarios, but agencies can agree to variations or modifications to this process on a case-by-case basis.

- 1) The Data Governing Board will develop, and regularly review and update, a set of data security guidelines for use in the data sharing process. The guidelines will be published on the P20 WIN website and made available to any entity upon request.
 - a. The guidelines will be developed in consultation with security personnel from the participating agencies, and from the Bureau of Information Technology Services (BITS).
- 2) Prior to submitting a data request for review by all participating agencies, data requestors will be prompted to complete a Data Security Questionnaire or submit a Data Security Plan that covers the established P20 WIN data security guidelines.
 - a. If the data requestor has submitted a Data Security Questionnaire or Plan within the prior calendar year, a new questionnaire/plan will not be required.

- b. If data requestors believe significant changes have been made that will impact their risk assessment, they may submit a new Data Security Questionnaire or Plan within the same year.
 - c. OPM will provide support to requestors to complete the questionnaire or plan.
- 3) Data Requestors will complete the Data Security Questionnaire or submit a Data Security Plan. Responses to the questionnaire and Data Security Plans will be stored by OPM and included with the Data Request materials.
- 4) OPM will distribute the completed Questionnaire or Plan and other documentation to Participating Agencies to review the data request. Requestors will be informed that completed questionnaires or plans will be shared with Data Governing Board representatives for any agencies involved in the request, with OPM and with BITS, and that DGB members may choose to share within their organization as needed.
 - a. Questionnaires and Plans will not be posted publicly or shared outside the P20 WIN agencies.
- 5) Each Participating Agency involved in the data request will review the data requestor’s submitted Data Security Questionnaire or Data Security Plan to confirm if the requestor meets their data security requirements.
 - a. If a participating agency does not find the requestors responses adequate, they must provide their reasoning as well as recommendations on changes to make in order to meet the requirements.
- 6) OPM will incorporate the results of the review as part of the decision-making process for approval of a data request.
 - a. Data requestors will be notified if any agencies found they did not meet their data security requirements and provided written feedback from agencies.
 - b. Participating agencies will be notified when the updated questionnaire or plan is available and will again review the data requestor’s submitted Data Security Questionnaire or Data Security Plan to confirm if the requestor meets their data security requirements.
- 7) Agencies will indicate approval, rejection or requested revision of the overall request, consistent with the procedures outlined in the E-MOU and Data Governance Manual and will then proceed with Data Sharing Agreements for approved requests.
- 8) Agencies will then have an ability to monitor changes in data security for the requestors through regular updates to the request, as needed.

Related Documents/Attachments

Data Security Working Group Memo

Data Security Plan Guidelines

Revision History

Version	Version Date	Description of Change	Approved by
1	2/3/2023		
2	4/19/2024	Amended to include the Data Security Questionnaire and Data Security Plan	Data Governing Board