Cradle-to-Career Data System Permissions Protocol

Introduction

This document presents recommendations to the managing entity to inform the development of a Cradle-to-Career (C2C) Data System Permissions Protocol related to the P20W data set, as defined in the Participation Agreement. This document includes high-level requirements that may serve as a draft protocol outline and recommends security controls for inclusion based National Institute of Standards and Technology (NIST) Moderate Impact Controls. The Permissions Protocol should complement the managing entity's access control policy and procedures.

Permissions Protocol Requirements

The following elements are recommended for the development of the C2C Permissions Protocol:

1. The managing entity shall develop a C2C account security and identification processes, account audit processes, and account revocation processes to ensure access is provisioned in an authorized manner and uses are in accordance with the managing entity developed C2C access control policy or standard.
2. The managing entity shall employ industry standards (ex: NIST) and industry leading identity and access management (IAM) solutions; keep access control policies and procedures (which includes the permissions protocol) and implemented solutions updated; and obtain governing board advance approval for any changes to the access control policies, standards, procedures, and technology solutions.
3. Each individual provided access will be required to sign a confidentiality agreement with terms and conditions that are approved by the governing board in advance of access credentialing. Access to any portion of the P20W data set shall follow the principle of least privilege for authorized purposes, in accordance with the documentation described below.
    a. Each data provider shall determine which of its employees and contractors will have access to its data repository in accordance with its own internal policies.
    b. Each data provider must comply with the managing entity security policies in providing its employees and contractors access to the P20W data set:
        i. If the data provider internal policies conflict with managing policies, the managing policies will prevail for access to the P20W data set
        ii. Data providers will need to safeguard their credentials in compliance with both managing entity and data provider security policies (for example, approved usage of solutions like Lastpass for credential safekeeping)
    c. The Participation Agreement between the data providers and the managing entity shall reference documents including:
        i. A schedule that contains the name and title of each managing entity employee and each managing entity contractor employee who will

be provided operational access, the parts of the P20W data set for which access will be granted, and the purpose of the access. The managing entity shall continually maintain/update the schedule during the term of the Participation Agreement as necessary to ensure that it is always current as staff changes are made.

ii. A schedule that contains the name and title of each data provider employee and each data provider contractor employee who will be provided operational access, the parts of the P20W data set for which access will be granted, and the purpose of the access, necessary to support the regular and ongoing operation of the P20W data set. The managing entity shall continually maintain/update the schedule during the term of the agreement as necessary to ensure that it is always current as staff changes are made.

iii. Any data provider may object to any particular individual's access to the data that the data provider contributed. Such objection may occur at any time and the managing entity shall defer to and implement such objections immediately upon written notice from the data provider. Such objection shall not restrict such individuals to parts of the system that do not contain the data provider's data contributions.

4. Each Business Use Case Proposal (BUCP) issued pursuant to the Master Data Exchange Agreement or Interagency Data Exchange Agreement shall identify each individual (employee or contractor) who is authorized to have access to the data that is the subject of the BUCP.
5. Each executed legal agreement with an entity that is not a signatory to the Participation Agreement shall identify each individual (employee or contractor) who is authorized to have access to the data that is the subject of the agreement.
6. Each parent and/or guardian of a minor and each adult individual represented in the P20W data set will not have access to the underlying data, but upon request, that will be provided with information about what is stored in the P20W data set about their child or themselves, as required by FERPA.

Policy Examples

To assist the managing entity in developing the protocol, the workgroup recommends a review of existing California and federal access control policies and procedures that would also govern the P20W data set. Relevant requirements from NIST Special Publication 800-53 (Rev. 4) are provided as a framework below.

AC-1 Access Control Policy and Procedures

- The governing board, data providers, and the managing entity are required to coordinate and implement necessary controls for providing authorized access and preventing unauthorized access to Cradle-to-Career IT resources and data on the basis of business and security requirements.

- Periodic reviews of this policy shall be performed and documented at least within every three years, or when there is a significant change.
- Periodic review of access control procedures shall be performed at least annually.

Below are additional NIST Moderate Impact Controls (strikeouts demonstrate NIST High Impact controls) that will be implemented by the managing entity per the data security framework:

AC-2 Account Management
AC-3 Access Enforcement
AC-4 Information Flow Enforcement
AC-5 Separation of Duties
AC-6 Least Privilege
AC-7 Unsuccessful Login Attempts
AC-8 System Use Notification
~~AC-9 Previous Login (Access) Notification~~
~~AC-10 Concurrent Session Control~~
AC-11 Session Lock
AC-12 Session Termination
~~AC-13 Supervision and Review~~
AC-14 Permitted Actions Without Identification or Authentication
~~AC-15 Automated Marking~~
~~AC-16 Security Attributes~~
AC-17 Remote Access
AC-18 Wireless Access
AC-19 Access Control for Mobile Devices
AC-20 Use of External Information Systems
AC-21 Information Sharing
AC-22 Publicly Accessible Content
~~AC-23 Data Mining Protection~~
~~AC-24 Access Control Decisions~~
~~AC-25 Reference Monitor~~