Hawai‘i Data eXchange Partnership

Security and Privacy Plan

June 22, 2021
# Table of Contents

- **Introduction** ................................................................................................................................................... 2  
- **Data Access and Use** ..................................................................................................................................... 2  
  - Federal and State Statutes, Regulations, Policies, Procedures, and Guidelines ........................................ 2  
  - Personally Identifiable information .............................................................................................................. 3  
    - Maintaining the Confidentiality of Individual Information ......................................................................... 3  
- **Employee Rules and Procedures** ................................................................................................................... 4  
- **Authentication** ............................................................................................................................................... 6  
- **Security Standards:** ........................................................................................................................................ 6  
- **Destruction of Data** ......................................................................................................................................... 8  
- **Reviewers** ...................................................................................................................................................... 9  
- **Appendix A – Encryption Methods and Protocols** ......................................................................................... 1
Introduction

The Hawai‘i Data eXchange Partnership (“DXP”) is a partnership of five state agencies: the Hawai‘i State Department of Education, Hawai‘i State Department of Health, State of Hawai‘i Department of Human Services, State of Hawai‘i Department of Labor and Industrial Relations, and University of Hawai‘i (each individually a “Partner” and collectively the “Partners”). Under the management of Hawai‘i P-20 Partnerships for Education (“Hawai‘i P-20”) the Partners have developed the Statewide Longitudinal Data System (“SLDS”), as Hawai‘i’s cross-agency, longitudinal education-to-workforce data system. Codified in Hawai‘i Revised Statute (“HRS”) 27-7, the SLDS supports research and program evaluation that will improve educational and workforce outcomes for Hawai‘i.

This Security and Privacy Plan (“Plan”) is intended to be reviewed and revised, particularly as industry best practices emerge over time. The Plan delineates policies and procedures that secure the confidential data that are shared with the DXP by the Partners. It also establishes protocols managed by Hawai‘i P-20 for obtaining, storing, and using data on behalf of the DXP. As the Managing Partner of the DXP, Hawai‘i P-20 has overall responsibility for the administrative, technical, and cross-sector reporting functions for the DXP. Hawai‘i P-20 staff managing the DXP (referred to as the “Data Team”) have specific, role-based access to DXP data, data warehouse, and the associated functions for analytics and technical infrastructure development and maintenance. Specific policies and procedures as outlined in this plan include: 1) system and data access; 2) data storage, use, and retention; and 3) destruction of data.

Procedures related to data misuse and data breaches can be found in the DXP Incident Response Plan.

This Plan incorporates Partners’ security policy and procedures that concern the protection of data. This plan may also provide appendices and/or references to Partner data security plans, if available, specific to one or more of the Partners. The University of Hawai‘i Information Technology Services (“UH ITS”) hosts DXP servers that maintain and manage DXP data; the Plan therefore links to UH ITS policies and procedures.

Data Access and Use

Federal and State Statutes, Regulations, Policies, Procedures, and Guidelines
The DXP does not permit unauthorized, inappropriate access to, or the disclosure of, education, program, or workforce records, or personally identifiable information (“PII”) pursuant to all applicable Federal and State statutes, regulations, guidelines, policies, and procedures pertaining to the confidentiality of data to protect the privacy of the individual.

Specific protections that apply to a Partner’s data are noted within their individual Memorandum of Agreement (“MOA”) for Data Sharing with Hawai‘i P-20, on behalf of the DXP. The DXP Data Governance Policy (“Policy”) requires that an agency must have an MOA with Hawai‘i P-20 in place before any data can be transferred to the DXP. This applies
for any centralized or federated data sharing. The Policy also outlines processes to protect Partner data from unauthorized access, misuse, or disclosure as well as addresses user access to the data.

Additionally, HRS Chapter 487N requires that operational procedures and systems developed and implemented shall provide contingencies to ensure that unauthorized access to PII is reported appropriately. Hawai‘i P-20 coordinates with UH ITS to comply with this statute.

**Personally Identifiable information**

DXP Partners have agreed that Social Security Numbers, credit card numbers, driver’s license, or other state approved identification numbers, and other personal financial numbers will not be stored in DXP databases. The DXP will protect any data that contain direct identifiers and other indirect identifiers –defined as sensitive data (medium risk) by UH Minimum Security Standards– though a variety of control mechanisms described throughout this Plan. Level of access to protected data will be dependent on role, data sharing need, and/or Policy controls. Identifiers include, but are not limited to: 1) full name; 2) numeric identifiers, such as full Social Security Number or student identification number; and 3) date of birth.

These data are used for identity matching and linking purposes only, except as authorized by the appropriate DXP data governance committee. Only the Data Team, with its job-related roles and responsibilities to manage DXP data, may access identified data. The Data Team has been granted DXP data privileges and is bound by the Policy and appropriate confidentiality and security agreements described later in this Plan. While Federal and State law may permit disclosure of the above-mentioned data under certain circumstances, Policy only permits the disclosure of identified data back to the original data owner, i.e., the Partner where the data originated from, and with the written request by the data owner. Output of data from the DXP to requestors will be in aggregated or in de-identified format.

Any data that requires extra protection, as determined by the DXP Data Governance and Access Committee (“DG&A”), will be stored in encrypted or hashed format. All datasets are transmitted via approved, secured protocol and are encrypted, whether in transit or at rest on a server (see Appendix A). Matching of individual records using direct identifiers as defined above is performed on servers that are not accessible to the public, or by any UH personnel without specific role-related responsibilities for DXP activities. UH ITS servers are housed in a secured physical environment, which is maintained through rigorous controls over physical and virtual access to the servers and networking equipment. Access to DXP metadata, such as the data schema is also restricted to the Data Team with role-based access to DXP data.

**Maintaining the Confidentiality of Individual Information**

The DXP utilizes various procedures and security measures to ensure the confidentiality of individual records. These procedures include the assignment of a unique DXP identifier to
each individual’s data, restricted access to data, and statistical policies and procedures regarding data handling or reporting as described in Policy.

- PII is used to link and validate records between the various Partner source data within the DXP server environment. Once the link is established, a unique DXP identifier is assigned to each record to mask individuals. These unique identifiers are computer-generated and contain no embedded meaning, nor are they based on any PII, or portions of PII.

- No identifiable, individual-level data are allowed outside of the DXP server environment (i.e., no laptops, downloads, hard drive on desktop computers, cloud storage, flash drives, etc.).

- Data may be exported to requestors in de-identified, individual-level or aggregate formats based on data sharing agreements between the DXP and individual agencies/programs, as well as approval of each specific request by the appropriate data owner.
  - For individual-level datasets, de-identified records are aligned to a unique Research ID specific to the dataset, and does not contain the DXP unique identifier. The IDs are created either using a random number of random length, generated from SQL code, Microsoft Excel/Access’s random number generator, or an additional identity column is created for a dataset so a number auto-increments into the field. All Research IDs are not based on any PII, data owner identification numbers, or the DXP unique identifier.

- For data within the SLDS, all software used to manage, manipulate, analyze, and report DXP data will be launched from and used within the UH ITS environment.

- The DXP Data Governance Coordinator maintains a list of current Data Team members who have access to any DXP data. DXP databases log data access by the individual.

**Employee Rules and Procedures**

To protect the confidentiality of DXP data, this Plan will be publicly available for all Data Team members and Partners to refer to. Data Team members will comply with the following actions:

- Execute a confidentiality agreement requiring the maintenance of the confidentiality of all PII as well as complete any privacy and confidentiality training required by Partners who contribute to DXP data stores, whether centralized or federated.

- Complete, at a minimum, the following certifications:
DXP Security and Privacy Plan

- UH Information Security Awareness Training (annual recertification).
- Any certifications required by Partners who contribute to DXP data stores.

- Follow best practices while using software to handle and analyze DXP data to ensure access to data remains secure. (e.g., when using Microsoft Access to conduct analyses using multiple sources, data should be linked in to limit exposure rather than importing it in and creating another copy of the data.)

- Understand security and privacy issues and the Data Team’s role in preventing data breaches. Data Team members will avoid actions that jeopardize the integrity and security of information technology resources.

- Use only information technology resources they are authorized to use and only in the manner and to the extent authorized. The Data Team recognizes that ability to access information technology resources and DXP data does not, by itself, imply authorization to do so. Data Team members are accountable for anything done under their DXP account, where misuse is subject to all appropriate corrective and/or disciplinary actions.

- Protect DXP assigned accounts and system authentication information, including passwords and any security tokens from unauthorized use. Data Team members will not share their account information or leave passwords or tokens in places that could be accessible by others.
  - If a user has reason to believe others have learned their passwords or their tokens, they must report the issue to their supervisor upon discovery of a compromised password and/or token. The supervisor will take appropriate action to have the passwords reset and tokens disabled and replaced.
  - Data Team members will not attempt to use the logins and passwords of others.

- Comply with applicable laws and regulations, contractual agreements, UH policies, and licensing agreements.

- Abide by the security controls on all information technology resources used for DXP business including, but not limited to, mobile and computing devices, whether UH, Hawai‘i P-20, or personally owned.

- Be responsible for the content of their personal communications which may also be subject to liability resulting from that use. The DXP accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

All offers of employment on the Data Team are subject to the results of a background check.
Authentication
Access to DXP data will be restricted to appropriate personnel by user authentication and password. Online access to DXP data by Data Team members and contractors is provided through strictly controlled user IDs and passwords. Privileged access requires Virtual Private Network (VPN) and DXP domain authentication. Domain login also involves a second factor authentication method via office or cell phone.

First Factor: VPN and domain authentication. VPN and domain access are required for privileged, secured access to DXP servers and data.

Second Factor: Log in confirmation via cell app push approval, office/cell call, or passcode via text/email.

The Data Team will follow password best practices which include, but are not limited to:
- Creating passwords that are at least 10 characters long and difficult to guess;
- Not sharing passwords;
- Not saving passwords in unsecure documents;
- Not including passwords as part of an e-mail message;
- Not creating a new password that is the same as a recently used password; and
- Not using the same password for two or more systems.

Security Standards:
Both the UH servers that host the SLDS, and the Data Team computers (endpoints) will comply with UH’s security standards listed below. The standards were selected from the Center for Internet Security's (CIS) Controls, which are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. (see https://www.cisecurity.org/controls/cis-controls-list/)

1. **Inventory and Control of Hardware Assets:** Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

2. **Inventory and Control of Software Assets:** Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

3. **Continuous Vulnerability Management:** Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

4. **Controlled Use of Administrative Privileges:** The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
5. **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**: Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

6. **Maintenance, Monitoring and Analysis of Audit Logs**: Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. Minimum 30 days retention required.

7. **Email and Web Browser Protections**: Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

8. **Malware Defenses**: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

9. **Limitation and Control of Network Ports, Protocols, and Services**: Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

10. **Data Recovery Capabilities**: The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

11. **Secure Configuration for Network Devices, such as Firewalls, Routers and Switches (DEFERRED by UH ITS)**: Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

12. **Boundary Defense**: Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

13. **Data Protection**: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

14. **Controlled Access Based on the Need to Know**: The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
15. **Wireless Access Control:** The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

16. **Account Monitoring and Control:** Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

**Destruction of Data**
The DXP will comply with State and Partner policies on how to properly dispose of data that are no longer needed.

All UH ITS storage devices are part of virtual machine environments in which data are striped across many individual drives. When mass storage devices fail or are decommissioned, they are returned to the manufacturer where they are destroyed or refurbished.
Reviewers

Per the DXP Data Governance Policy, the DXP Security & Access Sub-Committee (S&A) is tasked with, in part, developing and implementing processes for best practices in audit and monitoring for the security of DXP. The DXP Data Governance & Access Committee (DG&A) delegated authority to approve the DXP Security & Privacy Plan to S&A.

The following members of S&A have reviewed and approved this version of the Plan:

University of Hawai‘i
- Jodi Ito, Chief Information Security Officer
  Office of the VP for Information Technology & Chief Information Officer
- Melvin Quemado, Information Security Specialist
  Office of the VP for Information Technology & Chief Information Officer

Hawai‘i State Department of Education
- Hawai‘i Jonathan Chee, Director (Interim)
  Enterprise Architecture Branch

Department of Labor and Industrial Relations
- Bennett Yap, Chief
  Electronic Data Processing Systems Office

Hawai‘i State Department of Health
- Derek Vale, Health Systems Management Office Chief
  Child and Adolescent Mental Health Division

Hawai‘i Department of Human Services
- Jack Giardina, Security and Compliance Analyst
  Information Security Office

Office of Enterprise Technology Services
- Vincent Hoang, State Chief Information Security Officer

Hawai‘i P-20 Partnerships for Education (Managing Partner)
- Todd Ikenaga, System Architect

Updated and Approved by DG&A on: October 4, 2021
Appendix A – Encryption Methods and Protocols

Encryption methods:
Disk encryption: BitBlocker (password protected)
Database encryption: SQL Server encryption (certificate protected)

Approved file transfer protocols:
Secured File Transfer Protocol (SFTP)
UH File Drop (UH to UH or Other to UH)