Hawai‘i DXP Security & Privacy Plan

2017

Table of Contents

Introduction

This document is a dynamic plan of policies, structures, and procedures to secure the confidential and private data that are shared by the Hawai‘i Data eXchange Partnership (“DXP”) between Hawai‘i State agencies and affiliates. This plan establishes the protocols for obtaining, storing, and using DXP data managed by Hawai‘i P-20 Partnerships for Education (“Hawai‘i P-20”). Hawai‘i P-20 has been established as the Managing Partner with the overall responsibility of managing the administrative, technical, and cross-sector reporting functions for DXP. Hawai‘i P-20 staff have specific role-based access to DXP data and functions (“Data Team”). Specific policies and procedures as outlined in this plan include: 1) system and data access, and use; 2) data storage and retention; 3) destruction of data; and 4) incident response. There are references to Federal and State statutes and regulations that affect how DXP must securely manage its data.

Since DXP is a cooperative partnership comprised of multiple partner agencies and affiliates, this plan may also provide appendices and/or references to external data security plans, if available, specific to one or more of those agencies.

In addition, this plan has links to the University of Hawai‘i (“UH”) policies and procedures that apply to UH Information Technology Services (“UH ITS”), which hosts the servers that maintain and manage DXP data.

Data Access and Use

Federal and State Statutes, Regulations, Policies, Procedures, and Guidelines

DXP does not permit inappropriate access to, or the disclosure of, education, workforce, or any other 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.

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.
See: HRS chapter 487N

These laws and the DXP Data Governance Policy (Policy) – see http://hawaiidxp.org/files/HawaiiDXP_Data_Governance_Policy.pdf – require that all data collected by DXP be protected from unauthorized access, use, or disclosure. The Policy also addresses user access to the data.

Identifiable information

DXP will protect any data that contain direct identifiers and certain sensitive – as defined by UH Executive Policy EP 2.214 – indirect identifiers though a variety of control mechanisms described throughout this plan. Level of access will be dependent on role, data sharing need, and/or governance policy controls:

A. An individual's name;
B. Numeric identifiers, such as full Social Security Number or student number; or
C. 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 these 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 does not permit any disclosure of identified data to any individual or group within DXP or external to DXP, other than for purposes of identity matching and linking.

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.

At minimum, the following elements should be protected, pursuant to HRS chapter 487N:

1. Social security number;
2. Driver's license number or Hawai‘i identification card number; or
3. Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

Credit card numbers and other personal financial numbers are not stored in the DXP database.

All datasets are always transmitted via secure FTP or another approved, secured protocol and are encrypted, whether in transit or at rest on a server. Matching of

individual records using direct identifiers as defined above is performed on servers that are not accessible from the public internet, by any DXP partner employee, or by anyone on a UH network. UH ITS servers are housed in a secured physical environment, which is maintained through rigorous controls over physical 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 the DXP data.

Maintaining the Confidentiality of Individual Information

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

- A unique identifier is assigned to all of an individual's records in DXP, that cannot be traced back to the individual. These unique identifiers are computer-generated and contain no embedded meaning.

- No identifiable individual data are allowed outside of the DXP server environment. No identifiable individual record data are allowed flows outside of the DXP server environment (i.e., no laptops, downloads, cloud storage, etc.).
  - Any exceptions will be handled on a case-by-case basis and based on agreement between DXP and the involved data owners, as well as approval by the appropriate DXP governance committee.

- Data may be exported to requestors in de-identified or aggregate formats.
  - De-identification is the process used to prevent a person's identity from being connected with information.
  - The export of de-identified data will be based on agreement between DXP and the involved data owners, as well as approval by the appropriate DXP governance committee.

- Access to DXP data is only granted to approved users via DXP governance committee-approved applications and tools.

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

- The DXP Program Manager maintains a list of current Data Team employees who have access to any DXP data. DXP databases log data access by the individual.

Employees Rules and Procedures

- All DXP partner employees involved in DXP must sign the appropriate confidentiality and security agreements to be granted access to the Research Data Store (RDS), which houses de-identified, cleaned, formatted, and tabled data that approved users can access for research purposes.

- All Data Team employees using any individual data are provided with instructions regarding policies and procedures.

- All Data Team employees are responsible for anything done under their account and are subject to all appropriate corrective and/or disciplinary actions.

- Data Team employees will not share with others their system authentication information, including passwords and any security tokens, 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 employees will not attempt to use the logins and passwords of others, nor allow their logins and passwords to be used by others.

- As of the initial execution date of this plan, all offers of employment on the Data Team are contingent upon clear results of a thorough background check.

Account Management

Accounts to access DXP data are created only for DXP partner employees who must have cross-agency DXP data to perform their job functions or for contract employees (temporary access only) whose jobs involve the building and support of DXP infrastructure. These jobs include reporting, analyses, statistical research, Federal and State reporting, network administration, and database programming and administration. Individuals granted DXP accounts are generally data analysts, researchers, programmers, and database administrators.

The process for individual users to obtain access to DXP data is outlined below.

1) Data Team employees, all DXP partner employees involved with DXP, and those who seek access to DXP data must have signed the appropriate confidentiality and security agreements. The signed documents must be on file with the DXP Program Manager.
2) Access to DXP data will be granted only to the RDS. Access to the Operational Data Store, which contains PII, is only provided to Data Team employees whose job functions require this access.
3) A request, either in writing or via email, must be submitted to DG&A from a member of the DXP partner who supervises the work of the employee for whom the account is to be created. Each access request will be reviewed and approved by DG&A before access can occur.
4) In reviewing requests for access, DG&A shall consider situations in which it is absolutely necessary for an employee to obtain data in order to perform a particular job function.
5) Accounts that are inactive for 45 days will be disabled and terminated after 180 days.
6) Unsuccessful attempts to access servers will be logged and alerts will be triggered at a pre-determined threshold.
7) The DXP Program Manager will manage and maintain an active account/user list.

If a DXP partner employee with a DXP user account is terminated, retires, or otherwise leaves their employment with the partner, or if it is determined that the user no longer requires access to DXP, the process for terminating a user account is as follows:

1) The partner member who supervises the work of the user shall notify the DXP Program Manager, in writing or via email, to terminate the user account.
2) The DXP Program Manager will then send an account termination request to the UH ITS DXP technical support and the account will be terminated within 24 hours of receipt of the request.
3) The DXP Program Manager will remove the user and update the active account/user list.

4) Annual review of access and audit of utilization will be conducted by DG&A.

Authentication

Access to DXP data will be restricted to appropriate personnel by user authentication and password.

Online access to DXP data by Data Team employees and contractors is provided through strictly controlled user IDs and passwords. Privileged access requires Virtual Private Network (VPN) as a first factor and DXP domain or SQL authentication as the second factor.

First Factor - VPN:
Require VPN access for privileged, secured access to DXP data.

Second Factor – DXP domain or SQL authentication
Require a DXP domain or SQL account in order to access folders or databases.

- Create passwords that are difficult to guess.
- Change passwords on a regular basis.
- Do not share passwords.
- Do not save passwords in unsecure documents.
- Do not include passwords as part of an e-mail message.
- Do not create a new password that is the same as a recently used password.
- Prohibit use of the same password for two or more systems.

Acceptable Use of Resources

All DXP partner employees are required to sign and comply with the provisions of DXP's confidentiality and security agreements.

Each DXP partner may have an acceptable use policy (AUP) that specifies what an employee can do with agency technology and prohibits certain behaviors including viewing or storing pornography, pirating content, and conducting private business. The consequences of an employee violating such policies are usually defined in the AUP or in human resource policies.

- Acceptable use includes but is not limited to respecting the rights of other users, avoiding actions that jeopardize the integrity and security of information technology resources, and complying with all pertinent licensing and legal requirements.

- Users must comply with applicable laws and regulations, contractual agreements, Board of Regents and Administrative policies, and licensing agreements.

- Users must use only information technology resources they are authorized to use and only in the manner and to the extent authorized. Ability to access information technology resources does not, by itself, imply authorization to do so.

- Users are responsible for protecting their DXP assigned accounts and authentication (e.g., password) from unauthorized use.

- Users must abide by the security controls on all information technology resources used for DXP business, including but not limited to mobile and computing devices, whether DXP or personally owned.

- Users of information technology resources are responsible for the content of their personal communications and may be subject to liability resulting from that use. DXP accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

- Security Breach: In accordance with HRS section 487N-1, a security breach means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. An incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach. Any security breach that involves DXP data will follow UH policy and procedures for all notification and reporting requirements under HRS chapter 487N.

In addition, all DXP users are subject to their respective agency’s network access policies that govern attaching individual computers to the agency’s network both in and outside the workplace. These policies may apply to desktops and notebooks as well as tablets and smart phones.

- UH Infosec Policies

Software

Software changes can often result in a reduction of security. Changes include installation of new software, updates of device drivers, application of patches, modification to configuration, and physical reorganization.

DXP partners and their contractors are required to control and manage change to prevent security threats. Change management policies impose procedures to evaluate, test, and approve changes before they are allowed into a production environment.

DXP Software Practices

Installation Rights: Only network administrators have rights to install or otherwise add software to any server, desktop, or notebook system. Regular patching schedules are in place for all software, whether commercially and internally developed. Master copies of all software, licenses, and documentation are retained in a secure location and a database of licenses is maintained along with expiration and renewal schedules.

Copyright infringements: To counter possible copyright infringements caused by unlicensed software, inventories are performed on a regular basis. These comprehensive network-wide inventories include noting the product, name of the manufacturer, version number, and computer on which the software is installed. This inventory is reconciled against the DXP software license inventory to verify that no unlicensed software or software for which the DXP has inadequate licenses is installed.

Development and Change: Data Team employees regulate all custom software development and changes where the software is developed by DXP's UH technology support or a vendor under contract. All custom software is developed following a prescribed software development life cycle that includes four basic steps and environments: development, testing, staging, and production (testing and staging may be combined in some circumstances). These include separate test networks and servers where applicable. Once the modified or new copy/version of the software is thoroughly tested by the software development employees and prospective end-users, it will be deployed to a production environment. Production rather than development copies of software are

always maintained to avoid putting active applications and files at risk. All new development is done in a separate development/testing environment.

Test Servers: Initial software testing occurs on non-production servers and on a non-production network. No non-production servers are turned into production servers without being properly wiped first.

Change Requests: Before anyone modifies or creates any software, a formal, written change is submitted. Such requests result in an audit trail of artifacts and events as the request is processed.

Design Reviews: Continued feedback is expected from users during the software development process to ensure that the new or changed software will satisfy functional specifications and security requirements.

Program review: Before new or changed programs are put into production, the code changes are reviewed by at least one other person who understands the change request that initiated the new or changed code. This step precedes actual testing and is just one step in the quality assurance/quality control process.

Vulnerability checking: Program code is reviewed and tested for potential vulnerabilities, such as buffer overflows and SQL injection attacks that would make it susceptible to various software exploits.

Master files: Master files of all developed software are maintained independently of the development employees. Software belongs to the organization that employs the programmer and not the programmer. All original copies are controlled and the organization clearly guarantees this ownership. It is required that any new or modified software is tested rigorously and certified as fully operational before releasing it for general use.

Required documentation: For all new or revised programming, requisite documentation includes but is not limited to: name of the developer, name of the system, modules/objects impacted, programming languages/technologies, development/change dates, nature of the revision, and revision number.

Software Verification: Before putting the software into operation, verify that all software user functions are working properly. Check that new software meets anticipated user needs, current system requirements, and all organizational security standards. This is also applicable when upgrading software.

Application software testing: Developers never risk using live data with newly installed software. They always run sample files and/or copies of non-sensitive files through the software to verify software's integrity and proper functioning.

Installation of new software: Before installing new software or software upgrades, representative copies of the latest data files are used for testing until the new software or upgrade is proven to be running properly.

Network and Servers

- Firewalls are installed at all external access points.
- All cabling and wires are protected to the extent possible. This means they should reside in trays in cubicles or within walls or ceilings.
- All servers are secure so they cannot be booted from removable devices or their BIOSs altered with administrative access.
- Aside from DXP public web servers, all DXP user connections to DXP servers are made through a VPN.
- The Data Team has established a secure FTP server for which authentication is required, source IP confirmed, and all transmissions to and from the site are encrypted and password/certificate-protected. All files coming into or leaving the DXP network, whether or not they contain PII or otherwise sensitive information, must employ this site.
- All devices (including desktops, notebooks, tablets, and smart phones) and servers attached to any DXP partner's network must have the agency's prescribed antivirus, anti-spyware, anti-malware, and firewall software installed. All updates/upgrades to either the antivirus engine, data files (used to identify virus signatures), or other security software are automatically pushed to the individual client machines.
- Only devices approved by DXP or the appropriate DXP partner with appropriate vulnerability protections (some of which are mentioned above) are allowed to connect to the DXP domain and servers.

See:
http://www.hawaii.edu/policy/?action=viewPolicy&policySection=ep&policyChapter=2&policyNumber=210&menuView=closed

Data Storage and Retention

Retention of Structured Data (includes data that are stored in databases for analysis, reporting, and research)

- Since the primary purpose of DXP is to maintain longitudinal data over long periods of time, all DXP data will be generally retained forever unless otherwise stated in agreements. DG&A will decide which DXP data may be purged and after what period of time. Over time, some data may become obsolete and need to be permanently deleted. Some retention decisions may be driven by existing retention schedules on file at the State Archives for DXP partners' source data.

- If the Data Team takes over the production of an official State or Federal report that was once produced elsewhere, it will follow the applicable existing retention schedule on file at the State Archives for that report.

- DG&A or the appropriate DXP sub-committee will develop, maintain, and update retention schedules for any data extracts on DXP servers and non-official reports. The generally prescribed time period for such retentions for audit purposes is five years.

- Some directly identifiable DXP data that are critical for ongoing matching as new data are introduced may need to be retained past the time specified in the retention schedules of some source agencies. However, these data will continue to be securely maintained as described in this plan and inaccessible to anyone, including non-Data Team employees with approved DG&A access to conduct reporting and/or research.

- If at any point in time, the volume of data within the DXP database becomes so large that all of it cannot be economically managed as one entity, DG&A, working with UH ITS, will decide which data should be archived. Any such archived data will be cataloged and deleted when it reaches the end of its retention period.

Retention of Meta-data and Other Information

DXP has a responsibility for the retention of data and information that are not structured or hard data, which include items such as systems and project documentation as well as meeting agendas and minutes.

DXP will comply with the following retention rules.

- **Activity Monitoring Records:** Records that monitor the activities of an information/database system. These include logs, physical access, and online access. **Retention:** 1 calendar year.

- **Documentation for a Permanent Database**: Records that describe how a database system is operated. These may include records that document the development or modification of a database, which are necessary to access, retrieve, manipulate, or utilize the system. May also include user guides, system definitions, flowcharts, program descriptions, and logical relationships. This documentation only pertains to databases that are considered permanent or otherwise significant.
  Retention: Permanently retained by DXP.

Backups – DXP will employ UH ITS' comprehensive backup system

- Any backup of PII that is used only for validation and matching of data will be stored following the same security measures used for active PII data.

- DXP may use offsite storage employed by the UH ITS data center for the DXP and other mission-critical databases, if feasible. At a minimum, recovery backups will be created before and after processing cycles and whenever necessary. Offsite storage will be done as needed for disaster recovery.

- Any employee or contractor must immediately notify the system administrator/security manager when data are discovered to be, or are suspected of being, lost, stolen, or damaged.

- Since technology continually changes over time, DXP may at times need to retain old devices, backup/restore software, and other compatible software such as operating systems and databases, in storage together with the data that is stored on them.

Hardware Scope: Certain servers, as well as critical operating software for various switches, routers, and firewalls, may need to be backed up. Individual client workstations are not backed up and users are thus advised to keep all data on network servers.

Software scope: Original operating system software, along with service packs and other upgrades, are securely backed up and kept offsite.

Backup files: These require appropriate levels of security as do the master files (e.g., if the original file is confidential, so is its backup). In the case of DXP data, all database tables containing individual records are considered confidential.

OS directories/folders and the swap files on each server: Specific directories/folders on certain servers may be identified as the only backup requirement for that server. All commercially purchased and custom-developed software are also backed up and kept offsite. This includes all application software.

Backup hardware and software: Service and support agreements are in place for all backup software and hardware.

Data scope: Identified resources requiring backup includes all server-based user and group folders, reporting/analysis software, and database software. Such software may be purchased or custom-developed.

Catalogs: Catalogs are generated from the backup software which logs all backup dates and media for recoverability.

Test of backup system: In the course of normal events, the backup system is periodically tested when users ask to retrieve some data that was accidentally deleted. Restorations of full servers should also be tested. More comprehensive restorations exercises are also scheduled.

Disaster Recovery Including Co-location and Contingency Plan

DXP is not a mission-critical system and will be down in a disaster situation. At minimum, data backups will be done annually or as needed, and the latest copy will be stored offsite. Data recovery will be done when infrastructure is available.

Destruction of Data

Every organization that maintains data should have policies to properly dispose of any data that are no longer needed, regardless of storage medium and format.

- DXP will inventory files and databases to indicate the contents, their expected life cycles, and appropriate destruction dates.

- 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.

- Data in motion: All file transfers to or from the DXP infrastructure, both incoming and outgoing, will be transferred via the securely encrypted SFTP protocol. Incoming transfers will be removed from the SFTP server upon arrival and encrypted on the DXP fileserver, where they will remain encrypted until temporarily decrypted for importing into the DXP database. Decrypted files will be destroyed immediately after import, leaving only the encrypted temporary/work versions to be archived as needed, after which they will be destroyed. Outgoing files will only be placed on the SFTP server in encrypted form. Outgoing files will be destroyed on the SFTP server after confirmation from recipient.

See: HRS chapter 487R

Incident Response Plan (due to a security incident or AUP violation)

Such plans should define levels of severity and do the following:

- Minimize downtime;
- Reduce loss; and
- Improve availability, including:
  - Preparation;
  - Detection;
  - Containment;
  - Eradication;
  - Recovery; and
  - Post-mortem review.

DXP will use as guides the incident response policies established by DXP partners.

Some security breaches or unacceptable behavior may require the notification of law enforcement or other legal authorities pursuant to HRS chapter 487N. If any of the following are discovered in regards to the DXP network, the Data Team will notify the

appropriate officials: 1) Child pornography; 2) Attempts to solicit a minor; and 3) Death threats.

Human Resource Policies Related to Technology

While each DXP partner has its own human resource policies, human resource policies within any organization need to be integrated with or at least complement DXP data security and confidentiality policies. For example:

- DXP agencies may have somewhat different policies regarding monitoring of Internet access. These policies will define what information is collected, what information can be disclosed to whom, and for what reasons the information is collected.

- There will be training resources and opportunities for employees to learn about security and confidentiality policies and practices.

- In addition to training, there will be assessments to ensure employees have the proper knowledge and skills to keep data secure and confidential.

- There will be clear definitions of the consequences for violating a policy and under what circumstances (accidental, ignorance, or intentional) an employee will be disciplined and possibly terminated.

- Personnel issues must be handled through the human resource departments of the relevant agency. For example, while DXP personnel may discover and report a violation/infraction, it is up to human resources department of the relevant DXP partner to do any investigation and enforcement.

Training

Employees must be adequately prepared for making security policies a part of the work environment. Although individual DXP records are not accessible outside the server environment, aggregate data are allowed to be downloaded. Even those data may require some protection. If the proper disclosure avoidance steps (e.g., suppression of small cells) have not been taken, aggregate data may put confidentiality at risk.

- All must be adequately trained on the software used to access data.

- Everyone must have an understanding of security issues and their role in preventing data breaches.
- AUPs and parts of this plan must be kept visible throughout the workplace.
- Training should be tailored to meet the requirements of the security policy and employee needs.

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 this draft of the Plan:

- University of Hawai‘i
  - Jodi Ito, Chief Information Security Officer, Office of the VP for Information Technology & Chief Information Officer
  - Sandra Furuto, Director, Data Governance & Operations
- Hawai‘i State Department of Education
  - Christine Shaw, Interim Director, Enterprise Systems Branch
  - Jonathan Chee, Interim Director, Enterprise Architecture Branch
- Hawai‘i Department of Labor and Industrial Relations
  - Bennett Yap, Chief, Electronic Data Processing Systems Office
- Hawai‘i Department of Health
  - Derek Vale, Health Systems Management Office Chief, Child and Adolescent Mental Health Division
- Department of Human Services
  - Malia Taum-Deenik, Complaints Liaison & Legislative Coordinator
- Hawai‘i P-20 Partnerships for Education (Managing Partner)
  - Todd Ikenaga, Hawai‘i DXP Program Manager

Other reviewers:

- Office of Enterprise Technology Services
  - Vince Hoang, Chief Information Security Officer (May 23, 2017)

Adopted by the DXP Executive Committee on: _____

Future updates/revisions will be submitted to DG&A for adoption. If approved, the Executive Committee will be informed.