DLIR Policies (subject to change)

Personnel Security

PERSONNEL SCREENING

DLIR ensures an internal coordination between HR, IT, division in charge (who creates and process user authorization requests) to ensure that appropriate background checks are completed prior to providing system access to personnel joining DLIR.

The following criteria apply:

a. Conduct background screening to all individuals prior to authorizing access to the network and information systems. The level of screening depends on the nature of engagement (Full-time, contractor etc.,), level of access to the sensitive systems etc., and the same is determined by HR department.

b. Based on the discretion of State and Divisional HR procedures, periodic rescreening exercises may be performed on individuals.

c. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

PERSONNEL TERMINATION

Divisions within DLIR shall, upon termination of individual employment or contract engagements should notify Information Security at the earliest so that the Security team can plan and perform access disablement.

DLIR Information Security team performs following activities upon receiving separation notification:

a. Disable information system/network access within 1 or 2 days of termination.

b. Terminate/revoke any authenticators/credentials associated with the individual.

c. Divisional in charges are responsible to collect all security-related information system-related property and return to Information Security team for further disposition.

   Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes.

d. IT Security team will enable the retention of any data associated with the separated personnel, based on the received request from the Divisional in charge.

THIRD-PARTY PERSONNEL SECURITY

a. DLIR IT coordinates and process all user requests related to third party personnel. This may include consulting staff, vendors, temporary employees, interns.
b. DLIR requires that personnel complete acknowledgment of "Acceptable Usage Policy" (AUP

Data and Record Retention

DLIR is responsible to protect and maintain the data for an extended period as part of its services to the residents of the state. In addition, residents may be involved transacting with DLIR over multiple years apart in their lifetime, which requires DLIR to retain the data for an indefinite period. Based on certain legal guidance DLIR may impose "legal holds" on transactional data as part of its compliance obligations. DLIR follows Federal and State guidelines for governing records retention.

Backup / Recovery

DLIR Requires Adherence to best practices regarding data backup and retention considering the following factors:
Regulatory requirements
Backup Datasets, types, and frequency
Identification and validation of restoration scenarios
Ease of access to the last incremental and full backup
Backup schedules, capacity, and available bandwidth
Industry best practices

State of Hawaii Acceptable Use Policy

0103001-021323.pdf (hawaii.gov)

Data Classification

DLIR formally organizes the data under its custody into the following data classification types:

1. **Public Data** – Public domain data, press releases, Labor statistics / research data
2. **Confidential Data –** PII/PHI/PCI data
3. **Sensitive Data –** Sensitive within DLIR (financial, legal)
4. **Restrictive Data –** FTI data, SSA data

Public Data refers to any data that is collected, retained, or published by DLIR through physical and electronic sources that is devoid of any personally identifiable information. Most of such data is reflected on the DLIR public website and applications posted in labor.hawaii.gov, research, statutes, and forms. In addition, any information posted by DLIR on the social media is also considered as public data.

Confidential Data refers to any data that is under DLIR's custody, however, contains Personally Identifiable Information such as SSN, Bank ACH information and Payment Card Industry (PCI) data, electronic Health information (PHI) data.

Sensitive Data refers to data elements that are specific to DLIR operational activities including financial, legal, and other operational transactions involving vendor acquisitions, RFP, etc., Though some of such information may to divulged to the public after certain time, such data will be considered sensitive till the data become public. From a technology standpoint, privileged access to the network, databases, applications is considered sensitive.

Restrictive Data refers to the data elements referring to individuals FTI and SSA related transactions. Such data is protected with highest care and access to such data is further restricted to limited individuals even within DLIR.

DLIR implemented multi-layer security controls to ensure that data under its custody is protected while the data is at rest or in transit by employing relevant tools and techniques such as encryption and DLP (Data leakage Protection).

Data Disposal

DLIR ensures that all the data is disposed in a safe manner during the asset decommissioning process. All the divisions within the DLIR are instructed to physically submit obsolete technology equipment to DLIR security team. Hardware containing data (hard drives, RAM, SSD) are removed from the equipment and will be crushed using industry standard hard disk and SSD destroyers. This disposal activity is performed on-site at DLIR and none of the data sensitive equipment is handed to other third-party vendors for disposal.