CALHR
CALIFORNIA DEPARTMENT OF HUMAN RESOURCES

Discrimination Complaint Tracking System Security and Access Guidelines

Introduction

The California Department of Human Resources (CalHR) sets forth these guidelines to define security and access requirements for all users of the Discrimination Complaint Tracking System (DCTS). The DCTS is California's system of record to track and monitor statewide discrimination and harassment complaint activities.

CalHR's DCTS is a comprehensive cloud-based case management and tracking system that enables data collection of discrimination and harassment complaints across state departments. The DCTS provides a monitoring foundation of the complaints filed with state entities by capturing data such as discrimination complaint type, parties involved, dates of filing, investigation information and outcomes. Government Code section 18573[1] requires each appointing power to provide access to records and prepare reports as required by CalHR. All department Equal Employment Opportunity (EEO) Offices will utilize DCTS to report complaint data in a single and secure location.

The CalHR Office of Civil Rights (OCR) will utilize the DCTS to fulfill its mandate to advocate, coordinate, enforce, and monitor equal employment opportunity programs[2] statewide.

CalHR adheres to the regulations and requirements as set forth in the California Information Practices Act of 1977 (IPA)[3] and the Federal Privacy act of 1974[4]. Department staff accessing DCTS data should be familiar with these state and federal statutes.

This document outlines the individual expectations for system users.

Privacy and Data Security Standards

All statewide discrimination and harassment complaint data collected within the DCTS is confidential and subject to state policy and data security standards. Information systems used to process/store confidential or sensitive information must protect data from unauthorized access. While the cloud-based service offers many benefits for online data storage, access to confidential or sensitive online data increases the risk of unnecessary disclosure of this data. Access to the DCTS is granted only to those with

[1] Government Code section 18573
[2] State Civil Service Equal Employment Opportunity Program (Government Code, § 19790 et seq.)
[3] Information Practices Act of 1977 (California Civil Code, § 1798 et seq.)
[4] The Federal Privacy Act (Public Law 93-579)

an authorized legitimate business need and in the performance of governmental duties requiring access.

Careless, accidental, unintentional or malicious disclosure of information to unauthorized persons may result in civil and/or criminal actions against those involved in inappropriate disclosure (refer to California Penal Code 502 and the IPA). To mitigate risk, CalHR has established the necessary security protocol and access requirements to be followed, without exception, by all DCTS users to ensure department and user compliance.

Responsibility to Protect DCTS Data

The responsibility for protecting confidential and sensitive data contained within the DCTS is a shared effort. While CalHR maintains an oversight role to secure data and eliminate vulnerability within the DCTS, the initial point of access security resides with department management staff who request access for users and certify user credentials. CalHR has no responsibility or control over departments' physical security controls. Once the DCTS is accessed, security of confidential data becomes the responsibility of the accessing department and its authorized staff. All hard copies (including printouts) of data extracted from the DCTS remain confidential and must be protected by department staff from unauthorized disclosure in a manner as stipulated in the IPA. Any failure in this area can result in violations in which individuals, staff and/or management may be held personally liable.

Each user must be aware of the potential risks of disclosure of confidential data either through unlawful use of login credentials, an unattended active PC/terminal, or inadvertent disclosure (i.e., unauthorized individuals viewing confidential data via an open computer screen or documents left out on a desk). Regardless of the manner in which unauthorized disclosure arises, individual users are responsible to secure passwords and DCTS data and information. Individual users are accountable for any violation of the Discrimination Complaint Tracking System Security Agreement and/or subsequent legal consequences resulting from unauthorized use of access credentials.

DCTS System Administrator

The CalHR DCTS System Administrator acts on behalf of the CalHR OCR for the various functions of the DCTS, including security access and monitoring. The DCTS System Administrator manages the technical application of the tracking system and serves as CalHR's liaison with all department users. The DCTS System Administrator is required to ensure compliance of all DCTS activity and security procedures as identified within these guidelines. If unauthorized activity is suspected, the DCTS System Administrator may monitor and investigate all department DCTS activities, including individual users.

The DCTS System Administrator has the express authority to approve, deny and revoke user access as determined necessary.

DCTS Access Requirements

Access to the DCTS may only be granted to individuals that have met the criteria outlined in this section. The most common access granted is to department EEO Officers and EEO investigators. Access for individuals not serving in an EEO Officer or EEO investigator capacity for the department shall be evaluated on a case-by-case basis.

Access and use of the DCTS shall only be initiated from workstations that are owned, leased or controlled by the user's department. Access from personal computers, laptops, cell phones, tablets or any other personal electronic device in which users may access the DCTS is strictly prohibited.

The DCTS Security Agreement communicates security requirements for state departments and their employees. The DCTS Access Request form documents the addition and deletion of system users. Users are primarily awarded access by department EEO Officer justification and approval. CalHR restricts access to only those individuals that require it in order to perform the duties of their job. Careful consideration should be taken by departments in requesting any user access.

CalHR grants access in accordance with current User Guidelines as follows:

1. User is a bona fide employee of the State and specifically of the requesting department assigned in the capacity of EEO Officer or EEO Investigator. Additional justification is required for individuals with no direct role in either investigations or supervision of investigations.
2. Access is granted only after the CalHR DCTS Security Agreement and DCTS Access Request form are fully executed and on file with CalHR.
3. Permission determinations and access levels are granted for only those areas of the DCTS that are determined necessary to perform assigned job duties. The CalHR DCTS Administrator should be contacted for any clarification needed regarding access.
4. Misuse or unauthorized disclosure of login credentials by any user may result in the revocation of access to the DCTS.

User Roles

The DCTS supports three types of EEO users with different roles and access levels:

EEO Officer- By statute, oversees the department EEO program. The primary DCTS user who will open new cases and may view, enter and edit all case information for their department. CalHR's Primary contact for all DCTS activity. Verifies claim information is properly entered and finalizes case closure. For small departments with only one staff member serving as the EEO Officer, this will be the user type designated.

EEO Investigator- Assigned to investigate complaints. Able to view, enter, and edit specific cases as assigned. Must submit the case to the EEO Officer for case closure.

EEO Manager- Reports to the EEO Officer. May investigate and/or supervise employees who investigate discrimination and harassment complaints. Assigned the same user rights as the EEO Officer. May open new cases, view, enter and edit all case information for their department. EEO Officer may reassign case closure approval to the EEO Manager on a case-by-case basis.

Security Agreements

CalHR requires General Security Agreements (GSA) to be on file for all access levels granted to system users. The Discrimination Complaint Tracking System (DCTS) Security Agreement is a standardized document which is designed to communicate expected security measures important to the handling of confidential data related to discrimination and harassment complaint activities.

Criterion applied to GSA requirements:

1. CalHR's current version of the DCTS Security Agreement must be utilized.
2. Users must sign and date the DCTS Security Agreement, agreeing to accept personal responsibility to adhere to security requirements.
3. The EEO Officer's signature is required for all DCTS Security Agreements with the exception of their own. For the EEO Officer's Security Agreement, the department Director's signature is required.
4. Annual renewal is required of all DCTS Security Agreements. Expired agreements will result in access removal as determined by the DCTS System Administrator and/or CalHR OCR.
5. Departments must keep copies of DCTS Security Agreements in accordance with State Retention rules, and no less than five years per this CalHR DCTS Security Requirements document.
6. When an authorized user vacates their role and/or position, the Department EEO Officer shall immediately notify CalHR. When a role or position is vacated, the user's access becomes void and must be immediately revoked.
7. When an authorized EEO Officer vacates their position, the employing department shall immediately notify CalHR. The user's access becomes void and must be immediately revoked.