CALHR
CALIFORNIA DEPARTMENT OF HUMAN RESOURCES

# Family Connect Project - Department Security Agreement

The Department of Human Resources (CalHR) is committed to the privacy and security of personal information maintained within the Family Connect Project (FCP). Our policies regarding personal information collected and managed by our department are governed by law, including the Information Practices Act of 1977 (Civil Code section 1798 and following).

If granted access to CalHR's FCP, your designated staff will be exposed to a variety of sensitive and confidential state employee and dependents' benefits information. This may include information about the designated staff's co-workers, supervisors, management and executive staff. Additionally, information they will encounter may encompass various employment activities of state employees. If granted access, they are expected to appropriately handle all confidential/sensitive information of state employees and their dependents. In addition, as the hiring authority, you must protect the security and privacy of state employees and their dependents' data from unauthorized disclosure by strictly adhering to the following Department responsibilities.

## DEPARTMENT CERTIFICATION

Department Responsibilities

1. Department shall not use or disclose CalHR's FCP data for any purpose except as permitted by this Agreement or as required by law.

2. Department shall use appropriate administrative, physical and technical safeguards specified in the Information Practices Act of 1977 (Civil Code sections 1798, et seq.) and the State Administrative Manual (SAM) Chapter 5300 to prevent unauthorized use or disclosure of Personally Identifiable Information (PII) contained on CalHR's FCP.

3. Department will report to CalHR any unauthorized use or disclosure immediately upon discovery and follow up with a detailed report of the breach to CALHR immediately upon discovery.

4. Access to CalHR's FCP under this agreement shall be effective as of July 1, 2022, and shall remain in effect until all access granted to CalHR's FCP is terminated.

5. Upon CalHR's knowledge of a material breach or violation of this Agreement by the Department, CalHR will terminate and discontinue access to CalHR's FCP, and report the problem to the CALHR Information Security Officer. Access to the FCP will not be restored until the Department has provided reasonable assurance to CalHR of the resolution of the any reported breach or violation of this agreement.

6. Department shall, in accordance with the requirements of this agreement comply with all applicable California statutes and regulations regarding the privacy and security of PII. Department shall in all other respects maintain the privacy and security of PII at a level and scope that is not less than the

level and scope of requirements the Information Practices Act of 1977 (Civil Code sections 1798, et seq.), and information security practices and standards SAM Chapter 5300.

7. Department must maintain a level of security in any automated information system in accordance with the requirements of this agreement.

8. Department shall restrict access to the FCP data obtained under this Agreement to only those authorized Department employees, contractors, and agents who need CalHR's FCP data to perform their official duties in connection with purposes identified in this agreement.

9. Ensure that laptops and other electronic devices/media containing PII, and CalHR data used to access FCP data are encrypted and password-protected.

10. Send emails containing PII, and confidential FCP data only if encrypted, and is only sent to and is received by email addresses of persons authorized to receive such information.

11. Only authorized participating Department personnel and its agents shall transmit CalHR FCP data provided under this agreement.

12. End-to-end encryption shall always be used to protect confidential CalHR FCP data, or personal information that it is transmitted or accessed outside secure internal networks (e.g., email, file transfer, Internet/website communication tools) of the state entity, or stored on portable electronic storage media (e.g., USB flash drives, tapes, CDs, DVDs, disks, SD cards, portable hard drives), mobile computing devices (e.g., laptops, netbooks, tablets, and smartphones), and other mobile electronic devices as required by SAM Chapter 5350.1.

**Department User Responsibilities**

**Department users granted access to FCP are required to adhere to the following operational standards:**

1. Safeguard your FCP account login credentials to protect disclosure, and unauthorized access. In the event of compromise or breach of login information, you agree to immediately notify your immediate supervisor and CalHR.

2. FCP login passwords are individually assigned to authorized users. You are prohibited from sharing system access information with anyone including but not limited to your supervisor, subordinate employees, or persons performing your job duties in your absence. To the extent that is necessary for other employees to access FCP data, such employees designated as system admins must grant system access credentials.

3. You agree to protect FCP data against unauthorized access by securing unattended active PC/terminals. Workstation computers shall be kept secure.

4. The FCP shall be accessed only from workstations that are owned, leased, or controlled by the employer. You are prohibited from accessing the FCP from personal computers, laptops, cell phones, tablets, or any other personal electronic device.

5. You agree to immediately notify the FCP System Administrator of any suspected or known unauthorized activity that is or may be in violation of this agreement.

6. If you suspect or have knowledge that your FCP password or login credentials have been compromised, you agree to immediately change your password and notify the FCP System Administrator.

7. Employee and Dependent information are confidential, and you are prohibited from revealing any information to an unauthorized person.

8. Unauthorized modification or deletion of FCP information outside of the system's intended and approved use is strictly prohibited. Illegal access or misuse of your user account will result in revocation of your access and may be punishable by dismissal.

9. You agree that if your job assignment changes, for example, a move or transfer to another position outside of your current employer or unit, your access will be void and you may not continue to access the FCP and must immediately inform your system admin contact.

10. If at any time you discover you have, or may have, violated this agreement and/or compromised system security in any manner, you agree to immediately report it to your immediate supervisor and the CalHR FCP program manager.

11. You understand that CalHR has the right to investigate any potential security breaches or other incidents involving the FCP and agree to fully cooperate with any such investigation.

12. Violation of any of the user responsibilities above is considered serious. Users who violate their user responsibilities will have their access immediately terminated. In addition, the department reserves the right to pursue corrective and/or adverse action against any employee who violates any provision of this agreement.

---

**Signatory Authority**

| *<CALHR Official>* | *< Agency Official>* |
|---|---|
| _____ | _____ |
| Signature Date | Signature Date |
| _____ | _____ |
| Printed Name | Printed Name |
| _____ | _____ |
| Title | Title |