Information Security

Requirements for Employees and Contractors With Access to Confidential Information

California Department of Tax and Fee Administration
Board of Equalization
Employment Development Department
Franchise Tax Board

Confidential Information

As a general rule, treat all tax and nontax program information received, maintained, or generated by the California Department of Tax and Fee Administration (CDTFA), Board of Equalization (BOE), Employment Development Department (EDD), Franchise Tax Board (FTB), Department of Motor Vehicles (DMV), or the Internal Revenue Service (IRS) as confidential.

Confidential information remains subject to the same safeguard requirements and highest levels of security regardless of your work location.

Examples of confidential information include, but are not limited to:

- Taxpayer information and records, such as account information, tax returns, and nonpublic registration or return information.
- Personally Identifiable Information (PII). Personally Identifiable Information is information about individuals that relates to their personal life or that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.
- Tax account, taxpayer, wage earner, claimant, and nonpublic employee information; employee personnel records; criteria used for initiating audit selection.
- Methods agencies use to safeguard their information and information about how agencies' computer systems operate.
- Information that is considered proprietary, a trade secret, or otherwise protected by law or contract.

Rules Relating to Confidential Information

Confidential information is for state business use only.

In order to safeguard confidential information:

- Do not request, access, examine, modify, or use confidential information unless there is a need to do so in the normal course of your work as a state employee or contractor. This includes even casual or curious browsing of any information that is not a part of your assigned work.
- Do not request, access, examine, modify, or use confidential information to achieve private or personal gain.
- Do not make any type of disclosure (i.e., written or verbal) of confidential information to unauthorized individuals, including members of your family, friends, or other employees who do not have a work-related need to know.
- Do not request, access, examine, modify, or use confidential information about celebrities or other well-known individuals unless this activity is necessary as part of your assigned work.
- Do not make any type of disclosure (i.e., written or verbal) of confidential information to unauthorized individuals, including members of your family, friends, or other employees who do not have a work-related need to know.
- Do not intentionally destroy confidential information, make copies of it for personal use, or remove it from your worksite location without proper authorization.
- Do not dispose of confidential information in any manner that is inconsistent with your agency-approved destruction policies and methods.
- Do not use personal devices (including, but not limited to, cameras, video recorders, portable media players, or mobile phones/smartphones) in the workplace to capture or record confidential information, including that which appears in the background in work areas.

Protect User IDs, Passwords and Passphrases

You are personally responsible and accountable for all activity occurring under your User ID(s), password(s) and passphrase(s). It is in your best interest to protect them!

- Never use anyone else's User ID, password or passphrase, nor allow anyone to use yours.
- Secure all passwords and passphrases. Do not post them anywhere or include them in a data file, logon script, or macro.
- Make sure your work User IDs, passwords, and passphrases are different from your personal User IDs, passwords, and passphrases.
- Select strong passwords and passphrases by including an unusual combination of characters. Avoid using words and names.
- If you believe your system or an online account you access has been compromised, change your passwords and passphrases and notify your supervisor or your department's Information Security Office immediately to determine if any additional action is needed.

Clean Desk and Clear Screen Procedures

Secure confidential information when you leave your PC or workstation, even if it is only for a few minutes.

- Always log off or lock your PC/workstation when not in use.
- Personal or confidential information, as defined in State Administrative Manual section 5850.1, must be encrypted when it is stored on, transmitted to, or accessed by portable electronic media and devices (including, but not limited to, CDs, thumb drives, laptop and notebook computers). Additionally, the media or device containing the information must be stored in a secure place.
- Ensure paper documents containing confidential information are locked up when unattended and after business hours.
- Make sure your monitor/screen is never visible to members of the public or to another agency's employees if in a shared facility.

Access

Access is a privilege granted by your agency. Your agency reserves the right to limit, extend, or withdraw access to its computer systems, devices, and data resources.

- Use only computers, networks, applications, and information for which you are authorized.
- Use your access for approved business-related purposes only.
- All access to confidential information is monitored. Anyone using BOE, CDTFA, EDD, FTB, DMV, or IRS computer systems expressly consents to such monitoring.

Information Security Violations and Incidents

Examples of information security violations and incidents include:

- Unauthorized access, use, or disclosure of confidential information.
- Unauthorized use of a User ID, password, or passphrase.
- Suspicious unsolicited emails that instruct you to click on a link, open an attachment, or call a phone number provided within the message.

- Unusual circumstances on the computer network, such as data that appears to be of questionable accuracy, since this may indicate a security violation, a computer virus, or a cybersecurity threat.
- Malicious insider crimes committed by current or former coworkers or contractors. Insider crimes include, but are not limited to, unauthorized use, theft, destruction, and disclosure of confidential information, IT sabotage, and fraud.

If you suspect an insider threat or security breach of confidential information or IT resources, report it!

Employees and contractors with information security or disclosure questions may request information from their agency contact listed below:

CDTFA

Information Security Office
PO Box 942879, MIC:94
Sacramento, CA 94279-0094
Email: *InformationSecurity@cdtfa.ca.gov*
Telephone: 1-916-309-1862

Disclosure Office
PO Box 942879, MIC:82
Sacramento, CA 94279-0082
Email: *Disclosure.Office@cdtfa.ca.gov*
Telephone: 1-916-445-2918

Unauthorized access, inspection, acquisition, use, disclosure, modification, removal, or destruction of confidential information is a crime under state and federal laws. Employees and contractors who violate the law may be subject to administrative discipline, criminal prosecution, and/or civil lawsuit.

EDD

Information Security Office
PO Box 826880, MIC:33
Sacramento, CA 94280-0001
Email: *Infosec@edd.ca.gov*

FTB

Disclosure Office
PO Box 1468, MS A-181
Sacramento, CA 95812-1468
Telephone: 1-916-845-3226

Information Security Audit & Investigations Unit
PO Box 1468, MS A-190
Sacramento, CA 95812-1468
Email: *SecurityAuditMail@ftb.ca.gov*
Telephone: 1-916-845-5555

BOE

Disclosure Office
PO Box 942879
Sacramento, CA 94279-0121
Email: *BOEPRARequests@boe.ca.gov*

Information Security Office
PO Box 942879
Sacramento, CA 94279-0094
Email: *InformationSecurity@cdtfa.ca.gov*
Telephone: 1-916-309-1862