Information Security

Requirements for Employees and Contractors with Access to Confidential Information

Board of Equalization
Employment Development Department
Franchise Tax Board

Standards and Rules Relating to Confidentiality

As a general rule, treat all tax and nontax program information received, maintained, or generated by the 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.

Examples of confidential information include:

- Information about individuals that relates to their personal life or that identifies or describes an individual.
- Tax account, taxpayer, feepayer, wage earner, claimant, and employer 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.

Agency Information Is for State Business Use Only

- Do not request, access, examine, modify, or use information unless there is a need to do so in the normal course of your work. 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 request, access, examine, modify, or use information about your family, friends, neighbors, coworkers, or business associates. Also, do not request, access, examine, modify, or use information related to your own personal or business accounts, including the account of any corporation or exempt organization in which you have a financial interest. If any of these accounts are assigned to you as a part of your work, do not work the account. Notify your supervisor immediately.
- 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 discuss or disclose confidential information to unauthorized individuals, including members of your family, friends, or other employees who do not have a need to know. This includes both written and verbal disclosure.
- Do not intentionally destroy confidential information, make copies of it for personal use, or remove it from the premises without proper authorization.
- Dispose of confidential information using agency-approved destruction policies and methods.

Protect User ID and Password

You are personally responsible and accountable for all activity occurring under your user ID and password. It is in your best interest to protect them!

- Never use anyone else's user ID and password nor allow anyone to use yours.
- Do not write your password down, post it anywhere, or include it in a data file, logon script, or macro.
- Make sure your work user IDs and passwords are different from your personal user IDs and passwords.
- Select strong passwords that contain 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 immediately.

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, sensitive, and confidential information, as defined in State Administrative Manual section 5320.5 must be encrypted when it is stored on 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 secure when not in use.
- Make sure your monitor/screen is never visible to members of the public or to another agency's employees if in a shared facility.

Use of and Access to the Agency's Information Assets

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, EDD, FTB, DMV, or IRS computer systems expressly consents to such monitoring.

Report Any Suspected Information Security Violation to Your Supervisor or Information Security Personnel

Examples of information security violations include:

- Unauthorized access, use, or disclosure of confidential information.
- Unauthorized use of a user ID or password.
- Suspicious unsolicited email that requests you 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 hacker intrusion.
- 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 agency information, IT sabotage, and fraud. If you suspect an insider threat to the agency's information and IT resources report it!

Unauthorized access, use, or disclosure 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.

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

BOE

Information Security Office
450 N Street, MIC:93
Sacramento, CA 95814
Email: *InformationSecurity@boe.ca.gov*
Telephone: 1-916-322-3185

Disclosure Office
P.O. Box 942879, MIC:82
Sacramento, CA 94279-0082
Telephone: 1-916-445-2918

EDD

Information Security Office
P.O. Box 826880, MIC:33
Sacramento, CA 94280-0001
Email: *Infosec@edd.ca.gov*
Telephone: 1-916-654-6231

FTB

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

Information Security Audit Unit
P.O. Box 1468, MS A-190
Sacramento, CA 95812-1468
Telephone: 1-916-845-5555

BOE Publication 353 (4-13)
EDD DE 7420 (Rev. 2)
FTB 7700 (Rev. 04-2013)