

City/County Business Tax Program Administration and Safeguard Overview

Data Resources and Services Unit

Privacy, Disclosure, & Data Resources Section

Contents

Objective	3
Program Background	4
Legal Authority	4
Revenue and Taxation Code (R&TC) Section 19551.5	4
Revenue and Taxation Code (R&TC) Section 19551.1	4
Revenue and Taxation Code (R&TC) Section 19542	4
Use of Data and Ownership	5
Annual Training	5
Confidentiality Statement	5
Due Dates	6
Common Errors	6
Incident Reporting	7
Safeguards	7
Destruction of Records	8
Resources	9

Objective

The purpose of this overview is to inform the city/county and its employees of the appropriate safeguards to mitigate the risk of unauthorized disclosure and access of FTB confidential tax data.

- Program Background
- Legal Authority
- Use of Data and Ownership
- Confidentiality Statement
- Annual Overview
- Due Dates
- Incident Reporting
- Safeguards
- Destruction of Records
- Record Layout
- Resources

Program Background

Participating cities and counties provide local business license data to Franchise Tax Board (FTB). In exchange, FTB completes a data match for business activity in the respective city or county. This data exchange aids FTB in finding businesses who do not file income tax returns, and cities and counties to identify unlicensed businesses within their jurisdiction.

- The program originated in the 1990s
- Name history:
 - 1990: Local Government Sharing Program
 - 2009: City Business Tax Program
 - 2016: City/County Business Tax Program

Legal Authority

[Revenue and Taxation Code \(R&TC\) Section 19551.5](#) mandates cities and counties to provide business tax data to FTB.

[Revenue and Taxation Code \(R&TC\) Section 19551.1](#) authorizes a reciprocal agreement for the exchange of city/county business tax and confidential information between a city/county and FTB.

[Revenue and Taxation Code \(R&TC\) Section 19542](#) states it is a misdemeanor to disclose confidential information. The penalty for each violation may be:

- Up to \$10,000 fine
- One to three years' incarceration
- Civil lawsuit

Use of Data and Ownership

The confidential tax data being provided to the city/county under the exchange agreement remains the exclusive property of the FTB, and must be used exclusively to administer the CCBT Program.

Confidential tax data is not available to the public and requires special precautions to protect from:

- Loss
- Unauthorized use and disclosure
- Modification
- Destruction

Annual Training

In addition to signing the confidentiality statement, all city/county employees who may have access to FTB confidential tax data must complete the CCBT Program Administration and Safeguard Overview.

- May be completed in a group space or individually
- For the most current version visit the CCBT website

Confidentiality Statement

Upon approval of the exchange agreement, and prior to any access to FTB confidential tax data, each city/county employee who may have access to the data is required to sign the City/County Business Tax Program Confidentiality Statement.

The signed statement(s) must be retained by the city/county and furnished to FTB upon request.

Due Dates

Action	Date
Cities/counties transmit their data to FTB	By June 30
FTB transmits data to participating cities/counties	By December 31

- All data must be transmitted via Secure Web Internet File Transfer (SWIFT)
- The data provided by FTB will cover the prior year
 - Example: Tax year 2017 data is provided December 2018

Common Errors

Common errors when submitting files via SWIFT:

- Length of first and last name fields do not meet required specifications
- Document not converted to a .txt file prior to uploading to SWIFT
- Fields overflowing into the next; causing data to be out of alignment
- Not formatting the file correctly to prevent the data from being cut short

Incident Reporting

Report all unauthorized or suspected unauthorized access, use, and disclosure of FTB data within 24 hours of incident.

- Email incident report to SecurityAuditMail@ftb.ca.gov
 - Cc: FTBCCBT@ftb.ca.gov
- Include:
 - Date and time of incident
 - Date and time of discovery (if different)
 - Name of employee involved
 - Description of incident
 - Action(s) taken
 - Your name and contact information

Safeguards

A secure environment is required to protect the confidential tax data obtained from FTB.

- Accessible only by employees of the business license program
- Electronic data must be password protected
- Hardcopies of the data must be locked in a file drawer

Additional safeguard recommendations include:

- Maintaining a visitor log for non-city/county employees
- Setting a predetermined 10-minute lockout period on your system
- Using strong passwords
- Displaying warning banners on all systems that may contain FTB confidential tax data
 - Example: *This computer contains confidential FTB data. Unauthorized access, use, inspection, or disclosure of this information may be punishable under Revenue and Taxation Code sections 19542.1 and Penal Code section 502.*

Destruction of Records

All confidential tax data received from FTB must be destroyed within three years of receipt. The data must be destroyed in a manner to be deemed unusable or unreadable, and to the extent that an individual record can no longer be reasonably ascertained.

- Purge all files on your system(s)
- Degauss, demagnetize, or damage CDs to prevent use
- Shred paper documents

Notify the CCBT program manager annually when the destruction of records has been completed.

- Email FTBCCBT@ftb.ca.gov
- Include the purge date and tax year(s) purged

Resources

CCBT Program Contact Information

- FTBCCBT@ftb.ca.gov
- (916)845-6304

[Franchise Tax Board Website](#)

[City/County Business Tax Program Website](#)

[California Law Codes](#)

[CCBT Confidentiality Statement](#)

[SWIFT Login](#)

[SWIFT User Guide](#)

[Record Layout](#) – cities/counties must follow these specifications when sending files