FTBNet

Skip to main content

Policy File 4133 - Acceptable Use

Subject	Number
Acceptable Use	**4133 PF**
References to Other (Related) FTB Policies or Procedures **California Government Code Section 8314** **Policy File 4130 — Incompatible Activities and Rules of Conduct** **GPM 9135 — Outside Employment Survey** **PF 9500 — Information Security Policy** **California Penal Code Section 1546(b)** **GPM 7013 — Wireless Access for Business**	Implementation Date: **October 2008** Review Date: **June 2022** Revision Date: **June 2022**
Authority **FTB 7808 — Statement of Incompatible Activities and Rules of Conduct for Departmental Employees** **FTB 1131H — Franchise Tax Board Employee Privacy Notice on Collection** **NIST Special Publication 800-53 rev 4** **IRS Publication 1075** **California Penal Code Sections 1546-1546.4** **California Government Code Sections 11015.5 & 11019.9** **California Civil Code Sections 1798.14 & 1798.17** **Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53)** **Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i (NIST Special Publication 800-97)** **Guidelines for Securing Wireless Local Area Networks (NIST Special Publication 800 -153)**	Issuing Unit/Owner **Privacy, Security, and Disclosure** Robert Mayorga

Introduction	We expect responsible, effective, and lawful use of the Franchise Tax Board (FTB) wired or wireless network, computer systems, the Internet, and other technology resources such as electronic mail (email) and telephones as a means to achieve the department's business goals and mission. FTB is the sole authorized possessor of these resources as well as the information stored on or generated through them. These resources are provided to conduct state business and are routinely monitored for improper use. Anyone using these resources expressly consents to such monitoring. Anyone granted access to FTB technology resources is required to read and agree to abide by the FTB Acceptable Use Policy.
Scope	This policy applies to anyone having access to or use of technology resources owned, operated, or managed by FTB or the State of California. This policy applies to the use of FTB technology resources from remote locations (e.g., while telecommuting) as well as from an FTB worksite.
Policy	**Acceptable Activities** Acceptable activities are those in accordance with the laws and policies of the United States Government and the State of California; are consistent with the purpose, goals, and mission of the Franchise Tax Board; and are appropriate to each user's assigned job duties and responsibilities. The following list provides examples of acceptable activities: • Research to enhance compliance and filing program activities. • Communications for business and administrative purposes. • Incidental, necessary communications pertaining to personal and family matters, such as a phone call or email to a child's daycare or school.

Unacceptable Activities
The following list provides examples of unacceptable activities:

- Use for outside employment, business, or personal gain.
- Use for any illegal, discriminatory, or defamatory purpose, including the transmission of threatening, obscene, or harassing messages.
- Activities that interfere with an employee's ability to perform their job duties or responsibilities.
- Browsing inappropriate websites such as those that contain nudity or sexual content, malicious content, or gambling activities.
- Intentionally attempting access to information resources without authorization and a business need.
- Installing or connecting unauthorized software or hardware on FTB owned and/or managed information systems.
- Storing personal or nonbusiness related data and multi-media files on FTB servers or other centrally managed resource.

FTB Email Messages and Instant Messages (IM): Email messages and instant messages distributed via FTB email and IM systems are FTB property and not the private property of individual users.

FTB email and IM systems must not be used for:

- Automatic forwarding of email messages to external recipients.
- Transmitting confidential information to external recipients unless encrypted with a method approved by the FTB Chief Security Officer (CSO) and appropriate to the employee's job duties and responsibilities.
- Circulating chain mail, jokes of the day, nonbusiness related video clips, and digital images.
- Distributing religious, political, sexual, or offensive content.

External Email and IM Services: While connected to the FTB network, use of external email and IM services (e.g., your home email and IM accounts) is prohibited unless expressly approved by the FTB CSO.

File Sharing: State and federal law prohibits the unauthorized transfer, or sharing of music, movies, software, and other intellectual property. Therefore, unauthorized use of peer-to-peer (file sharing) software is prohibited at FTB. Peer-to-peer technologies must be approved by the FTB CSO for business use.

Return to Table of Contents