State Compensation Insurance Fund

COVID-19 Work Options Program

Policy and Procedures

A policy and procedural guide to Work at Home for supervisors and employees during the COVID-19 Pandemic for State Compensation Insurance Fund

March 2020

Contents

COVID-19 WORK OPTIONS PROGRAM

Foreword	The COVID-19 Pandemic has ushered in uncertain and extraordinary times. In order to address the needs of State Fund employees during the COVID-19 crisis, this program will outline the ability of employees to work from home or from an alternate work location, to the extent possible based on available equipment, the capacity of the network, and whether the employees job can be performed at home with the proper equipment. We are asking employees to be flexible while we work to accommodate as many employees as possible with this process. We may implement shift work in order to maximize the bandwidth of the State Fund network. The COVID-19 Work Options Policy and Procedures and Information Systems Security Corporate Policy documents are intended to avoid confusion or misunderstanding about this practice. It also provides a detailed guide for executive staff, managers and supervisors implementing this practice within their workgroups.
Duration of Policy	The COVID-19 Work Options Program is in effect only during the response period for COVID-19 and will sunset when the Executive Committee determines the program should end. At that time, all employees approved to telecommute under this program will return to their regular work locations.

Policy	State Fund may authorize an employee to work at home during the COVID-19 crisis to decrease the risk of employees from contracting COVID-19 at work. Eligibility for telecommuting is based on the following criteria and will be prioritized by risk, as indicated below. **Criteria:** Employee's job can be performed at home with proper equipment such as computer, monitor, phone and internet access, as determined by the employee's Program. Stage 0—Individuals who have school-age children, are in schools that are closed, and have the necessary equipment to work from home Stage 1 –High Risk Individuals • Those that the CDC has identified as high risk (individuals with hypertension, heart disease, lung disease or diabetes) • Individuals over 60 years old • Individuals who are pregnant (There is no evidence that this group is at higher risk; however, we are including them out of an abundance of caution) • Individuals who are returning from international travel from cruise ships or a restricted area as defined by the CDC Stage 2— • Those employees who take mass transit to work those employees who live with someone who is high risk. • Employees who have returned to the United States from a country that does not currently have travel restrictions as defined by the CDC. State 3—All others Alternate Work Location: Employees who are not able to work from home may be permitted to work at a State Fund location closer to their residence, space permitting Work Schedules: We may determine that it is necessary to change employee's current work schedules, including eliminating Alternate Work Schedules, as we have more employees working from home, in order to maximize the bandwidth of the State Fund network. Supervisor approval is required for COVID-19 Work Options participation. Employees under the current Telework Program will continue on that program.
Confirmation	Employees will receive a confirmation email from their supervisor approving the temporary work option, which will outline schedule and expectations.

COVID-19 WORK OPTIONS PROGRAM –SECURITY AND PRIVACY CORPORATE POLICY

Information Systems Security Corporate Policy	State Fund is required to ensure that its COVID-19 Work Options Program is implemented in accordance with all applicable laws, policies, and standards including those governing the protection of State Fund information assets.
Privacy & Confidentiality Corporate Policy	For the purposes of the duration of the use of the COVID-19 Work Options Program, employees are authorized to use personal equipment such as monitors, routers, and cell phones in the course of their work at home. Personal printers are not authorized for use at home. State Fund will not assume responsibility for payment of personal cell phone plan or internet plan as part of this agreement, unless the participant experiences additional fees above your regular plan in the course of your work. The Information Systems Security Corporate Policy and Privacy & Confidentiality Corporate Policy is available in the Corporate Policy Library, http://governance.scif.com/CorpPolLibrary.html

COVID-19 WORK OPTIONS PROGRAM - IMPLEMENTATION	
Department	State Fund is responsible for the implementation of the COVID-19 Work Options Program and encourages the use of the program where work conditions warrant. State Fund will ensure that: ▪ Employee compensation or benefits will not change due to participation in the program, however, employees may be asked to shift responsibilities to support this effort. ▪ The amount of time the employee is expected to work per pay period will not change. ▪ *Managers and employees will familiarize themselves with the COVID-19 Work Options policy and procedures contained or referenced in this document.* ▪ State Fund information assets are secure and confidential, personal and sensitive information is protected.
Executive Staff	Executive staff is responsible for encouraging managers and supervisors to use COVID-19 Work Options where work conditions permit.
Management Staff	State Fund management staff is responsible for administration of the COVID-19 Work Options Program within respective areas of responsibility. These responsibilities include: ▪ Receiving COVID-19 Work Options requests, allocating into prioritization groups, and logging them in the designated SharePoint. ▪ Ensuring managers, supervisors, and COVID-19 Work Options employees have read and understand the COVID-19 Work Options Policy and Procedures document, Information Systems Security Corporate Policy, and Privacy & Confidentiality Corporate Policy. ***Ensuring compliance with all applicable policies, procedures, and guidelines.***

COVID-19 WORK OPTIONS PROGRAM - IMPLEMENTATION

Managers and Supervisors	State Fund encourages managers and supervisors to support the use of the COVID-19 Work Options program. Managers and supervisors are responsible for: ▪ Reading and understanding the contents and requirements of this COVID-19 Work Options Policy and Procedures document in addition to the Information Systems Security Corporate Policy and Privacy & Confidentiality Corporate Policy. ▪ Identifying job tasks and classifications suitable for COVID-19 Work Options. ▪ Overseeing the day-to-day performance of COVID-19 Work Options employees, as they would on-site employees, including communicating general office updates and related information to the COVID-19 Work Options program. ▪ Ensuring COVID-19 Work Options employees indicate the hours they have worked while at home are in accordance with the State Fund's established policy and procedures. ▪ Approval of the COVID-19 Work Options employee's use of sick leave, vacation, time off, or other leave credits, as well as any overtime work. ▪ Ensuring compliance with the Information Systems Security Corporate Policy and Privacy & Confidentiality Corporate Policy to protect State Fund assets when accessing, storing, or transporting State Fund information. ▪ Reporting security incidents immediately when they occur. ▪ Retaining copies of COVID-19 Work Options employees' confirmation email. ▪ Facilitating the tracking and return of State Fund-owned equipment.
Manager Services	Manager Services will: ▪ Assist Supervisors with timecard related questions, if not answered by AskAdmin. ▪ Serve as a COVID-19 Work Options resource for management.

Employees

Employees interested in a temporary work option are responsible for:

- Understanding the requirements contained in the State Fund COVID-19 Work Options Program Policy and Procedures and Information Systems Security Corporate Policy, and Privacy & Confidentiality Corporate Policy.
- Submitting a COVID-19 Work Option request to their supervisor, via email, identifying the priority the employee falls under.

When a COVID-19 Work Options arrangement is approved, employees are responsible for:

- Abiding by the provisions set forth in the State Fund COVID-19 Work Options Program Policy and Procedures, Information Systems Security Corporate Policy, and Privacy & Confidentiality Corporate Policy.
- Establishing and maintaining a work area that is clean, safe, and free from hazards.
- Maintaining State Fund-owned equipment, devices, and services associated with achieving a safe, secure and healthful temporary work option environment as identified in the Information Systems Security Corporate Policy.
- Reporting security incidents immediately to IT and their supervisor.
- Complying with all applicable policies, standards, procedures, and guidelines.
- Ensuring the security and protection of any physical documents needed in the course of their work
- Complying with tax laws.

  State Fund is not responsible for substantiating an employee's claim of tax deductions for operating an office in the employee's home. An employee should seek advice from a tax advisor concerning in-home office deductions.

COVID-19 WORK OPTIONS PROGRAM—MANAGING COVID-19 WORK OPTIONS

Eligibility

It is State Fund's discretion to determine which employees are eligible to participate in the COVID-19 Work Options program. State Fund will attempt to accommodate those wishing to have a temporary work option based on availability of equipment and capacity of the network, and the determination that work duties can be performed from home.

Participating in the COVID-19 Work Options program is a privilege, not an employee right. An employee that is eligible to COVID-19 Work Options Program does not guarantee that their request to COVID-19 Work Options will be approved.

It is State Fund's intent to allow everyone who can, to work from home, but recognizes that this is not possible for some positions. Functions that require physical presence to perform effectively are not suitable for COVID-19 Work Options. To be considered for participation in the COVID-19 Work Options program, the following minimum criteria must be met:

Employee's job can be performed at home with proper equipment such as computer, monitor, phone and internet access, as determined by the employee's Program

Approval

Approval of an employee's COVID-19 Work Options request is subject to the Stages defined above, availability of equipment and network capacity, and verification that the work can be performed at home.

Scheduling	Managers and supervisors will follow these scheduling guidelines: State Fund employees who participate in the COVID-19 Work Options program are expected to work their regular schedule, but may be required to work alternate hours based on network capacity or other operational needs. COVID-19 Work Options participants must be accessible via telephone, voicemail, or e-mail, just as they are at the main office. COVID-19 Work Options employee's leave usage, overtime, or alternative work schedule policies will be consistent with those used for non-COVID-19 Work Options employees.
Types of COVID-19 WORK OPTIONS Schedules	State Fund provides for one COVID-19 Work Option schedule: For the duration of participation in the COVID-19 Work Options program, the employee will work from home, or at an alternate State Fund work location, 100% of the time, unless required by their job, such as for Board appearances. Schedules for participating employees may be staggered to accommodate more employees, while not straining the capacity of the network. Due to these extraordinary circumstances, participants may be asked to temporarily suspend their Alternate Work Schedule in order to accommodate as many employees as possible. It is expected that participation in the COVID-19 Work Options program may be temporary depending on the reason for the participation, such as a school closure. Employees covered under the Fair Labor Standards Act (FLSA) participating in the COVID-19 Work Options are expected to request time off and use leave credits for anything that takes them away from their work during their shift, such as medical appointments, running errands, or for whole day absences whether vacation days or sick days. Further, these employees are expected to follow normal practices for requesting time off based on their program's expectations. FLSA exempt employees are expected to keep their supervisor or manager apprised of their schedule and request time off, whether full or partial days, based on established practice in their specific program. An employee may request or continue a reasonable accommodation in accordance with State Fund policy and procedures, if feasible. Participants are expected to work with their supervisor and the Medical Management Unit in these situations.
Ending Participation	Participation in the COVID-19 Work Option Program will end when the Executive Committee determines the program is no longer necessary. At that time, all employees approved to telecommute under this program will return to their regular work locations, as soon as directed by their supervisor.

COVID-19 WORK OPTIONS PROGRAM – TECHNOLOGY, EQUIPMENT AND WORK PROCESSES	
Technology and Equipment Needs Overview	State Fund will provide the necessary equipment for employees approved to telecommute, including a laptop or desktop computer, monitor, cables, and VPN access as needed. An employee will be required to utilize their home internet, and may be required to utilize their personal phone for work calls or hotspot access. Before allowing a COVID-19 Work Options arrangement, the manager and/or supervisor and employee will determine the equipment needed for COVID-19 Work Options on a case-by-case basis. The types of technology services (internet services), access to state IT infrastructure and equipment that will be necessary to support the proposed COVID-19 Work Options arrangement must be identified. Managers and/or supervisors must: • Work with State Fund's Enterprise Security, and Information Technology in their locations, and Business Services Offices to assess COVID-19 Work Options technology hardware and software needs and to provide the necessary services, equipment and supplies to COVID-19 Work Options employees. The acquisition and furnishing of services, equipment and supplies (if applicable) shall be in accordance with all state laws, policies, standards and procedures including, but not limited to, the Information Systems Security Corporate Policy.
Office Supplies	Office supplies should be obtained through the COVID-19 Work Options employee's supervisor in conjunction with Shared Services.
Restricted Use	The employee acknowledges that the use of any State Fund provided equipment, software, data, and supplies is limited to authorized COVID-19 Work Options employee use and only for purposes related to State Fund business, or as allowed by law.

Return of Equipment	State Fund requires a COVID-19 Work Options employee to return all State Fund-owned equipment, software, data, and supplies when: ▪ The employee terminates employment with State Fund. ▪ State Fund terminates the employee. Upon notification that the COVID-19 Work Options arrangement will end or notification of employee separation, the manager and/or supervisor will review and compare the equipment and services checklist, provided on the COVID-19 Work Options Arrangement form, to ensure the equipment is returned and services are terminated.
Equipment Malfunction	If equipment malfunctions, the COVID-19 Work Options employee must notify his or her supervisor immediately. ▪ The COVID-19 Work Options employee is responsible for returning the malfunctioning equipment to the main office for repair. ▪ The State Fund IT Service Desk will provide telephone service and assistance to COVID-19 Work Options employees for State Fund-owned equipment and services. ▪ IMPORTANT: State Fund will not provide any at home service. When necessary, the COVID-19 Work Options employee is responsible for returning State Fund-owned equipment to State Fund for maintenance and repairs.
Work Products	State Funds owns any software, products, or data created as a result of work-related activities.

Work Environment	State Fund provides the opportunity to participate in a home COVID-19 Work Options program with the understanding that it is the responsibility of the employee to maintain a safe and productive work environment. ▪ Personal disruptions, such as non-business phone calls and visitors, should be kept to a minimum. ▪ The COVID-19 Work Options approval email confirmation shall identify work hours, and should be consistent with the employee's regular work schedule, unless an adjusted schedule is necessary as described above.
Health and Safety	State Fund expects COVID-19 Work Options employees to maintain the same safe working environment at the COVID-19 Work Options site as they would have at the main office. ▪ Resources on how to set up an ergonomic workstation are available on State Fund's Worksite
Work-Related Injury	If a COVID-19 WORK OPTIONS employee incurs a work-related injury, worker's compensation laws and rules apply just as they would if such an injury occurred at the main office. *Employees must notify their supervisors immediately and complete all necessary documents regarding the injury.*

Information Security	Security of information assets is of primary concern and importance to State Fund. Information security policies, standards and procedures serve to protect the availability, integrity and confidentiality of information assets. These policies, standards and procedures also serve to protect the agency, as well as its citizens and employees. For example, use of an improperly configured computer or wireless network computer may lead to unauthorized access, viruses and other forms of malicious code that may compromise the availability of computers and lead to data integrity and confidentiality issues. The loss or theft of a COVID-19 Work Options computer that is not encrypted and password protected may lead to data loss and confidentiality issues. The use of a personally-owned asset may expose the employee to privacy-related issues, such as all personal information, as well as work information, stored on the personally-owned device may become subject to disclosure under subpoena or legal action taken against the state. Therefore, it is essential that those engaged in COVID-19 Work Options arrangements are aware and understand the following: ▪ COVID-19 Work Options employees, like all State Fund employees, must adhere to all applicable laws, rules, regulations, policies, and procedures regarding information security. ▪ COVID-19 Work Options employees shall apply State Fund policies, standards and procedures including the Information Systems Security Corporate Policy and Privacy & Confidentiality Policy, to all State Fund information assets, State Fund equipment, software, and information used within the COVID-19 Work Options Program. ▪ State Fund reserves the right to monitor and log, without notice, all COVID-19 Work Options activity, including E-mail and Internet activities. COVID-19 Work Options employees, as with non-COVID-19 Work Options employees, should have no expectation of privacy in the use of computer related resources. Whenever a COVID-19 Work Options employee is unclear about the requirements of an information security policy, standard or procedure he/she should consult with their Supervisor and the State Fund Information Security Officer.

IT QUICK REFERENCE GUIDE FOR EMERGENCY TELEWORKING PROGRAM (ETP)

General Guidelines:

- All telework users must understand that due to limitations of the speed and performance of the Internet, the teleworker's experience when working remotely will not be the same as when working onsite at a State Fund campus.
- An Internet connection with appropriate bandwidth designated for teleworking should be made available at the teleworker's location. The bandwidth of this circuit must be **5Mbps** upstream and downstream.
- The teleworker must prohibit all non-work essential Internet activities from sharing the home network at all time when teleworking, including those from the teleworker's other household members. Examples of non-work essential Internet activities are: Video/audio streaming, moving watching, gaming, online shopping etc.
- Teleworkers are advised to use State Fund Webmail to check email whenever possible instead of using the VPN connection.
- Teleworkers are advised to avoid using their home WiFi or wireless connectivity whenever possible when teleworking. Instead, use the Ethernet LAN connection on the home router. An Ethernet LAN cable will be provided with State Fund supplied Desktop/Laptop for this purpose. If you do not have a cable, please notify your supervisor.
- Avoid using the Webcam feature when using Webex or video conferencing when teleworking. Use audio feature only during Webex or audio conferencing instead.
- The same State Fund IT Security Policies still apply when teleworking and there should be no installation of unauthorized software on State Fund devices at any time.
- Please try to troubleshoot any network connectivity issues at your home setup, including your home Internet connectivity, before contacting the IT Helpdesk.

Computer Equipment and Other Work Resources

- State Fund equipment will be assigned to the teleworker to utilize working remotely. The teleworker must exercise reasonable care for the equipment. Department approval should be obtained, prior to allowing State Fund owned equipment to be taken home or elsewhere for the purpose of teleworking.
- State Fund equipment should not be used for personal/other purposes beyond the incidental personal use it might receive if in the office.
- Printing and keeping physical copies of company documents will not be allowed.

Supported Business Applications

- Due to the emergency situation, not all business applications used within State Fund have been fully evaluated and certified for teleworking. Most applications may not experience issues when used in a telework setup, but some may experience unpredictable behavior. It is important that the teleworker files ESP tickets for any applications that they have experienced difficulties during teleworking and document their challenges with their direct supervisors.

Physical and Data Protection Best Practices

- Never work at public places such as a coffee shop, etc.
- Never connect to public or untrusted/insecure WiFi connection.
- Never disclose confidential or sensitive data to any unauthorized personnel including friends and family.
- Always lock your computer when leaving it unattended.
- Do not store sensitive or confidential information on your desktop or laptop. Instead, store any sensitive or confidential information on encrypted media approved by IT Security policies only.
- Ensure confidential paper documents are properly disposed of, i.e. shredding.
- Report security incidents or security concerns to IT helpdesk and your supervisor immediately.
- Refrain from using personal email for business use.
- Always comply with State Fund policies and procedures to protect specific high risk data elements required by the various regulations that State Fund has to be compliant with.

STATE COMPENSATION INSURANCE FUND®	**CORPORATE POLICY**	Number: **EC&F 2.0** Owner: **Governance, Compliance & Privacy** Type: **Ethics, Compliance & Fraud** Effective Date: **01/2020** Last Revision Date: **09/2017**
Title **PRIVACY & CONFIDENTIALITY**		

SECTION 1 – PURPOSE

- To fulfill State Fund's legal duty to protect the privacy rights of our Workforce members, policyholders, injured workers, and third parties.
- To establish the framework for authorized collection, access, use, and sharing of personal or confidential information.

SECTION 2 – POLICY STATEMENTS

In its normal business operations, State Fund accesses, creates, and collects personal and confidential information about policyholders, injured workers, and third parties.

As an employer and contractor for services, State Fund also collects and keeps personal and confidential information about its Workforce.

2.1 Information Practices

State Fund's business operations follow the Federal Trade Commission's Fair Information Practices Principles when it applies.

2.1.1 Notice and Awareness

State Fund:

- Workforce members are responsible for understanding:
  - Laws and policies that define personal/confidential information.
  - Disclosure standards applicable to the information for which they have access to and use.
- Requires a clearly defined purpose when personal information is collected.

2.1.2 Consent and Choice

State Fund:

- Requires its Workforce members to use personal information only for the specific purpose collected.
- Requires consent from data owners when personal information is used for purposes other than when the information was originally collected.

2.1.3 Access

State Fund:

- Requires its Workforce members to access, view, and disclose personal information State Fund possesses only as permitted by law or policy and as necessary to perform their job duties.
- Provides a way for employees, policyholders and injured workers to modify or correct personal information that State Fund keeps about them.

2.1.4 Data Integrity and Security Measures

State Fund:

- Requires its Workforce members to protect personal information by methods that restrict access, destruction, use, modifications or disclosure.
- Discloses personal information to its Workforce only as needed to perform business or meet its legal obligations.
- Does not disclose, sell, trade or otherwise transfer customer or third-party personal information to others for any third party's commercial purposes.
- May disclose personal information when the law requires.

2.2 State Fund Workforce Responsibilities

Each State Fund Workforce member must:

- Limit the use of personal or confidential information to business needs.
- Report as soon as possible the suspected unauthorized disclosure of personal or confidential information.
- Electronically certify that they have read and understand this Policy when they acknowledge State Fund's Code of Conduct.

2.2.1 Reporting Privacy/Confidentiality Incidents

Report suspected unauthorized access, use, or disclosure of personal and confidential information through the Privacy Hotline 24/7 by toll-free phone at **866-294-1742,** or online**,** or directly to PrivacyOffice@scif.com. Anonymous reporting is available.

2.3 Use of State Fund Computer Systems

Use of State Fund computer systems for the transmission of personal and confidential information for non-State Fund business purposes is prohibited except for:

- Accessing State Fund sponsored programs and State websites, which are considered business related activities and classified as "State Fund business purposes". Websites related to these activities may be accessed using State Fund equipment.

- Personal electronic devices and personal accounts must not be used to send or receive Writings during the course of conducting State Fund business, except as directed or allowed by State Fund.

2.4 No Expectation of Privacy for State Fund Property and Information Systems

State Fund:

- Controls or owns records created, stored or transmitted with its Information Systems, unless contract or law provides otherwise.

- Has the right to:
  - Access
  - Review
  - Inventory
  - Monitor and
  - Use

any records, property, and information stored, generated or communicated through its Information Systems or at its locations without notice to Members as federal and state law allows.

2.4.1 Information Stored

State Fund Workforce members cannot expect personal privacy for information stored or transmitted on or through State Fund Information Systems or stored at property owned by State Fund.

2.5 Use of Anonymized or Aggregated Information

State Fund:

- May use information about Workforce members, policyholders, injured workers, or third parties for statistical research or reporting purposes.
- Publicly disclosed results or reports shall exclude personal information.

2.6 Investigation Cooperation

State Fund:

- Cooperates with law enforcement agencies investigating suspected illegal use of State Fund resources.
- May release information to law enforcement agencies without notice to customers or third parties as allowed by law or valid legal order.
- Reports any activity it reasonably believes fraudulent or otherwise illegal to law enforcement agencies along with relevant private/confidential information.

2.7 Privacy Shield Statement

State Fund aligns its practices with the data protection principles of the EU-U.S. Privacy Shield Framework when consistent with State Fund business needs and operations.

SECTION 3 – APPLICABILITY, SCOPE, & BASIS

The policy applies to all members of the State Fund Workforce.

3.1 Related Laws and Regulations

Complete text of the California statutes is available at: http://leginfo.legislature.ca.gov/.

Complete text of the California regulations listed below is available at:
http://ccr.oal.ca.gov/linkedslice/default.asp?SP=CCR-1000&Action=Welcome

Cal. Bus. & Professions Code, §§ 22575-22579, Online Privacy Protection Act of 2003;
Cal. Civil Code, §§1798 et seq., Information Practices Act of 1977
Cal. Financial Code, §§ 4050, et seq., California Financial Information Privacy Act
Cal. Government Code, §§ 6250 et seq., California Public Records Act
Cal. Insurance Code, §§ 791 et seq.,Insurance Information and Privacy Protection Act
Cal. Code of Regulations, Title 10, §§ 2689 et seq., California Privacy Regulations

SECTION 4 – AUTHORITY

The Chief of Internal Affairs is responsible for policy assurance and oversight. The Governance, Compliance & Privacy Program Manager is the policy owner responsible for complying with, updating, and enterprise monitoring of this Corporate Policy.

State Fund's Privacy Office has the authority to:

- Respond to privacy concerns, questions, and complaints from all sources.
- Develop, coordinate, and maintain State Fund's Privacy Incident Response Plan.
- Notify affected persons as necessary.
- Develop and deploy programs to prevent and detect privacy incidents.
- Monitor handling of personal information by State Fund business units.

SECTION 5 – RELATED CORPORATE POLICIES

EC&F 2.1 Complaint Reporting and Anti-Retaliation
EC&F 2.5 Intellectual Property
GOV 1.4 Records and Information Management
IT 6.1 Information Security

Related Corporate Policies can be found: Corporate Policy Library

SECTION 6 – DEFINITIONS

Confidential Information – Information about State Fund, a State Fund Workforce member, State Fund policyholder or Injured worker, or a third party that is not generally known or is otherwise legally protected.

Devices – Devices include: computer equipment, telephones, voice mail, fax machines, wireless devices, cell phones, copiers, scanners, Global Positioning System (GPS) trackers, and any other similar means of communication technology currently in use. Information formats include: oral; electronic; telephonic; magnetic; video; audio; or paper.

EU-U.S. Privacy Shield Framework- The framework based on Privacy Principles issued by the U.S. Department of Commerce in conjunction with the European Commission (EU) to foster, promote, and develop international commerce.

Fair Information Practices Principles – Principles adopted at the national level guiding the collection, use, and safeguarding of personal information.

Information System – An organized collection, storage, processing, and presentation system of data and other knowledge for decision-making, reporting, and planning and evaluating programs. It can be either manual or computerized, or a combination of both.

Personal Information – Information that can be used alone or with reference to another source to identify, contact, or locate an individual. Personal information does not include publicly available information lawfully made available to the general public from federal, state, or local government records.

Personal Information includes, but is not limited to:

For any individual - Information, which alone (e.g. no reference to another source is needed), or in combination with an individual's name if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

- **Examples under California law:**
  Includes without limitation: An individual's name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information, tax identification number, military identification number, any other government-issued identification number, biometric data from measurements or technical analysis of characteristics used for authentication, such as fingerprints, retina patterns, or iris images.

For Policyholders: Any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit information or any other personal characteristics.

Property – Objects, devices, information, or material found in State Fund information systems or at its locations. Locations include:

- Buildings owned, occupied, leased or rented by State Fund
- Desks, filing cabinets, and other physical storage equipment
- State Fund-owned or -issued vehicles

State Fund Workforce – The term 'State Fund Workforce' is used herein solely for purposes of describing a collective group of people working at State Fund, including Board members, officers, employees, and non-employees. No employer-employee or agency relationship is intended or created by using the term. Using the term has no impact on State Fund's relationships with consultants or independent contractors.

State Fund Business Purposes:

State Fund sponsored activities –include Savings Plus, Employee Benefits, Tuition Reimbursement, Wellness, Employee Engagement, Employee Emergency Notification (EEN), State Fund Store, Strategic Alliance partners (American Cancer Society, Kids Chance California).

State of California Websites- include CA Department of Human Resources (CalHR), CA Public Employees Retirement System (CalPERS), and CA State Controller's Office

Valid Legal Order – A court-issued order or one that has other legal force.

Writings: Means any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.

SECTION 7 – HELP & ADVICE

For help and advice regarding this Corporate Policy, privacy and security issues or Privacy & Confidentiality procedures, contact the Governance Department's Privacy Office at **PrivacyOffice@scif.com** or toll-free during business hours at **1-888-724-3237**.

SECTION 8 – REVIEW HISTORY

Review Date	Action Date	Action	Section(s) Revised	Effective Date
05/06/2011	05/06/2011	Final QA –dept. change	New	05/2011
04/30/2012	04/30/2012	Annual Review. Added 2.2.1 *Private Information Collection & Use*; 2.2.6 *Safeguards*; In 2.3.2 added "stored or transmitted on or through State Fund Information Systems" Moved section 2.4 *State Fund PrivacyOffice* to section 4 - *Authority*	2.2.1; 2.2.6; 2.3.2; 4	07/2012
02/28/2013	02/28/2013	Annual review: alignment with Fair Information Practices Principles; compliance notice revision	2 and 6	03/2013
04/11/2017	06/20/2017	Annual Review: Added additional Fair Information Practices Principles, updated definitions of personal information to align with Civil and Insurance Codes.	2 and 5	09/2017
06/20/2017	06/20/2017	PAG review and approval	2 and 5	09/2017
07/03/2017	07/03/2017	Executive approval	2 and 5	09/2017
08/29/2017	08/29/2017	Board approval	2 and 5	09/2017
10/30/2019	10/30/2019	Annual Review: Added 2.3 Section; Use of State Fund equipment in IT 6.1 Corporate Policy Section 6: Added data elements to the definition of personal information, AB 1130	2.3 and 6	01/2020
11/07/2019	1/10/2020	PAG Review and Approval	2.3 and 6	01/2020
01/17/2020	01/17/2020	Executive Approval	2.3 and 6	01/2020

STATE COMPENSATION INSURANCE FUND	**CORPORATE POLICY**	Number: **IT 6.1** Owner: **ENTERPRISE SECURITY** Type: **INFORMATION SECURITY** Effective Date: **07-2018** Last Revision Date: **01-2014**
Title **INFORMATION SYSTEMS SECURITY**		

SECTION 1: PURPOSE

This policy supports State Fund's commitment to protect the confidentiality, integrity, and availability of State Fund information assets and to comply with regulatory and legal requirements related to Information Security.

SECTION 2: POLICY STATEMENTS

State Fund information and applications shall be protected in a manner commensurate with their sensitivity, value, and criticality.

Information Security policies, standards and procedures shall be followed to maintain the confidentiality, integrity, and availability of State Fund information.

2.1 Information Security Awareness

Communication to the organization about information security awareness will be periodically issued addressing best practices and Information System user responsibilities.

2.2 Authorized State Fund Information System User Responsibilities

Authorized users of State Fund's Information System shall adhere to all applicable legal, statutory, regulatory, contractual requirements, and internal State Fund policies and procedures.

2.3 Infrastructure

State Fund's Information System and network infrastructure are designed and implemented to protect State Fund and third parties information. Members of the State Fund Workforce are responsible for the protection of private, confidential, and operational information.

2.3.1 Use of State Fund computer systems for the transmission of private information for non-business purposes is prohibited.

- Personal electronic devices and personal accounts should not be used to send or receive tangible writings during the course of conducting State Fund business.

2.4 Computer Hardware, Software, and Equipment

2.4.1 Only authorized hardware, software, and supporting equipment is allowed for use on State Fund systems.

2.4.2 Authorized hardware, software, and supporting equipment purchased or obtained by State Fund shall be used only for State Fund business purposes.

NOTICE
All members of the State Fund Workforce are required to electronically certify that they have read and understand the *State Fund Systems – Proprietary System Notice* as part of State Fund's *Code of Conduct* acknowledgement process. Failure to complete this obligation will result in referral for disciplinary action up to and including termination.

2.4.3 State Fund may remove any unauthorized software or hardware from its systems or premises without notice.

2.5 Reporting Information Security Incidents
Members of the State Fund Workforce shall report information security incidents upon discovery.

SECTION 3: APPLICABILITY, SCOPE, & BASIS
This policy applies to all members of the State Fund Workforce.

3.1 Related Laws and Regulations
This policy is developed in accordance with federal and state law, including: Cal. Civil Code §§ 1798.29 and 1798.82, Security system breach disclosure
Cal. Financial Code §§ 4050, et.seq California Financial Information Privacy Act
15 USC §§ 6801-6809, 6821-6827, Financial Services Modernization Act of 1999
Cal. Civil Code § 1798.3(a) and § 1798.80(e) Personal Information
Cal. Insurance Code, § 791.02(s) Personal Information
Cal. Evidence Code § 250 Writings
Cal. Government Code §§ 6252(e) and §§ 6252(g) Writings

SECTION 4: AUTHORITY
The Chief Information Officer (CIO) is responsible for policy assurance and oversight. The Chief Information Security Officer (CISO) as policy owner is responsible for compliance with, updates to, and enterprise monitoring of this Corporate Policy and its related IT Information Security Sub-Policies and Standards.

SECTION 5: RELATED CORPORATE POLICIES
EC&F 2.0 Privacy & Confidentiality
EC&F 2.5 Intellectual Property
GOV 1.4 Records and Information Management
GOV 1.8 Data Classification
S&BC 7.3 Business Continuity

Related Corporate Policies can be found: Corporate Policy Library

SECTION 6: DEFINITIONS
Confidential Information – Information about State Fund, a State Fund Workforce member, State Fund policyholder or claimant, or a third party of such nature that it has independent

economic value from not being generally known to the public.

State Fund confidential information includes, but is not limited to marketing strategy or research, information related to rates and rate setting, short and long term business planning, trade secrets, investment strategy, claims handling policies and procedures, information related to real estate transactions and any other confidential information that would give a competitor an unfair advantage if it were released.
State Fund policyholder confidential information includes, but is not limited to, wage, salary and tax information, trade secrets, financial statements, credit reports, or any other information that the insured has lawfully designated as proprietary or trade secret.

Confidentiality, Integrity and Availability:

- **Confidentiality:** A set of rules that limits access or disclosure of information only to authorized individuals, entities, and processes.
- **Integrity:** Assures information as trustworthy, accurate, and complete over its entire life-cycle without being modified in an unauthorized or undetected manner.
- **Availability:** Guarantee of reliable access to information by authorized people. The computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must function correctly.

Information Security Incident / Event:

- **Security incident:** An adverse event that threatens the confidentiality, availability, or integrity of a State Fund system or the data stored on such a system that requires Information Technology Subject Matter Experts (SMEs) action and has a negative impact that adversely affects finances, reputation, non-public data, or intellectual property. It violates State Fund information technology security policies and standards.
- **Security event:** An attempt to cause a security incident stopped by preventive measures such as firewall, anti-virus software, or intrusion prevention system. A failed security event is not considered a security incident.

Information System – An organized collection, storage, processing and presentation system of data and other knowledge for decision making, reporting, and for planning and evaluation of programs; this can be either manual or computerized, or a combination of both.

Operational Information – Information intended solely for use by State Fund employees. Operational is the default classification of State Fund data.

Private Information – includes, but is not limited to:

a. **For State Fund Workforce Members –** Information that identifies or describes an individual, including but not limited to, his or her social security number, physical description, home address, home telephone number, education, financial matters, and medical and employment history. It includes statements made by, or attributed to, the individual. *Private information does not include information about civil service employees which is disclosable under California law, including but not limited to the California Public Records Act and Fair Political Practices Act.*

b. **For Policyholders, Claimants, and Third parties –** Any individually identifiable

information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit information or any other personal characteristics. It includes an individual's name and address, and medical record information.

State Fund Workforce – The term 'State Fund Workforce' is used herein solely for purposes of describing a collective group of people who work for State Fund, including Board members, officers, employees, and non-employees. No employer-employee or agency relationship is intended or created by the use of the term. The use of the term has no impact on State Fund's relationships with consultants or independent contractors.

Writings: Means any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.

SECTION 7: HELP & ADVICE

Phone the IT Service Desk at (877) 782-7338 or email Enterprise Service Point.

SECTION 8: REVIEW HISTORY

Review Date	Action Date	Action	Section(s) Revised	Effective Date
10/2011	10/2011	Final QA	Comprehensive	10/2011
06/2013	06/2013	Annual Review & QAP	Section 2.3; 2.3.1; 2.4.2;, 6 & 7	
09/2013	09/2013	Approval	As above	01/2014
05//2018	06/2018	Comprehensive Review	All	07/2018
06/2018	06/2018	ISAC and CISO Approval	All	07/2018
07/2018	07/2018	PAG Review	All	07/2018