

Information System Security and Confidentiality Acknowledgement (ISSCA)

CalPERS provides access to electronic resources, information, capabilities, and functions (electronical assets) to enable the proper conduct of CalPERS business. Access to electronic assets is only granted to individuals that agree to comply with the Information Security Code of Conduct specified below. Failure to comply with this Code of Conduct may result in termination, civil or criminal prosecution, or the loss of access to CalPERS electronic assets.

By initialing each section of the Information Security Code of Conduct, I demonstrate I have read and agree to abide by the following:

Information Security Code of Conduct

Acceptable Use

- I will only use electronic assets in ways approved by CalPERS management.
- I will only use CalPERS electronic communication systems (e.g., email, messaging, social media) when conducting CalPERS business. I will never use any other electronic communications systems to send or received CalPERS business information.
- I will only use my assigned User ID when accessing electronic information assets and systems, unless I have obtained approval from the Information Security Office to use another User ID.
- I will not disclose the secret information (e.g., passwords, PINs, security tokens) that protects my CalPERS electronic identity (User ID), as I am responsible for all actions that are performed by that User ID.
- I will only access and modify information assets and systems that CalPERS management has approved for my use (for business related purposes only).
- I will not access any CalPERS information (electronic or paper) that pertains to me, my relatives, my associates, or my friends without the explicit approval from CalPERS management.
- I will limit the physical access to the information assets and systems I control to only authorized persons (for business related purposes only).
- I will restrict access to electronic information assets and systems to only individuals that are authorized to view or use that information (for business related purposes only).
- I will not use information assets and systems for personal benefit, political activity, unsolicited advertising, unauthorized fundraising, or for the solicitation of performance of an activity that is prohibited by any local, state, or federal law.
- I will not use information assets and systems for any unlawful, invasive, infringing, defamatory, or fraudulent purpose.

- I will not use information assets and systems to violate or encourage the violation of the legal rights of others.
- I will not engage in activity that may degrade the performance of information resources; deprive an authorized user access to CalPERS resources; obtain extra resources beyond those allocated; or circumvent CalPERS security measures.
- I will not download, install, or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of CalPERS computer resources, unless approved by CalPERS Information Security Office.
- I will not use hardware and software on CalPERS systems and/or networks unless it has been approved by the CalPERS Information Technology Services Branch.
- I will dispose of all electronic media (e.g., CDs, DVDs) containing confidential information by physically destroying the media.
- I will not make unauthorized copies of copyrighted or CalPERS owned software.
- I will regularly review and comply with CalPERS Information Security policies, procedures, and control standards.
- I will contact the Information Security Office if I have any questions regarding acceptable use compliance.

Initial: _____

Incidental Use

- Government Code Section 8314 permits incidental personal use of state resources. At CalPERS, this means:
- I will restrict all incidental use of electronic mail, internet access, fax machines, printers, and copiers to only CalPERS approved users, which does not include family members or others not affiliated with CalPERS.
- I will not participate in incidental use that may result in direct costs to CalPERS, cause legal action against, or cause embarrassment to CalPERS.
- I will not participate in incidental use that interferes with my performance of work duties.
- All storage of personal email messages, voice messages, files, and documents within my authorized CalPERS computer resources will be nominal.
- I will contact the Information Security Office if I have any questions regarding incidental use compliance.

Initial: _____

Reporting

- I will report any information security violations I become aware of to my Manager/Supervisor and/or the Information Security Office. This includes unauthorized access to information, capabilities, or systems; unauthorized disclosure of information; and unauthorized modification or destruction of information.
- I will report any unapproved software or hardware being used in CalPERS electronic information systems and/or networks to my Manager/Supervisor and/or the Information Security Office.
- I will report any security weaknesses I find that could result in a security violation to my Manager/Supervisor and/or the Information Security Office.

Initial: _____

Monitoring/Enforcement

- I understand that electronic assets owned, leased, administered, or otherwise under the custody of control of CalPERS are the property of CalPERS.
- I understand that CalPERS reserves the right to monitor and/or log any usage of electronic assets.
- I understand that the information stored on CalPERS systems can be viewed, copied, and removed by CalPERS management without notice.
- I understand that information on CalPERS systems may be disclosed as required by law or for use in disciplinary action.
- I understand that a violation of the Information Security Code of Conduct may result in disciplinary action that may include termination, civil or criminal prosecution, or loss of CalPERS electronic asset access and privileges.

Initial: _____

For Third Parties Only

I attest that I have been provided and have completed annual basic security and privacy awareness training. My certification of completion is attached.

Consulting Firm Name:		
Contract/LOE Name:		
Contract/LOE #:		
Contract/LOE Term Dates (mm/dd/yyyy):	Start Date:	End Date:
Contract Manager Name:		
		Initial:

Endorsement

Name (print):	
Signature:	Date:
Branch/Division:	Phone:
Supervisor/Contract Managers Signature:	
Name:	
Signature:	Date: