State of California

California Department of Technology

Office of Information Security

Remote Access Agreement

SIMM 5360-B

January 2018

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**December 2010**	**California Office of Information Security**	
Minor Update	**September 2013**	**CISO**	**SIMM number change**
Minor Update	**January 2018**	**Office of Information Security (OIS)**	**Office name change**

Employee Name:		Office/Branch:	
Employee Telephone:		Employee Email Address:	
Supervisor/Manager Name:		Supervisor/ Manager Email Address:	
Supervisor/Manager Telephone:			

This agreement is to be used in lieu of a Telework Agreement when an employee is authorized to establish a remote access connection to IT infrastructure for work-related functions which fall outside the realm of a traditional telework arrangement, such as use of a Smartphone or other mobile computing device which establishes a remote access connection to state IT infrastructure. As with any casual or formal telework arrangement, the employee, Supervisor/Manager and Office Chief are to acknowledge they have read, understand and agree to adhere to all applicable state policies, standards and procedures including, but not limited to the agency's Acceptable Use Policy, the Telework and Remote Access Security Standards (SIMM 5360-A) and applicable provisions of the Telework Program Policy and Procedures. Applicable provisions of the Telework and Remote Access Security Standard and Telework Program Policy and Procedures include but are not limited to the following:

- Maintaining established security controls, such as strong passwords, two-factor authentication, device and data encryption, antivirus and antispyware software, personal firewalls, content filtering software and automatic updates;
- Electronic registration of device information;
- Disabling of non-essential functions and services on the device;
- Not altering, disabling or circumventing established security controls;
- Maintaining back-ups, only in accordance with authorized state entity procedures;
- Allowing IT Administrators to define, manage and validate device security controls;
- Providing IT Administrators the ability to issue remote data wipe and device kill commands in order to protect the confidentiality of state data residing on the device, and;
- Immediately reporting the loss, theft or damage of the device.

The following assets are authorized and will be used to make remote connections:

Make	Model	Asset Identification

The following state information systems will be accessed remotely with the above referenced assets:

I have read, understand and acknowledge the state entity Telework Program Policy and Procedure and state Telework and Remote Access Security Standard. I also understand that when my use of any personal computing equipment is authorized by the state entity for remote access purposes, this use may result in a lack of privacy related to those items.

Employee Signature:		Date:	
Supervisor/Manager Signature:		Date:	
Entity Head Signature:		Date:	