



Computing Systems Use Acknowledgement For Non-SCE Personnel



As a condition of granting use of its **telecommunications, computing and information systems**, including, but not limited to, computers, servers, applications, files, electronic mail, instant messaging services, electronic equipment, wireless devices, data resources, and SCE-sponsored connections to the Internet communications network (collectively, "SCE Computing Systems"), Southern California Edison (SCE) requires that each individual read, understand and acknowledge by signing, this Computing Systems Use Acknowledgement (CSUA).

1. SCE grants you access to SCE Computing Systems and related resources solely so you can perform SCE-related business, and access and transmit/receive business-related information.

2. You will not use SCE Computing Systems in a manner that disrupts SCE business, is offensive to others, or violates SCE's Equal Opportunity or Sexual Harassment policies.

3. You will not:

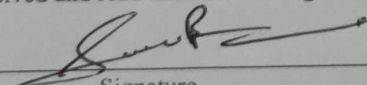
- Store or use unapproved software on SCE Computing Systems.
- Disclose, share with, or allow another to use your IDs, passwords and dial-up numbers, except as required by authorized IT personnel to resolve technical issues.
- Knowingly introduce illegal or destructive code into SCE Computing Systems.
- Copy, transfer or sell SCE-developed or licensed software, data, information or documentation to unauthorized systems or destinations.
- Employ unapproved data encryption schemes on SCE Computing Systems.
- Install SCE-licensed software on any device not owned or approved for such installation by SCE.
- Store confidential SCE data or information on any unauthorized device or media.
- Have any unauthorized software, including mobile software, on any portable storage media that is attached to SCE Computing Systems.
- Install unauthorized hardware or software on SCE-owned equipment (including wireless devices).

4. You should be aware that SCE continuously monitors activities on SCE Computing Systems. Security monitoring extends to personal or other non-SCE devices or media while they are attached to SCE Computing Systems. Monitoring can include all information and communications stored, transiting or that has transited thereon, including erased or deleted files that may still be recovered by SCE and communications stored by a third party for which you are the sender or intended recipient, whether protected by SCE-assigned or personally-selected passwords. SCE may remove any material stored on SCE Computing Systems that it deems offensive or inappropriate. By using SCE Computing Systems, you consent to such monitoring. You should have no expectation of privacy when using SCE Computing Systems or personal or non-SCE devices or media attached to SCE Computing Systems.

5. Remote connections to SCE Computing Systems require authorization and an SCE assigned VPN token or SCE authorized remote access software on a computer/tablet/laptop/cell phone that has up to date antivirus capability and that is allowed under your employer's contract with SCE or is otherwise authorized by SCE.

6. Violations of SCE policies or this CSUA may lead to loss of access privileges and could result in SCE reporting your behavior to your employer. SCE will report unlawful activities to the appropriate enforcement/regulatory agencies.

I have received and read this acknowledgment.


Signature

09/18/2024

Date

Parwar, Sourabh
Print Name (Last, First, Middle Initial)