Any Connected Entity (CE) requiring connection to California ISO networks via the Energy Communications Network (ECN) shall comply with the security requirements described below to ensure the integrity and protection of its networks and the confidentiality and integrity of information being transmitted.

1. Only authorized and properly authenticated CE personnel shall be allowed to use the hosts and workstations that are used to access California ISO networks.

2. The CE workstation or LAN(s) connecting to California ISO networks must be logically and/or physically isolated from other CE LANs and the Internet. Firewalls or other appropriate boundary security controls should be used.

3. The CE access points to the ECN must be configured to allow only those TCP/IP packets that are absolutely required and which originate from the specifically designated California ISO network access hosts, workstations and equipment.

4. Each party is responsible for protecting their internal networks from all unauthorized traffic via the external connections in accordance with the objectives in both the CAISO Information Security Requirements and NERC Cyber Security Standards.

5. As a matter of course, authorized and properly authenticated California ISO personnel shall conduct network problem diagnosis and administrative functions that include monitoring, scanning, and auditing of California ISO networks (and traffic to such California ISO networks) using manual and automated software tools or coordinated physical inspections. Such automated functions shall be conducted only from the California ISO sites. The California ISO shall have the right to obtain such information from the CE such that the California ISO can ensure that all CE infrastructure connections to California ISO networks are authorized, and that the CE has implemented appropriate firewall, patch, and anti-virus measures. Monitoring, scanning and auditing activities undertaken by the California ISO as to CE will be limited to the links between the CE and the California ISO networks. Furthermore, such monitoring, scanning and auditing activities shall be limited to ensuring compliance with this Network Connectivity Security Requirements Agreement and will be coordinated with designated members of the CE information security staff in advance. The CE expressly consents to such monitoring, scanning and auditing as described above. Any proprietary or other information of the CE obtained as a result of such monitoring, scanning, and auditing will be kept in strict confidence, will not be disclosed to third parties, and will be used by the California ISO only for the purposes set forth in this paragraph.

6. Each CE shall be responsible for any network activity that originates from or passes through its premises into the others network. If, in the course of conducting network problem diagnosis and administrative functions, the California ISO or the CE discovers evidence of possible malicious activity originating from its facilities, the party discovering such activity (the "Notifying Party") will immediately notify the other party and provide information as to such evidence (to the extent the Notifying Party determines that providing such information does not increase the likelihood of further malicious activity). The other party may ask for the Notifying Party's assistance in investigating the malicious activity and may request the Notifying Party to take additional precautionary measures if warranted. If this joint investigation reveals possible evidence of criminal activity, upon the written consent of the Notifying Party, that evidence will be provided to the appropriate law enforcement agency.

7. If, as a result of the joint investigation, a party claims that the malicious activity resulted from negligence on the part of the other party and if the claiming party wishes to pursue a remedy for any resulting damages, the parties involved agree to adhere to the dispute resolution procedures of section 13 of the ISO Tariff in connection with such claim.

8. ISO Tariff Section 14, Force Majeure Indemnification and Limitations on Liability shall apply to all CAISO responsibilities stated herein.

9. ISO Tariff Section 22.8, Applicable Law and Form, and 22.9, Consistency with Federal Laws and Regulations, are incorporated herein by reference.

On behalf of the undersigned CE, I have read this Network Connectivity Security Requirements Agreement and agree to comply with them and read and review annually. These security requirements are in effect as of the date of connection.

Print Name and Title	Resource Owner Company Name	Division or Department

Signature	Date

Where Applicable:

Project Name	NRI/New Resource Interconnect ISO Internal Tracking #

Additional Comments: