
	Corporate Policy Information Security	Review Date No.:	03/23/07 TBD
	Network Connectivity Security Requirements and Agreement	Version No.:	v 3.4
		Effective Date	10/01/2003

A Communication Subscriber (CS) requiring direct connection to California ISO networks shall comply with the security requirements described below to affect the integrity and protection of its networks and the confidentiality and integrity of information being transmitted.

1. Only authorized and properly authenticated CS personnel shall be allowed to use the hosts and workstations that are used to access California ISO networks.
2. The CS workstation or LAN(s) connected to California ISO networks must be logically and/or physically isolated from other CS LANs. If the workstation or LAN is not physically isolated, firewalls or other appropriate security mechanisms should be used.
3. The CS access router must be configured to allow only those TCP/IP packets that originate from the designated California ISO network access hosts and workstations.
4. The CS is responsible for protecting its internal networks from unauthorized traffic from the Internet in accordance with the objectives in both the California ISO ECN Policy 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 including monitoring, scanning, and auditing of California ISO networks (and traffic to such California ISO networks) using automated software tools. Such automated functions shall be conducted only from the California ISO site. The California ISO shall have the right to obtain such information from the CS such that the California ISO can ensure that all CS infrastructure connections to California ISO networks are authorized, and that the CS has implemented appropriate firewall, patch, and anti-virus measures. Monitoring, scanning and auditing activities undertaken by the California ISO as to CS will be limited to the link between the CS 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 CS information security staff in advance. CS expressly consents to such monitoring, scanning and auditing as described above. Any proprietary or other information of the CS 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. If, in the course of conducting network problem diagnosis and administrative functions, the California ISO or the CS 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 responsibilities stated herein.
9. ISO Tariff Section 22.8 and 22.9, Consistency with Federal Laws and Regulations, are incorporated herein by reference.

	Corporate Policy Information Security	Review Date No.:	03/23/07 TBD
		Network Connectivity Security Requirements and Agreement	

On behalf of the undersigned CS, 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	CS Company Name	Division or Department
----------------------	-----------------	------------------------

Signature	Date
-----------	------