

	Corporate Policy Information Security	Review Date No.:	06/20/06 TBD
		Internet Connectivity Security Requirements and Agreement for Data Processing Gateway Devices	

A Connecting Entity (CE) using an approved Data Processing Gateway (DPG) device and connecting directly to the Internet to transmit information to CAISO shall comply with these security requirements to ensure the integrity and protection of their respective networks and the confidentiality and integrity of information being transmitted.

1. It is *strongly recommended* that only authorized and properly authenticated personnel of the CE shall be allowed to access and use the DPG connected to the Internet.
2. It is *strongly recommended* that the CE's DPG connected to the Internet should be logically and/or physically isolated from other internal networks and LANs. If the DPG is not physically isolated, then firewalls or other appropriate security mechanisms should be used with the concurrence from CAISO's Information Security department.

REQUIREMENTS:

3. The access points to the DPG must be configured to only allow traffic that originates from the designated access hosts, workstations or other equipment. A network diagram depicting the topology and security devices must be included with the DPG engineering package submitted for each site. Future changes to the network topology affecting the DPG must be submitted to CAISO for review.
4. Each party is responsible for protecting their internal networks from unauthorized traffic from external connections in accordance with the NERC Security Standards.
5. As a matter of course, authorized and properly authenticated CAISO personnel shall conduct network problem diagnosis and administrative functions including monitoring, scanning, and auditing network connections, using automated software tools or physical inspection. Such automated functions shall be conducted only from a CAISO site. Physical inspections of the DPG will be coordinated with the CE. The intent of the monitoring, scanning, auditing activities and physical inspections is limited to ensuring all connections to CAISO networks are authorized. Furthermore, the activities shall be limited to ensuring compliance to the CAISO Internet Connectivity Security Requirements for DPG Devices and will not include penetration testing. CEs using DPGs to connect to the Internet expressly consent to such monitoring, scanning, auditing, and physical inspections.
6. Each party will be held responsible for results of any network activity that originates from its premises or passes through its premises into the others network. If, in the course of conducting network problem diagnosis and administrative functions, one party discovers evidence of a possible security incident originating from the other party's device, that party will be immediately notified and asked to assist in an investigation of that incident and take precautionary measures if warranted. If this joint investigation reveals possible evidence of criminal activity, 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 security incident 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, Liability and Indemnification shall apply to all responsibilities stated herein.
9. ISO Tariff Section 20.7, 20.8, Consistency with Federal Laws and Regulations, are incorporated herein by reference.

I/we have read the California ISO Internet Connectivity Security Requirements and Agreement for DPG Devices and agree to comply with them and review annually. These security requirements are in effect as of the date of connection.

Print Name and Title	Company Name	Division or Department
Signature		Date