CITADEL
INFORMATION GROUP, INC.

Information Security Guiding Principles

1. Our company is committed to protecting the private sensitive information that members of our community have entrusted to us.
2. We protect information because we are legally obligated to do so, it is ethically correct, and our clients and staff expect it of us.
3. Our company has appointed a *Chief Information Security Officer* (CISO) who is responsible for managing information security at our company.
4. All information has an *Information Owner* as defined by our information security policies. The *Owner* is a staff member responsible for the protection of that information. *Owners* classify information into three sensitivity buckets:
   - Public
   - Internal Use Only
   - Restricted

   Owners identify staff and other users who they authorize to have access to that information.
5. Staff is expected to protect information commensurate with the consequences of its loss or exposure and in accordance with instructions from the information *Owner*.
6. Staff is only allowed access to information for which they have been authorized access and for which they have a need-to-know.
7. Staff is to share sensitive information only with others who are authorized to access it and who have a need-to-know.
8. Staff is to use information only for purposes expressly authorized by the information's *Owner*.
9. Staff is to comply with security requirements identified by the CISO. These include:
   a. Use of strong passwords
   b. Encrypting confidential information when sent via email or transported off site
   c. Special rules for laptops, PDAs, USB drives and other portable devices
   d. Properly securing sensitive information when printed on paper.
10. Staff is to be alert to their surroundings, be wary of potential intruders and other perceived dangers to our offices (physical security).
11. Staff is never to leave sensitive documents unattended or unlocked.
12. Staff will take information security awareness training at least annually.
13. Except for designated IT staff, staff is not to make changes to workstations, servers, and other IT devices. This includes adding or downloading software.
14. In the event of a security incident, staff is to immediately contact the IT Department.

www.citadel-information.com
2060 Hercules Drive
Los Angeles, CA 90046
Tel: 323.876.1441
Fax: 323.876.7794