Internet Security Policy

Our goal is to protect our client's assets, information, integrity and reputation from potential threats. We recognize that secure operations are dependent upon our participation, commitment and accountability. Therefore we adhere to general principles laid out below which provide the basis of conduct and framework to the ever-changing landscape of internet security.

1. The security and protection of employees must be the overriding priority of all business activity.
2. Security policies and procedures must be implemented according to regulation and guidelines provided by the State of California and the SEC.
3. Management and employees must be continually aware and take responsibility for the security aspects of its business activities.
4. Prevention must be the first priority
5. Security measures and procedures must be submitted to regular inspections and verification by security specialists to maintain high levels of security standards.

In accomplishing the above we do the following:

1. Limit access to our Wi-Fi. Wi-Fi access is only given to employees and service personal directly involved with the implementation, monitoring, and inspection of our network.
2. Computer systems are backed up and information is stored off site with a third party vendor that uses the most current and up to date encryption methods. They are also HIPPA and SEC compliant.
3. Any information on computers located in our offices or mobile devises is also encrypted.
4. No remote access to office computers is given
5. None of the computers in the office are networked together.
6. Active anti-virus and malware
7. Regularly change passwords
8. Log password and virus activity
9. Do a penetration test annually to insure stability and security of our infrastructure form outside hacks.

As much as possible, security procedures and guidelines reflect the seamless integration of security and business activities.

Current as of May 2026