EVP SYSTEMS
ESTATE VALUATIONS & PRICING SYSTEMS

Information Security

The best defense is a really, really good defense

Any business that's unprepared for an on-line attack will eventually become the victim of an on-line attack. That's why **EVP Systems has extensive processes and policies** that protect all of our systems. A hardened data center, continuous intrusion detection, public notification of breaches—**that's how modern business is done.**

Industry Standard Best-Practices

EVP Systems uses financial industry best-practices for all its security: OS hardening, password complexity rules, mass-storage device limitations, restrictions on remote work, automatic software updates and nightly virus scans, off-site backups, and approved software lists.

Response and Notification Policy

No system is perfect, which is why EVP Systems has documented policies about how to respond if something goes wrong, and how we'll notify our clients if that ever happens. Because the only thing worse that getting hacked is not know about it.

No Weak Links

All EVP Systems employees go through criminal background checks and sign a non-disclosure agreement when they're hired. They receive annual training on information security, social engineering, and new threats. And, of course, only company business may be done on company machines or on the company networks.

Continuous Intrusion and Health Monitoring

Our data center has over two dozen test that run every five minutes, looking for trouble—external tests for connectivity problems, log tests for software and security issues, internal tests for CPU, RAM, and disk space concerns.