SECURITY BRIEF

The secure approach to safety & monitoring for VAs

Delegating admin work doesn't have to mean taking on extra risk. The real risk usually comes from messy access — shared credentials, files drifting into the wrong places, and accounts that aren't shut off cleanly.

SecureEVAs is built to keep VA work inside a controlled environment, with clear access and practical controls that reduce exposure by default.

Read on to learn more about how SecureEVAs keeps our clients — and their customers — safe.

SecureEVAs

Trained. Tested. Trusted.

Work stays inside a cloud-based PC

Executive Virtual Assistant work inside a secure, cloud-based PC (VM/VDI) using a program called Venn. That keeps agency work inside a controlled workspace — not on personal devices.

Access is tied to the individual

VAs use unique user logins, not shared credentials. Once a VA is onboarded, their credentials used to register and access Venn are created and provided by the client, based on the agency's requirements. Multi-factor authentication (MFA) is also required.

This makes access cleaner to manage and easier to remove when roles change.

Network security is built in

The Venn workplace includes a built-in VPN that runs automatically inside the workspace. VAs don't need to install separate VPN apps, and you don't have to rely on someone remembering to turn anything on. Network security is handled inside Venn.

Controls reduce accidental data movement

Most data exposure is casual: a quick copy/paste, a "temporary" download, a printed page, a session left open.

To reduce those risks, the workspace includes:

- copy/paste and clipboard restrictions
- upload restrictions
- printing restrictions
- session timeouts

Password tools are agency-approved and contained

SecureEVAs does not manage password storage inside Venn. Instead, the agency provides approved password management tools (such as RoboForm or 1Password), along with any required MFA.

Access and applications are configured to operate exclusively inside the Venn workspace, so credentials and password tools can't be accessed outside the secure environment.

Logging, monitoring, and escalation

Logging and monitoring are enabled within the workspace. SecureEVAs also has dedicated IT support and an escalation path with Venn IT, so issues can be investigated and addressed quickly.

Offboarding and deletion are managed

A VA's Venn workplace account is deactivated on the effective date of separation from the client or agency (role change or termination). Once the Compliance Officer deactivates the account, it is permanently deleted.

Security training is ongoing

Security training is conducted once per year and covers phishing awareness, cybersecurity best practices, password management, and security compliance.

SOC 2 Type 2 and HIPAA

SecureEVAs has earned both SOC 2 Type 2 and HIPAA certifications based on our rigorous approach to security and systematic, ongoing management of security and privacy risks.

We follow structured, control-based protocols required by these certifications. HIPAA-sensitive workflows are supported when PHI is involved, using controlled access and handling rules.

For more information on security and privacy standards and practices, please contact sales@secureevas.com

Or, book a consultation to learn more: secureevas.com/contact