Technology Updates and Assistance

Data security is concerned with securing sensitive data. Data security is primarily focused on preventing unauthorized access to data, via breaches or leaks, regardless of who the unauthorized party is. To achieve this, Pinnacle is using tools and technology such as firewalls, user authentication, network limitations, and internal security practices to deter such access.

Privacy, however, is concerned with ensuring that the sensitive data an organization processes, stores, or transmits is ingested compliantly and with consent from the owner of that sensitive data. This means informing individuals upfront of which types of data will be collected, for what purpose, and with whom it will be shared. So, privacy is less about protecting data from malicious threats than it is about using it responsibly, and in accordance with the wishes of customers and users, to prevent it from falling into the wrong hands.

Too often, the terms security and privacy are used interchangeably, but you can see that they are in fact different—although sometimes difficult to distinguish between. Whereas security controls can be met without also satisfying privacy considerations. In other words, privacy limits access, whereas security is the process or application for limiting that access. Put yet another way, security protects data, and privacy protects identity.

P.O. Box 33698
San Antonio, TX 78265

Pho: 866.344.4477
Fax: 210-344-2777

Client features of Dnet

A very important feature we offer at our Client Portal is electronic onboarding. If you are interested in electronic onboarding, you can email us IT@pinnaclepeo.com and provide your information. Our team will follow up with you and schedule a demo followed by providing the required documentation to get you started.

A good feature about electronic onboarding is you can onboard your new hires directly via Dnet portal without having to go through all the paperwork which is manual. The employee will finish the paperwork electronically via our client portal and submit it for review. You as an owner can review and approve the documents submitted. We can provide login access to existing employees as well, which makes it easier for you and the employees to look at their paycheck stubs and any other personal information.

Custom reports from Pinnacle

If you are looking for any custom reports for PPP Loan or anything in general, please contact your payroll coordinator with specific details you need on the report. We will usually provide you these reports within 48 hours, depending on the complexity of the report. We also provide a PEO relationship letter if needed for your lender. Pinnacle also has reports that can help you load your payroll costs into QuickBooks. These require some programming to customize them for your company.

New features our team is working on

Pinnacle IT Department is working on Benefits open enrollment via our Dnet Portal. This allows the employees to enroll to the benefits offered to them electronically. Employees can complete, review, and submit the enrollment forms electronically via our Dnet portal. Our Team is currently testing this feature and we are hoping to release this feature soon to our clients. We will keep you posted on our further development as time progresses.

Technology trends affecting our industry

Cyber-Security - how to prevent an infection

- **Never click on unsafe links:** Avoid clicking on links in spam messages or on unknown websites. If you click on malicious links, an automatic download could be started, which could lead to your computer being infected.
- **Avoid disclosing personal information:** If you receive a call, text message, or email from an untrusted source requesting personal information, do not reply. Cybercriminals who are planning a ransomware attack might try to collect personal information in advance,

which is then used to tailor phishing messages specifically to you. If in any doubt as to whether the message is legitimate, contact the sender directly.

- **Do not open suspicious email attachments:** Ransomware can also find its way to your device through email attachments. Avoid opening any dubious-looking attachments. To make sure the email is trustworthy, pay close attention to the sender and check that the address is correct. Never open attachments that prompt you to run macros to view them. If the attachment is infected, opening it will run a malicious macro that gives malware control of your computer.
- **Never use unknown USB sticks:** Never connect USB sticks or other storage media to your computer if you do not know where they came from. Cybercriminals may have infected the storage medium and placed it in a public place to entice somebody into using it.
- **Keep your programs and operating system up to date:** Regularly updating programs and operating systems helps to protect you from malware. When performing updates, make sure you benefit from the latest security patches. This makes it harder for cybercriminals to exploit vulnerabilities in your programs.
- **Use only known download sources:** To minimize the risk of downloading ransomware, never download software or media files from unknown sites. Rely on verified and trustworthy sites for downloads. Websites of this kind can be recognized by the trust seals. Make sure that the browser address bar of the page you are visiting uses "https" instead of "http". A shield or lock symbol in the address bar can also indicate that the page is secure. Also exercise caution when downloading anything to your mobile device. You can trust the Google Play Store or the Apple App Store, depending on your device.
- **Use VPN services on public Wi-Fi networks:** Conscientious use of public Wi-Fi networks is a sensible protective measure against ransomware. When using a public Wi-Fi network, your computer is more vulnerable to attacks. To stay protected, avoid using public Wi-Fi for sensitive transactions or use a secure VPN service.