Data Security Assurance

At BPAS, there is no greater imperative than keeping client data private, confidential, secure, and protected. All of our operational and data processing systems are in a secure environment that protects account information from being accessed by third parties or unauthorized users. We maintain and grant access to client information only in accordance with strict internal security standards, including user-based access and authentication controls by user. Client data is housed in secure applications, with safe delivery of data in both directions (never via email). We do not disclose personally identifiable information to parties outside of our affiliated companies, except as instructed by clients.

Safe

As a subsidiary of Community Bank System, Inc., BPAS is subject to audit and regulation by a diverse array of entities including the Federal Reserve, Texas Department of Banking, the Puerto Rico Commissioner of Financial Institutions, the Financial Industry Regulatory Authority (FINRA), the U.S. Department of Labor, the U.S. Internal Revenue Service, and the U.S. Securities and Exchange Commission.

BPAS maintains a robust SOC 1 audit report, with a SOC 2 underway.

We receive participant information only through a secure census portal, which limits access by requiring a Username and Password by authorized client representatives and BPAS employees. We accept changes to participant data only when submitted through our secure census system and information is not accepted or released through email. Data transactions are encrypted using industry standard encryption policies.

Secure

BPAS maintains a diverse security program that is constantly under review for our participant and client account portals. Access to an account requires a unique User ID and a strong Password.

At the initial login, we also require participants to enter a unique plan code. Our security protocols are multi-faceted, proprietary, and constantly evolving to deliver the most secure environment to clients.

Our websites also use Verisign certificates and SSL to protect data access and transmission. We perform regular risk analysis to manage, monitor, and identify any potential security breach.

In addition, our web environment is subject to multiple IT audits, which include infiltration testing, vulnerability assessment, employee testing and training, and ongoing awareness initiatives.

Monitored

We employ strict procedures within our call center where callers must be authenticated before any account information is discussed. All calls are recorded and archived, with ongoing training and QC review by our management team. We follow a variety of techniques, including red-flag rules, to ensure account security.

BPAS also requires that participant email communication containing any type of data or personal information be sent through our secure email system to a verified recipient.

Our parent company IT division manages all BPAS hardware, software, network, and telecommunication services to deliver a reliable, secure environment.

Users are segmented using Active Directory groups to prevent access to servers, software, or network drives that do not correspond to their job duties.

BPAS is vigilant about protecting the security of financial and personal information.

BPAS

Questions? Let's talk.

☎ 866.401.5272 | ✉ trustsales@bpas.com | bpas.com

SERVICES: Plan Administration & Recordkeeping | Actuarial & Pension | Collective Investment Trusts | Fund Administration
Fiduciary Services | Healthcare Consulting | IRA | VEBA | Consumer-Driven Health Plans

SUBSIDIARIES: BPAS Trust Company of Puerto Rico | Global Trust Company | Hand Benefits & Trust | NRS Trust Product Administration