BPAS Cybersecurity Best Practices

Guidance issued by the U.S. Department of Labor's Employee Benefits Security Administration (EBSA) includes 12 best practices for use by plan service providers responsible for the safekeeping of employee and participant data, and fiduciaries responsible for selecting plan service providers. **At BPAS, there is no greater priority than keeping our client data private, confidential, and secure while maintaining the integrity of systems, applications, and infrastructure.** Here's how we adhere to each of the 12 EBSA best practices.

EBSA Guideline	BPAS Best Practice
1 *Have a formal, well-documented cybersecurity program.*	Our cybersecurity program is a multi-pronged approach. It includes strict controls and procedures to reduce the threat of unauthorized access. The BPAS cybersecurity program consists of protective measures around network, physical, and information security. All of our operational and data processing systems are in a secure environment that protects account information from being accessed by third parties. We maintain and grant access to client information only in accordance with our internal security standards. We do not reveal specific information about our client accounts or other personally identifiable data to parties outside of our affiliated companies for their independent use. The BPAS security program is designed to protect customer information against any anticipated threats or hazards to the security or integrity of such information. It also manages the accountability of users with access to sensitive information, and protects against unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any client. We also adhere to the National Institute of Standards and Technology (NIST) regarding data in transit and data at rest. We use firewalls, anti-virus software, and security patches to protect the integrity of our operating system. Our website uses Verisign certificates and SSL to protect data access and transmission. Access to an account requires a user ID and password. All transactions are recorded, backed-up, and stored off-site. The BPAS external firewall uses an implicit deny policy to block inbound/outbound traffic on all unused ports, as well as any IP addresses and domains that are not necessary for operations. Security alerts are monitored closely by our IT staff; any applicable fixes are implemented. The rapidly changing nature of technology and critical nature of strategic core processing systems are vital to the success of our organization. BPAS, through our parent company, Community Financial Systems, Inc., has implemented a comprehensive Information Systems Security Policy to address all areas of information systems and technology. This policy includes computer systems and application security, physical security, operational security, network security, and procedural security. While protecting the security of retirement accounts is a top priority at BPAS, protecting participant accounts is a shared responsibility between participants, service providers, and employers. Our cybersecurity policy outlines steps participants should take to enhance chances of recovery if fraudulent activity or identity theft occurs within their account.
2 *Conduct prudent annual risk assessments.*	The Board of Directors, BPAS senior management, and each subsidiary are responsible for assessing and managing risks associated with their individual operations, regardless of whether the organization performs activities internally or through a third party. Audits and risk assessments occur throughout the year by internal staff as well as third parties. An annual IT/Cybersecurity risk assessment is completed using the FFIEC CAT and NIST Cybersecurity frameworks. Furthermore, all BPAS IT policies, as well as operational controls, are reviewed annually for compliance with best practices and current industry standards.

EBSA Guideline	BPAS Best Practice
❸ *Have a reliable annual third-party audit of security controls*	As a subsidiary of Community Financial System, Inc. (CFSI), BPAS is subject to audit and regulation by a diverse array of entities, including the Federal Reserve, Texas Department of Banking, 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 is also subject to a wide variety of audits and examinations, including: • Trust Related audits: Regulation 9 and compliance review, the annual Trust compliance audit, the Texas Department of Banking audit, and the Composite CIF audit. • Broker-Dealer audits: The FINRA audit and the Hand Securities, Inc. annual audit. • Financial/Operational Audits: Sarbanes-Oxley audit, Community Bank System, Inc. internal audit, the annual financial statement audit, the Hand Benefits & Trust Company audit, our annual SSAE 18/SOC audit, the Settling Bank audit by the OCC, and our extensive annual Information Technology audit conducted by Crowe, LLP. • Other Regulatory Compliance Requirements: The Gramm Leach Bliley Act, Patriot Act, Bank Secrecy Act, Anti Money Laundering Act, Pension Protection Act, and more. A large percentage of our time is spent ensuring compliance with laws and regulations that pertain to our business and the myriad audits to which we are subject. In addition to our annual SSAE 18 audit, which provides an extensive review of internal controls, procedures, and operations within BPAS, we retain Crowe, LLP to perform an annual Information Technology audit on our firm. This audit includes an extensive review of network security and penetration testing. It also reviews Network security for policies and procedures, access procedures, physical security, operations and recovery, MS Windows and active directories, anti-malware configurations, endpoint security, and network architecture. CBSI also completes an SOC2 report of the Pioneer data center in East Syracuse. While this is not the primary location of BPAS data, most security-related controls are at a parent-company level. Therefore, these reports are applicable regardless of where the data is housed. Future iterations of the report will expand the scope to include additional controls for both the Pioneer and BPAS data centers. Crowe, LLP performs penetration testing on internet-facing websites, web applications and services, as well as internal networks, systems, and services. This audit lasts approximately eight weeks each year, with a follow-up period to review findings before the report is finalized. BPAS implements changes and suggestions from this process throughout the year. In conducting this annual audit, Crowe, LLP scrutinizes our technology and operational procedures to confirm compliance with best practices. Therefore, rather than asking individual clients to each perform their own audit of IT policies and procedures at BPAS, we pay an independent, highly-qualified IT audit firm to conduct this audit on their behalf.
❹ *Clearly define and assign information security roles and responsibilities.*	Our Chief Information Security Officer, along with the rest of the Information Security and IT departments are responsible for managing and implementing our cybersecurity program. The teams use alerts from various threat intelligence sources to stay abreast of the latest risks to information security as it relates to BPAS systems. The Patch Management Procedure ensures that all critical system security-related patches are tested and applied as quickly as possible. A BPAS Computer Security Incident Response Team (CSIRT) performs, coordinates, and supports responses to security incidents. This team is comprised of members from management, legal, public relations, and information technology disciplines. Membership includes Information Security, IT Managers, BPAS Management, and others throughout the organization. All BPAS employees must submit any information relating to a suspected incident to their manager, who will then submit it to the IT Help Desk. We extensively test updated and new systems before being released to production. All systems are protected with anti-virus and additional endpoint protection software. Our Information Security and IT staffs monitor security alerts closely and immediately implement applicable fixes. If BPAS learns of potential unauthorized access or compromised information (including theft, employee carelessness or disclosure, social engineering, etc.), our IT/CSIRT will assess the nature and scope of the incident immediately and identify what customer information systems and types of customer information may have been compromised. Unauthorized access or compromised information may be identified through physical evidence, or through device, system, application, and databases logs. Incident Response would be triggered and the matter would be discussed with all applicable parties to determine appropriate next steps, including breach notification, if applicable.

EBSA Guideline	BPAS Best Practice
❺ *Have strong access control procedures.*	**Physical Security** Locations that process, maintain, and/or store customer information have information secured so only employees whose position necessitates may access it. All work areas maintain customer information as directed by Gramm-Leach-Bliley Act (GLBA), which ensures no customer information will be left accessible or visible to any persons not entitled to see such information. Access levels range from keyed entries, to fobbed access with video surveillance. All locations are secure to maximize the safety of our employees as well as protect our customer information. Keys, fobs, and access badges are distributed based on need; lists of key recipients are maintained at each location. **Network and Information Security** Firewalls, anti-virus software and security patches are all utilized to protect the integrity of our operating system. Our websites uses Verisign certificates and SSL to protect data access and transmission. Access to an account requires a User ID and Password. All transactions are recorded, backed-up, and stored off-site. The BPAS external firewall uses an implicit deny policy to block inbound/outbound traffic on all unused ports, as well as IP addresses and domains that are not necessary for operations. Security updates and alerts are monitored closely by our IT staff; applicable fixes are implemented. As noted above, our security program is designed to protect customer information against any anticipated threats or hazards to the security or integrity of such information. It also manages the accountability of users with access to sensitive information, and protects against unauthorized access to, or use of, information that could result in substantial harm or inconvenience to any customer.
❻ *Ensure assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.*	As previously noted, BPAS is subject to a wide variety of audits (no less frequently than annually) and examinations by a diverse array of entities. In addition to our annual SSAE-18 audit, we retain Crowe, LLP to perform an annual Information Technology audit on our firm. This audit includes an extensive review of network security and penetration testing. It reviews network security for policies and procedures, access procedures, physical security, operations and recovery, MS Windows and active directory, anti-malware configurations, endpoint security, and network architecture. Crowe, LLP also performs penetration testing on internet-facing websites, web applications and services, and internal networks, systems, and services. This Crowe, LLP audit lasts approximately eight weeks each year, with a follow-up period to review findings before the report is finalized. BPAS implements changes and suggestions from this process throughout the year.
❼ *Conduct periodic cybersecurity awareness training.*	All employees, contractors, and temporary workers with access to client data or client systems are required to participate in annual security awareness training. In addition, our Information Security team conducts internal phishing tests on all employees at least quarterly. A third party also completes a separate phishing test annually. Any employee that fails an internal phishing tests is required to complete additional training. We also distribute periodic awareness newsletters and email communications throughout the year on relevant topics regarding cybersecurity.
❽ *Implement and manage a secure system development life cycle (SDLC) program.*	Code development is limited to third parties that work with BPAS on custom applications. In those instances, we integrate them into our vendor management program, which includes an annual risk assessment along with due diligence documentation review. Where applicable, the third party SDLC is discussed along with verification that appropriate processes are in place to ensure secure code development.
❾ *Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.*	We maintain a Business Continuation Plan (BCP) and Disaster Recovery (DR) plan through a step-by-step process that each unit (or team) in our organization has completed, developed, and tested in the event of a disaster. We test these plans throughout the year. We also have the plans reviewed annually by all team managers. The plan and data backup is stored off-site. We also maintain a backup production system off-site. BCP testing requires all recovery teams to validate their recovery steps in the event of a disaster. These exercises are designed to improve the recovery plan by identifying gaps, documenting issues, identifying resolutions, and updating the BCP. Any revisions to the BCP are distributed and reviewed with executive management and recovery team managers. Our BCP/DR plans are tested both on a formal and informal basis, along with a regular semi-annual scheduled test.

BPAS Cybersecurity Best Practices

EBSA Guideline	BPAS Best Practice
10 *Encrypt sensitive data, stored and in transit.*	As previously noted, BPAS adheres to the National Institute of Standards and Technology (NIST) regarding encrypting sensitive data in transit, as well as data at rest. We employ firewalls, anti-virus software, and security patches to protect the integrity of our operating system.
11 *Implement strong technical controls in accordance with best security practices.*	At BPAS, all of our operational and data processing systems are in a secure environment that protects account information from access 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. Client data is housed in secure applications, with safe delivery of data in both directions. We do not disclose personally identifiable information to parties outside of our affiliated companies, except as instructed by clients.
12 *Appropriately respond to any past cybersecurity incidents.*	BPAS defends against anticipated threats with frequent patching to all systems, an Intrusion Protection system, a gateway firewall with anti-virus protection, a client anti-virus solution on all systems, user authorization governed by the principal of least privilege, a DMZ network for externally facing web servers, and mechanisms on the local network to stop unauthorized devices from connecting to the corporate local network. If BPAS learns of unauthorized access or compromised information (including theft, employee carelessness or disclosure, social engineering, etc.), our IT/CSIRT will assess the nature and scope of the incident immediately and identify what customer information systems and types of customer information may have been compromised. We would then discuss the matter with all applicable parties to take corrective measures. Furthermore, in the unlikely event that a cyber-intrusion or other unauthorized access were to occur, multiple options are available that would adequately cover costs if BPAS is found to be at fault.

At BPAS, information security is paramount. We adhere to strict internal policies, procedures, and controls to ensure information entrusted to our company remains protected. **It's more than a commitment, it's a promise.**

Contact your BPAS representative for more information about BPAS information security practices, operational controls, or audit-related items.

Questions? Let's Talk.

BPAS

☎ 866.401.5272 | ✉ TrustSales@bpas.com | bpas.com | u.bpas.com