Cybersecurity?
NBS® has it locked down

Long before the U.S. Department of Labor (DOL) issued guidance for plan sponsors, fiduciaries, participants, and record keepers on the best practices for maintaining plan cybersecurity, NBS was implementing industry-leading cybersecurity practices to safeguard our clients' data.

NBS has spent decades investing in technologies and enhancing our systems to keep our clients' plans safe and secure. NBS was one of the first third-party administrators in the country to implement a Service Organization Control (SOC) 2 Type II examination. We have received SOC 2 Type II Certification since 2018. We endeavor to ensure your peace of mind when it comes to cybersecurity risks.

The DOL cybersecurity best practices encourage service providers to provide the same data protections that NBS has been offering to our clients for several years. In addition to managing plan compliance and operations with exceptional service, you can rest easy knowing that NBS is also ensuring that your plan's data is safe and secure.

NBS continues to look for ways to improve our services, and we are excited to see that the DOL cybersecurity guidance directly aligns with our current processes and external audits. As illustrated below, you can see how NBS satisfies all of the best practice areas emphasized by the DOL cybersecurity guidance. This puts NBS in a great place to maintain your plan's compliance, enhance your service, and ensure your data security into the future. Please contact your NBS representative to learn more about how we safeguard retirement plan data like no one else.

DATA ENCRYPTION AND SECURITY

- Implement and manage a secure system development life cycle (SDLC) program
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response
- Encrypt sensitive data, stored and in transit
- Implement strong technical controls in accordance with best security practices

SECURITY EVALUATIONS

- Have a formal, well documented cybersecurity program
- Conduct prudent annual risk assessments
- Have a reliable annual third-party audit of security controls
- Appropriately respond to any cybersecurity incidents

TRAINING AND BEST PRACTICES

- Clearly define and assign information security roles and responsibilities
- Have strong access control procedures
- Ensure that any 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
- Conduct periodic cybersecurity awareness training

Salt Lake City, UT | Dallas, TX | San Diego, CA | Honolulu, HI | (800) 274-0503 | www.nbsbenefits.com | service@nbsbenefits.com