Innovative
INVESTMENT FIDUCIARIES

Cyber Security *Due Diligence Assessment* for Plan Service Providers

Cyber Security *Due Diligence Assessment* for Plan Service Providers

As a plan fiduciary, you need to establish a prudent process to understand the cyber security standards and practices of your service providers. The below questionnaire will help you fulfill your due diligence requirements to document such practices.

Send each of your service providers the below questions and retain for your records. It is recommended to complete this on an annual basis.

Note: As Plan fiduciaries, you should review the completed information and compare to other service providers.

1. Describe your information security standards. Please include a copy of your practices and policies and any audit results (SOC 1, SOC 2 etc.)
2. If you are unwilling to share audit results, please summarize the findings and explain the steps taken to address the findings in the audit report, if any.
3. How do you validate your cybersecurity practices?
4. What levels of security standards are in place?
5. Describe any (i) past information security incidents or data breaches, and (ii) litigation or legal issues related to your services. What was your response?
6. Do you maintain insurance policies that extend coverage to customers that would cover losses caused by identity theft or cybersecurity breaches (including breaches caused by internal threats, such as conduct by an employee or contractor)? If so, describe the policy, coverage, and any limitations.
7. If you do not have insurance coverage that address 7 and 8 above, will your company indemnify our company for any expenses or losses related to identity theft or cybersecurity breach?
8. Will you agree to keep any and all of our information private and take commercially reasonable steps to prevent its use or disclosure without our written permission?
9. Will you agree to notify us immediately in the event of a cybersecurity incident or data breach?