Cybersecurity best practices checklist

Use this checklist to review and strengthen your plan's cybersecurity.

Familiarize yourself with legal issues.

- Learn state law requirements that apply to your plan (there isn't a comprehensive federal cybersecurity law). Most states require "reasonable security procedures" that are "appropriate to the nature of the information."
- Follow the laws of every state in which your organization operates. State requirements may vary significantly.

Be aware of ERISA requirements.

- Although ERISA doesn't explicitly address cybersecurity issues, fiduciaries have a duty to act prudently and in the best interest of participants in maintaining online security. Defining and implementing a comprehensive cybersecurity plan may help you defend against a fiduciary claim based on a cybersecurity breach.
- Stay tuned for upcoming official guidance from the Department of Labor on additional cybersecurity best practice.

Know your cybersecurity risk profile

In developing a risk management strategy:

- Understand the types of data associated with the plan.
- Determine how information is accessed, stored, shared, controlled, transmitted, and secured (for example, by using encryption).
- Consider the plan's size, complexity, and overall risk exposure to effectively coordinate the plan's cybersecurity with your broader cybersecurity efforts.
- Know what controls you have in place to mitigate risks and consider testing and benchmarking those controls.
- Understand how any third party providers interact with your data.
- Engage experts to help, if needed.

Manage your third parties

- Ensure a security assessment process is in place to evaluate all third party service providers who have access to plan data.
- Have a written policy detailing security requirements for third parties.
- Include appropriate security requirements in your contracts.
- Determine whether the third party provider has cybersecurity insurance.
- Periodically review existing relationships.
- Confirm that your service providers have a track record of responsiveness to cybersecurity issues.
- Confirm that your providers have strong access controls such as multifactor authentication.

Build and evolve your program

- Assign responsibility for design and implementation of the plan's cybersecurity program to a single individual to maximize oversight.
- Conduct a risk assessment on a periodic basis to inform your program design.

Maintain adequate insurance

- Review your existing insurance policies for cybersecurity coverage.
- Investigate special cybersecurity coverage if your current insurance isn't adequate.
- Closely review the terms of your cybersecurity coverage.

Please note: Be sure to consider first party coverage, which would respond in the event of business interruption due to a cybersecurity event, and could cover items such as damage to digital assets, extra expenses incurred to keep your business operational, lost revenue, and cyber extortion. In addition, consider adding coverage for cybersecurity breaches occurring at third party vendors, for which you may be the party expected to respond.

Educate employees

- Provide your employees ongoing cybersecurity training.
- Teach employees how to report incidents.
- Help employees identify red flags and reduce their risks of falling victim.

Visit LincolnFinancial.com/CyberSecurityStrategy to learn more.

Not a deposit
Not FDIC-insured
Not insured by any federal government agency
Not guaranteed by any bank or savings association
May go down in value

LincolnFinancial.com

Lincoln Financial Group is the marketing name for Lincoln National Corporation and its affiliates.

Affiliates are separately responsible for their own financial and contractual obligations.

LCN-3394515-010721
PDF 3/21 **Z01**
Order code: DC-CKLST-FLI001

Lincoln Financial Group

For plan sponsor and financial professional use only. Not for use with the general public.