



Cybersecurity: Protect your Institution

The following provides information and actions that can be used to protect your institution from cyber criminals.

The cyber threat landscape is continuously evolving with new threat actors (cyber criminals), attack vectors (method or pathway used to access systems), and vulnerable devices.

In 2021, the Department of Labor (DOL) published **three brief cybersecurity guideline documents** that provide cybersecurity guidelines for retirement plan sponsors, participants, and service providers:

These tips align with the Department of Labor guidelines to help protect your institution:

- 1 Have a formal, well-documented cybersecurity program with clearly defined and assigned security roles and responsibilities.
- 2 Conduct careful annual risk assessments and have a reliable, independent, and unbiased auditor assess your organization's security controls.
- 3 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. Encrypt sensitive data, stored and in transit.
- 4 Implement strong technical controls in accordance with best security practices. Have strong access control procedures.
- 5 Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response. Appropriately respond to any past cybersecurity incidents.
- 6 Implement and manage a secure system development life cycle (SDLC) program.
- 7 Conduct periodic cybersecurity awareness training.

For more information about the Department of Labor guidelines documents, see list below:

- **Tips for hiring a service provider with strong cybersecurity practices** (this document is for plan sponsors).
- **Cybersecurity program best practices** (this document is for service providers such as TIAA).
- **Online security tips** (this document is for participants).

TIAA applauds the Department of Labor for thoroughly addressing a topic of such great importance. At TIAA, we operate a robust cybersecurity program and have long-standing practices that support the Department of Labor's guidance.

To review TIAA's alignment, take a look at these overview flyers:

- **An overview of our alignment to the DOL's Cybersecurity Best Practices**
- **TIAA's long-standing practices support DOL's new guidance flyer**

At TIAA, customer data security is a top priority and we combine technology, people and processes to protect our customers and their personal information. We comply with both state and federal regulations and industry guidelines. For more information, please visit the **Security Center**. If you are a plan sponsor, please visit the **Plan Sponsor Cybersecurity Page**.