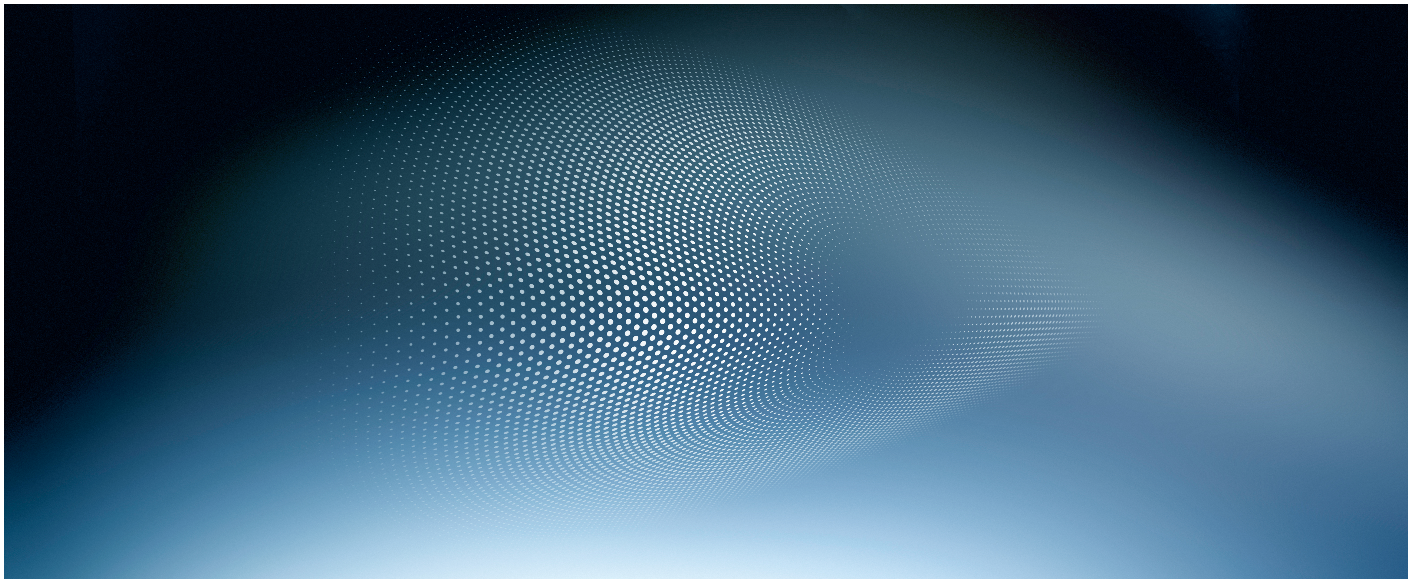
Morgan Stanley



Cybersecurity Guidance for Plan Sponsors

Financial companies accounted for 23% of total cyber breach incidents across all business sectors in 2024 and retirement plans have emerged as prime targets because of their access to significant personal and financial data.[1] That's why Morgan Stanley's highest priority is to protect your retirement plan assets and employee personal information.

To keep company and employee data safe, the Department of Labor (DOL) publicized guidance around qualified retirement plan cybersecurity practices for plan sponsors, fiduciaries, service providers, and participants. In this guide, Morgan Stanley has summarized this information to help you stay compliant with the impending changes.

Adapting to the Evolving Cybersecurity Landscape

When it comes to providing a retirement plan for your employees, remaining compliant with the DOL is one of your most important responsibilities as a plan sponsor. Over the past couple of years, the DOL has commenced an audit initiative focusing on retirement plan cybersecurity practices, asking plan sponsors and plan fiduciaries to share all cybersecurity program policies, procedures, and guidelines that relate to the plan, whether applied by the plan sponsor or by a service provider. The DOL has also requested detailed documentation of actions taken by the plan's fiduciaries and service providers regarding their cybersecurity practices.

As cybercrime continues to evolve and increase, with an estimated cost of $23.84 trillion globally by 2027, or 35% increase since 2022, the DOL will likely continue its effort to evaluate these practices and offer further guidance and regulations.[2]

Best Practices

Morgan Stanley can help you take action to protect your company and the personal data of your employees from cyberattacks.

Morgan Stanley discovered that

nearly half

of companies in 2025 were focusing their attention to technology investments and meeting regulatory requirements.[3]

Tips for Plan Sponsors

Under the Employee Retirement Income Security Act (ERISA), plan sponsors have a fiduciary duty to prudently select and monitor a plan's service providers. The DOL's guidance addresses how plan sponsors can evaluate a service provider's cybersecurity practices to effectively satisfy these obligations with the following recommendations:

- Carefully review and compare service providers' security standards to recognized industry standards and whether they have cybersecurity or identify theft insurance.
- Incorporate cybersecurity-related provisions in agreements with service providers, including terms that require ongoing compliance with applicable cybersecurity and information security standards that do not limit a service provider's responsibility for security breaches.
- Consult with legal advisors.

Tips for Service Providers

The DOL guidance provides best practices for service providers to promote a strong cybersecurity infrastructure including:

- Implement a formal, well-documented cybersecurity program that outlines safeguards for IT infrastructure and retirement data from internal and external threats.
- Institute formal and effective policies and procedures requiring annual risk assessments and review by a third-party auditor.
- Manage cybersecurity programs at the senior executive level.
- Service provider users/employees should be subject to strong access control procedures.
- Conduct annual cyber awareness training for employees.
- Establish a secure system development lifecycle program, a business resilience program, encryption of sensitive data while stored and in transit and technical controls (i.e., in hardware, software, or firmware).

Tips for Participants

We all know not to give out personal or account information to unsolicited contacts, to be careful on public Wi-Fi networks and to verify the email sender's address before clicking links, but additional security tips include:

- Set up online financial accounts with unique passwords to make it harder for thieves to set up an account on your behalf.
- Use strong passwords with longer unique characters that have a mixture of upper- and lower-case letters, numbers, and symbols.
- Keep personal contact information updated to make sure companies can alert you to any suspicious activity.
- Monitor financial accounts and credit reports regularly to peruse for suspicious activity.
- Be careful of the information you reveal on social media like your pet's name and birthday, which can provide clues for hackers on "forgot password" options.
- Consider reducing the number of financial accounts for fewer opportunities of cyber attacks.
- Sign up for multi-factor authentication.

The Morgan Stanley Approach

Morgan Stanley is committed to helping companies and employees wherever they are on their journey of wealth creation. Helping you navigate today's financial services landscape and legislative changes is an important part of this promise. With an end-to-end approach to workplace financial solutions, we pride ourselves on offering a unique combination of thoughtful education, insightful advice, and leading technology.

Contact your Financial Advisor today to learn more about Morgan Stanley's cybersecurity infrastructure and how we can help keep your sensitive data safe.

[1] Industrial Cyber, "US Homeland Security Committee Warns of Rising Cyber Threats, as Federal Shutdown and Lapsed Law Hamper Defenses", November 2025.
[2] Sentinel One, "Key Cyber Security Statistics for 2025", July 2025.
[3] Morgan Stanley, "2025 State of the Workplace Study". December 2025.

When Morgan Stanley Smith Barney LLC, its affiliates and Morgan Stanley Financial Advisors and Private Wealth Advisors (collectively, "Morgan Stanley") provide "investment advice" regarding a retirement or welfare benefit plan account, an individual retirement account or a Coverdell education savings account ("Retirement Account"), Morgan Stanley is a "fiduciary" as those terms are defined under the Employee Retirement Income Security Act of 1974, as amended ("ERISA"), and/or the Internal Revenue Code of 1986 (the "Code"), as applicable. When Morgan Stanley provides investment education, takes orders on an unsolicited basis or otherwise does not provide "investment advice", Morgan Stanley will not be considered a "fiduciary" under ERISA and/or the Code. For more information regarding Morgan Stanley's role with respect to a Retirement Account, please visit www.morganstanley.com/disclosures/dol. Tax laws are complex and subject to change. Morgan Stanley does not provide tax or legal advice. Individuals are encouraged to consult their tax and legal advisors (a) before establishing a Retirement Account, and (b) regarding any potential tax, ERISA and related consequences of any investments or other transactions made with respect to a Retirement Account.