ADP's cybersecurity program helps keep your business safe

Always Designing for People®

Your security **means everything to us**

AT ADP, SECURITY IS INGRAINED IN OUR SOLUTIONS —THAT'S WHY COMPANIES OF ALL SIZES HAVE BEEN COUNTING ON US SINCE 1949.

We deliver advanced services and technology for data security, privacy, fraud, and crisis management — all so you can stay focused on your business. ADP's security program continues to stay at the forefront of the industry. So, when the Department of Labor (DOL) recently issued its cybersecurity guidance for plan sponsors, fiduciaries, recordkeepers and participants, we were ready. Because we've been protecting client and employee data since the beginning.

Below are the tips and best practices released by the DOL and ADP's response to them.

Have a formal, well documented cybersecurity program

Rest assured, ADP has developed and documented formal information policies that set out ADP's approach to managing information security. Our information security measures and practices are designed to be consistent with the ISO 9001:2015 and ISO/IEC 27001:2013 information security standards. Our goal is to help ensure that the security program effectively and efficiently operates to protect all the information entrusted to us by our clients and their employees.

Conduct prudent annual risk assessments

ADP policy requires our management to promptly take appropriate actions and commit sufficient resources to reduce unacceptable loss exposures to acceptable levels. To meet this objective ADP created an operational risk management framework and has deployed supporting procedures and tools across the enterprise.

Have a reliable annual third-party audit of security controls

Risk assessments of third parties who require access to ADP and/or client information are periodically performed and ADP employs a process to internally perform compliance reviews on a periodic basis. Additionally, ADP performs a SOC1 Type II Audit on a periodic basis and in the case of certain services offered by ADP, there would also be SOC 2 Type II Executive Reports.

Clearly define and assign information security roles and responsibilities

The Global Security Organization (GSO) consists of cross-divisional security teams leveraging a multi-disciplinary approach to compliance with cyber and information security standards, operational risk management, client security management, workforce protection and business resilience. Roles and responsibilities have been formally defined for all members of the GSO and it is charged with the design, implementation and oversight of our information security program based on corporate policies.

Have strong access control procedures

ADP's Access Control Policy is part of the larger Global Security Organization Policy. Policies are published in the ADP intranet and are accessible to all employees and contractors from within the ADP network. ADP reviews its information security policies at least annually or whenever there are major changes impacting the functioning of ADP's information systems.

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

ADP SmartCloud was built with the security and privacy of our clients' data in mind. The configuration of the SmartCloud environment allows for the management of cloud vendors and services to be consistent globally with ADP information security policies and operations standards. This includes the requirement that new cloud service providers undergo a robust due diligence approval process that includes a detailed security review, in-depth security testing and static analysis.

The Vendor Assurance assessment workflow is managed through our Corporate GRC tool. Corporate Procurement Department performs a thorough analysis of vendor's financial, operational, compliance, and reputational risks, while the Global Security Organization reviews in detail the Data Security and Privacy posture of the vendor when applicable.

Conduct periodic cybersecurity awareness training

At ADP, our Security Training and Awareness Program is a continuous, dynamic and robust initiative that is designed to develop and maintain a security-focused culture, empower our associates and contingent workers to make responsible, secure decisions and to protect our most valuable assets. We employ a variety of tools, techniques and programs to embed security into our associates' and contingent workers' day-to-day professional and personal lives. All employees are required to complete information security training as part of their onboarding plan and are subsequently required to take and successfully complete an annual, interactive security training program that includes an overview of key security topics, policies and responsibilities. All contingent workers are required to complete this same training within one week of the start of their contract.

Implement and manage a secure system development life cycle (SDLC) program

ADP employs a well-defined change management process. All application and system changes must proceed through many testing stages in our development and quality assurance areas before they are promoted to a staging area in our web hosting centers. The staging area is used to assess the viability of applications in a secure environment while facing the Internet prior to promotion to the production areas. This type of change control management supports the concept of "separation of duties" as application and system changes are migrated from and to the various environments by different individuals and groups. Furthermore, individuals involved in this change management process are only provisioned rights to the resources they need in order to perform their specific duties.

Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response

ADP is committed to keeping our services and operations running smoothly, so that we can provide our clients with the best service possible. It's our priority to identify — and mitigate — the technology, environmental, process, and health risks that may get in the way of providing our business services. A Global Business Resiliency Policy and Program have been developed, in compliance with applicable regulations and guidelines, to establish a single, global framework that addresses how ADP manages and controls identified risks resulting from disasters and other significant business-disruptive events. We require that our business resiliency plans be reviewed, revised and tested at least annually.

Disaster Recovery and Business Continuity planning

Detailed disaster recovery plans have been developed to address a disaster impacting the data centers and to provide immediate response and subsequent recovery from any unplanned service interruption. Business continuity plans have been developed to maintain or restore business operations following interruption to, or failure of, critical business processes or systems. They are designed to provide prompt response to and recovery from interruptions such as critical service loss, loss of access to a building or facility catastrophe.

Encrypt sensitive data, stored and in transit

ADP has an internal Encryption Security Standard that includes well-defined key management and key escrow procedures, including both symmetric and asymmetric keys management. Encryption keys used for ADP information are always classified as confidential information. Access to such keys is strictly limited to those who have a need to know and if an exception approval is provided. Encryption keys and key lifecycle management followed industry-standard practices.

ADP requires that all confidential information in transit over a public network (which includes all ADP client information) must be encrypted using industry-accepted encryption techniques and strengths. ADP uses industry-accepted cryptographic methods when encrypting client information through well-known transmission protocols.

Implement strong technical controls in accordance with best security practices

ADP ensures compliance with security policies and standards. All ADP managed systems must comply with the installation of a specialized security-hardened operating system (or secure build process). Systems Administrators deploy a hardened, approved, and standardized build for every type of system used within our infrastructure. Out-of-the-box installation of operating systems is prohibited since these installations may create vulnerabilities, such as generic system account passwords, that would introduce an infrastructure risk. These configurations reduce the exposure of hosted computers running unnecessary services that can lead to vulnerabilities.

Appropriately respond to any past cybersecurity incidents

ADP has a documented methodology for responding to security incidents timely, consistently, and effectively. Should an incident occur, a predefined team of ADP employees activates a formal incident response plan. ADP policies define a security incident, incident management, and all employees' responsibilities regarding the reporting of security incidents. ADP also conducts regular training for ADP employees and contractors to help ensure awareness of reporting requirements. Training is tracked to ensure completion.

We deliver advanced services for **data security, privacy, fraud protection, and crisis management.**

Our commitment to you and your employees

Security is integral to our products, business processes, and our infrastructure. Our clients trust us to help them more effectively manage, deploy, compensate, and serve the human resource needs of their employees, while also handling and protecting their most sensitive data. Staying ahead of the curve is how we drive value for our clients.

We conduct our business with the highest level of integrity and we stand behind our expertise and advanced security intelligence platform. That's our commitment to you and your employees — and we honor our commitments. Every time.

ADP works hard to **keep your data safe.**

For more information on ADP retirement plan solutions and how we protect your business, please contact your licensed ADP Retirement Services District Manager or visit us at www.adp.com/401k.

Always Designing for People®