



# Protecting your plan

## Important information regarding the U.S. Department of Labor's cybersecurity guidelines

In the interest of protecting the retirement benefits of American workers, the U.S. Department of Labor (DOL) and the Employee Benefits Security Administration (EBSA) announced cybersecurity guidelines for retirement plan providers, plan sponsors, plan fiduciaries, and plan participants. At Empower, protecting our clients from cybersecurity threats — including theft, fraud, and other risks — is among our highest priorities, and we fully support the DOL's guidance. In the following pages, we provide important information on how Empower aligns with — and exceeds — the DOL guidelines, while being an industry leader in developing and implementing critical cybersecurity protocols.



## BEST PRACTICES AT-A-GLANCE

DOL cybersecurity best practices	Empower protocols
✓ 1. A formal, well-documented cybersecurity program	Empower's information security policies are aligned and documented to NIST 800-53, U.S. government standard for cyber defense and information security policies.
✓ 2. Prudent annual risk assessments	Empower exceeds the DOL's guidance for annual risk assessments. Since 2012, Empower has hired Verizon to conduct risk assessments every quarter. We've earned the distinction of being a Verizon Cyber Risk Program Certified Enterprise for 12 years.
✓ 3. A reliable annual third-party audit of security controls	Empower's external third-party auditor performs annual attestations of adherence to our security controls to produce SOC 2 type 2 annual reports, the industry standard for proof of compliance and security program thoroughness.
✓ 4. Clearly defined and assigned information security roles and responsibilities	Empower has clearly defined and assigned roles and responsibilities, including strategy and operational management from our CISO and oversight from our Information Security Board (ISB) and board of directors.
✓ 5. Strong access control procedures	At Empower, access to information is provisioned on the principle of least privilege (PoLP) and employs strong data access controls.
✓ 6. 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	We conduct third-party vendor risk assessments prior to contracting with critical suppliers, which includes reviews of financial, technical, and operational controls.
✓ 7. Cybersecurity awareness training conducted at least annually for all personnel and updated to reflect risks identified by the most recent risk assessment	Empower associates are systematically assigned mandatory security awareness, privacy, and fraud awareness training throughout the year.
✓ 8. Secure system development life cycle (SDLC) program	Empower has implemented a systems development life cycle (SDLC) methodology, which covers analysis, design, build-and-test, quality assurance, and installation, and governs the development, implementation, and maintenance of application systems.
✓ 9. A business resiliency program that effectively addresses business continuity, disaster recovery, and incident response	Empower has an established, mature Computer Security Incident Response Team (CSIRT), documented business continuity/disaster recovery plan (BC/DR), and Incident Response Plan (IRP) to help ensure that business products and services remain available in the unlikely event of a major business interruption. The BC/DR plan incorporates business impact analyses and contingency planning at multiple levels, incident management guidelines, emergency notification, clearly defined roles, responsibilities and authority levels, and disaster declaration processes.
✓ 10. Encryption of sensitive data stored and in transit	Empower encrypts all sensitive data at rest (stored) and in transit.
✓ 11. Strong technical controls implementing best security practices	We employ industry-leading technology and security measures designed to defend against cybersecurity threats and safeguard client-sensitive information.
✓ 12. Responsiveness to cybersecurity incidents or breaches	Empower's incident Response Plan is designed to ensure a rapid and comprehensive response should a cybersecurity incident or breach ever occur.
✓ Empower aligns with DOL guidelines	

## Cybersecurity best practices

The following guidance from the DOL, [Cybersecurity Program Best Practices](#) ►, is intended to help plan sponsors ensure their retirement plan provider has sufficient cybersecurity programs, IT systems, and plan data protocols to mitigate cybersecurity risks. Each item from the DOL document is accompanied by a response detailing Empower's protocols.

### 1. A formal, well-documented cybersecurity program

Empower's Information Security Policies include high-level program management requirements for planning and communication regarding information security, both internally and externally. Empower's information security policies are aligned and documented with NIST 800-53, which is a gold standard framework and a U.S. cyber defense standard. NIST 800-53 is composed of over 1,000 controls with 18 control families, and is considered to have one of the most robust coverage over other standards. Our information security policies (ISPs) are reviewed annually by a committee representing various lines of business and systems areas and are reviewed and accepted by the Information Security Board. Our ISPs provide administrative, physical, and technical safeguards to limit access to protected information, establish proper handling practices, and secure the facilities and systems where the information is stored.



## 2. Prudent annual risk assessments

Empower exceeds the DOL's guidance for annual risk assessments. Since 2012, Empower has been hiring Verizon (the same company that creates the annual authoritative Data Breach Investigations Report (DBIR)) to perform comprehensive risk assessments on a quarterly basis. In recognition of our industry-leading, comprehensive information security program, we've earned the distinction of being a Verizon Cyber Risk Program Certified Enterprise for 12 years.

By exceeding the Verizon Cyber Risk Programs Certification requirements, Empower has achieved an assessor's letter of certification, an independent third-party enterprise cybersecurity certification issued by Verizon. Achieving certification confirms an organization's strong defenses and demonstrates an organization's commitment to security of its IT assets, reputation, and sensitive information. This achievement demonstrates that we employ proven security processes and technologies to maintain a proactive and comprehensive information security program. Proof of certification can be provided by contacting the Empower Sales or Relationship Management teams.

Annual penetration tests of our network and externally facing web applications are performed by rotating vendors, who are payment card Industry qualified security assessors (PCI QSAs). While Empower is not subject to PCI compliance, and it's not essential to have a QSA perform our penetration tests, Empower respects the in-depth annual certification program of the PCI council for QSAs, who offer compliance standards and top industry guidance on testing threats and fighting data compromise.



### VERIZON CYBER RISK PROGRAM

A cybersecurity risk reduction, and certification program that addresses all aspects of proactive cybersecurity measures and controls, from network and system analysis to physical security, including enterprise policy inspections — evaluating the effectiveness of our organization's administrative, technical, physical, and environmental control implementation via an evidence-based risk management program. The program includes an independent professional review of our network and security controls and is measured against 31 policy categories that affect all critical control groups across an organization (policy, human, physical, device, and network).

### 3. A reliable annual third-party audit of security controls

Empower maintains annual third-party audits of our security controls including SOC 1 type 2 and SOC 2 type 2 audit reports.

Empower's external third-party auditors perform annual attestations of adherence to our security controls, to produce SOC 2 type 2 annual reports, the industry's frequently requested proof of compliance and security program thoroughness by prospective and existing clients.

Our annual SOC 2 type 2 reports are specific to IT and security controls of our recordkeeping system that include a wide spectrum of information security and business resiliency. The annual audit provides assurance that Empower's service commitments and system requirements are achieved based on the trust services criteria relevant to set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing, Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Since each organization can define what is in scope for their controls, it is important to verify that the SOC 2 report specifically includes the recordkeeping system in scope, as Empower has done with our SOC 2 type 2 report.

Unlike a one-page, point-in-time ISO 27001 certification, 100+ page in-depth SOC 2 type 2 reports test and transparently convey both the design effectiveness and the operating effectiveness of our security and regulatory compliance control objectives. For ease of comparison across providers, ask for an SOC 2 type 2 report that is mapped to the SPARK Institute's 16 control objectives.

The SPARK Institute is a member-driven, non-profit organization and leading voice in Washington, D.C., for the retirement plan industry. SPARK helps shape national retirement policy by developing and advancing positions on critical issues that affect plan sponsors, participants, service providers, and investment providers. SPARK's 16 control objectives were derived from a list of over 1,300 questions submitted to member firms and then organized into overall control topics that align closely with these DOL best practices.



#### **SOC 2 TYPE 2 REPORTS PROVIDE:**

- Evidence of adherence to security controls.
- Transparency of the scope of testing.
- Auditor testing conclusions with quantities and details of issues noted.
- Management remediation plans if issues are noted.
- A modern U.S. standard.

We also contract with independent security firms to perform annual penetration tests and assessments of our key applications, plus an external network-layer assessment of our entire internet-facing infrastructure. These assessments and penetration tests seek vulnerabilities that a cybercriminal would try to use to breach our security controls, such as SQL injection, cross-site scripting, and other common attacks. Yearly results of these evaluations have been excellent, and relevant findings are remediated immediately.



#### 4. Clearly defined and assigned information security roles and responsibilities

Empower has clearly defined and assigned roles and responsibilities, including oversight from our Information Security Board (ISB). Empower’s Chief Information Security Officer (CISO) establishes and maintains the vision, strategy, and operation of the cybersecurity program. Our CISO leads teams that manage corporate information security policies, security awareness and training, numerous forms of risk assessments, threat and vulnerability assessments, security architecture, security incident management, and enterprise resiliency. Our CISO reports to our Chief Information Officer (CIO), and these positions have membership within the ISB.

*“Empower’s quality cybersecurity program is executive driven and board supported to ensure cohesive and global oversight to govern cyber risks effectively.”*

— **Doug Peterson**  
Chief Information Security Officer

Criteria responses	DOL cybersecurity best practices	Empower protocols
✓	Sufficient experience and necessary certifications	A combination of relevant work experience, training, and/or professional certifications is required for all Empower information security positions.
✓	Initial and periodic background checks	Empower performs background checks on all candidates prior to employment in accordance with applicable laws.
✓	Regular updates and training to address current cybersecurity risks	Empower associates are systematically assigned mandatory security awareness training annually and made aware of current security events and vulnerabilities through periodic management communications. Training is assessed through a grading system to achieve certification, and sessions are tracked to completion.  In addition, unannounced email phishing campaigns are performed throughout the year. Follow-up training is leveraged to ensure our associates have the knowledge to properly identify incoming threats to our environment.
✓	Current knowledge of changing cybersecurity threats and countermeasures	Empower is also a Premier member of FS-ISAC, which provides early notification of security threats and attacks; anonymous information sharing across the financial services industry; and regularly scheduled member meetings, including biweekly conference calls. We receive alerts and notifications from US-CERT and have memberships with Threat Alert services. Select security personnel are members of the FBI InfraGard, a partnership between the FBI and the private sector dedicated to sharing information and security intelligence to prevent hostile acts against the United States.



## 5. Strong access control procedures

At Empower, access to information is provisioned on the principle of least privilege (PoLP). PoLP is an information security concept in which a user is given the minimum levels of access — or permissions — needed to perform their job functions. These access controls are widely considered to be a cybersecurity best practice, and they provide a fundamental step in protecting privileged access to high-value data and assets. The principle of least privilege extends beyond human access.

Criteria responses	DOL cybersecurity best practices	Empower protocols
✓	Access to systems, assets, and associated facilities is limited to authorized users, processes, devices, activities, and transactions.	The principle of least privilege is strictly enforced based on business need and management approvals for access to all Empower informational assets and resources.  Unique user IDs are issued and forced password complexity rules are enabled that include, but are not limited to, minimum length, invalid attempts, password history, and a mixture of characters and numbers.
✓	Multi-factor authentication is used wherever possible, especially to access the internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control methodology.	Forced multi-factor authentication (MFA) measures are used to access Empower’s Virtual Private Network (VPN), and our VPN is always on.
✓	Policies, procedures, and controls are implemented to monitor the activity of authorized users and detect unauthorized access, use of, or tampering with nonpublic information.	Empower uses user and entity behavior analytics (UEBA) technology to analyze typical and atypical activity of humans and machines within our network and detect unauthorized access and use of our data.
✓	Confirm the identity of the authorized recipient of the funds.	Positive identity is accomplished through the multi-factor authentication (MFA) and identity verification measures that are in place. Notification of participant-requested account changes and fund distributions are sent to the participant’s preferred method of contact.

**6. 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**

We leverage a hybrid cloud data center strategy that utilizes multiple Tier IV data centers and providers. We remain in full control of our industry-leading security requirements for cloud and third-party managed data and services within this strategy. We determine how the data/services are stored and secured and who has access to the data/services.

Criteria responses	DOL cybersecurity best practices	Empower protocols
✓	Requiring a risk assessment of third-party service providers	<p>Prior to contracting with critical suppliers, we conduct third-party vendor risk assessments that include reviews of financial, technical, and operational controls. In addition, security requirements are included in contract language, and audits are performed at least annually.</p> <p>Physical and environmental security controls of our hybrid cloud strategy are evaluated within our SOC 2 Type 2 audits by independent AICPA auditors. These facilities are also compliant with all required regulatory compliance laws and cloud provider compliance standards associated with the services performed.</p>
✓	Defining minimum cybersecurity practices for third-party service providers	<p>Our service vendors maintain the same level of security and privacy controls required of Empower based on the confidentiality category of the information shared.</p> <p>Requirements are governed by contractual agreements and regulatory compliance law.</p>
✓	Periodically assessing third-party service providers based on potential risks.	Third-party due diligence evaluations are performed at least annually for all partners who have access to NPI/PII.
✓	<p>Ensuring that guidelines and contractual protections at minimum address the following:</p> <ul style="list-style-type: none"> <li>• The third-party service provider’s access control policies and procedures, including the use of multi-factor authentication</li> <li>• The third-party service provider’s encryption policies and procedures</li> <li>• The third-party service provider’s notification protocol for a cybersecurity event that directly impacts a customer’s information system(s) or nonpublic information</li> </ul>	Confirmed







## 7. Cybersecurity awareness training conducted at least annually for all personnel and updated to reflect risks identified by the most recent risk assessment

Empower associates are systematically assigned mandatory security awareness, privacy, and fraud awareness training throughout the year and additionally educated on current security events and vulnerabilities through periodic management communications. Training is assessed through a knowledge assessment system to achieve certification, and sessions are tracked to completion. In addition, unannounced email phishing campaigns are performed throughout the year. Follow-up training is leveraged to ensure our associates have the ability to properly identify incoming threats to our environment.

## 8. Secure system development life cycle (SDLC) program

Empower has implemented a systems development life cycle (SDLC) methodology that covers analysis, design, build and test, quality assurance, and installation and governs the development, implementation, and maintenance of application systems.

### Best practice response

DOL cybersecurity best practices	Empower protocols
<p>✓ Procedures, guidelines, and standards that ensure all in-house applications are developed securely. This would include such protections as:</p> <ul style="list-style-type: none"> <li>• Configuring system alerts to trigger when an individual's account information has been changed</li> </ul>	<p>If we receive account information changes, we proactively notify the individual plan participant to all points of contact that we have.</p>
<p>✓ Requiring additional validation if personal information has been changed prior to request for a distribution from the plan account and for distributions (other than a rollover) from the participant's account</p>	<p>Empower has a comprehensive fraud prevention program that includes additional verification for certain activities associated with a higher risk of fraud.</p>
<p>✓ Procedures for evaluating or testing the security of externally developed applications, including periodic reviews and updates</p>	<p>Security and Change Management assessments are performed on third-party software prior to implementation within the Empower network. Testing is based on OWASP (Open Web Application Security Project) standards.</p>
<p>✓ A vulnerability management plan, including regular vulnerability scans</p>	<p>Empower's vulnerability management program systematically identifies, evaluates, prioritizes, and mitigates vulnerabilities that may pose a risk to infrastructure and applications. Our modern vulnerability management program combines automation, threat intelligence, and data science to predict which vulnerabilities represent the greatest risk to a given environment.</p>
<p>✓ Annual penetration tests, particularly with respect to customer-facing applications</p>	<p>Empower performs annual security assessment and penetration tests of our network and externally facing web applications. Testing steps follow best practices and cover authentication and authorization, user and session management, error handling and exception management, and data validation (includes SQL injection, cross-site scripting, command injection, and client-side validation). Tests include the current OWASP (Open Web Application Security Project) top 10 and use the OWASP ASVS (Application Security Verification Standard) as a standard for application development.</p>

## 9. A business resiliency program that effectively addresses business continuity, disaster recovery, and incident response

Empower takes a multi-tiered approach to resiliency that includes an Incident Response Plan (IRP). The IRP provides guidelines for specific scenarios, including cyber-attacks, facility or technology disruptions, and many other scenarios. The IRP also provides a framework to assess and facilitate rapid remediation related to unknown disruptions and defines roles, responsibilities, and disaster declaration processes. A dedicated Enterprise Resiliency team oversees updates to and validations of the IRP, Business Continuity, and Disaster Recovery plans. An annual Business Impact Assessment (BIA) is conducted.

A multi-channel emergency communication system is utilized to allow rapid response and communication during disruptions. Additional information is found here on our website: [Business Continuity Plan](#) >.

## 10. Encryption of sensitive data stored and in transit

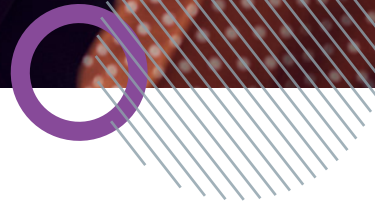
Empower encrypts all sensitive data at rest (stored) and in transit. All data at rest within the Empower network, including mobile devices, removable media, and backup media, is encrypted. All Empower laptops and desktops are fully encrypted. Empower does not allow copying of data to USB drives, personal devices, or personal cloud storage. Empower's cloud data, both in transit and at rest, is encrypted.



## 11. Strong technical controls implementing best security practices

We employ industry-leading technology and security measures designed to defend against cybersecurity threats and safeguard client-sensitive information. Protection methods and resources include, but are not limited to:

- Network security controls and perimeter infrastructure risk assessments, including the use of multi-tiered firewalls, intrusion prevention systems, and web application firewalls designed to protect the network from outside attack
- Distributed denial of service (DDoS) defense and mitigation, endpoint security, and data loss prevention (DLP) solutions
- Malicious code protection, including anti-virus technology, Endpoint Detection and Response (EDR), and other systems and controls designed to protect against malware
- Threat-management procedures, including security operation centers, operate 24/7/365, designed to detect and manage advanced computer security incidents and persistent threats, and follow a formalized process for acting on identified threats
- Regularly scheduled internal and external network and application development vulnerability scans performed by independent security assessment firms and Empower security administration teams
- An enterprise-wide computer security incident response team (CSIRT) linked with the enterprise crisis response team
- Empower consumes numerous threat intelligence sources to stay informed of the latest risks, including solutions such as membership in threat intelligence sharing groups, monitoring of vendor announcements, and consuming intelligence feeds from security vendors.
- Encryption of sensitive information at rest and when transferred electronically on public communication networks



## Best security practices include

DOL cybersecurity best practices	Empower protocols
✓ Hardware, software, and firmware models and versions that are kept up to date	All hardware, software, and firmware models and versions are kept up to date, and automation is utilized when possible.
✓ Vendor-supported firewalls, intrusion detection, and prevention appliances/tools	Network security controls, including the use of multi-tiered internal and external firewalls, intrusion prevention systems, and data loss prevention solutions (DLP) and malware protection, are implemented to protect our network from attacks.
✓ Current and regularly updated antivirus software	Formal management software is utilized to manage desktop and server antivirus products. Virus reports are managed by the relevant system administration teams. Updates are automated.
✓ Routine patch management (preferably automated)	Empower performs regular and routine patch management. Patches are prioritized based on severity and applied using automated processes.
✓ Network segregation	Our network is segregated into zones protected by multi-tiered firewalls, web application, and next-generation firewalls (perimeter and internal) as well as VLANs, routers, and content services switches.
✓ System hardening	Empower servers and workstations are hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls.
✓ Routine data backup (preferably automated)	Automated full backups are performed on a routine basis.



## 12. Responsiveness to cybersecurity incidents or breaches

Empower has not experienced a security breach of our internal systems or unauthorized access to client data. All security breach notifications are coordinated through the Empower legal department in accordance with applicable contracts and state and federal law requirements. Empower would notify our plan sponsors of a data breach in accordance with regulatory requirements.

Best security practices include

DOL cybersecurity best practices	Empower protocols
<p>✓ Informing law enforcement</p>	<p>All response activities are coordinated with internal and external stakeholders and external support from law enforcement agencies as applicable.</p>
<p>✓ Notifying the appropriate insurer</p>	<p>Notifications for our contracted insurance policies pertaining to recordkeeping services are overseen and facilitated by the Empower Legal Department.</p>
<p>✓ Investigating the incident</p>	<p>Empower has a computer security incident response team (CSIRT) and response procedure to investigate known or suspected security breaches within our computing environment. The incident response procedure includes steps to research, respond, manage, and report suspected security breaches to help ensure business continuity.</p>
<p>✓ Giving affected plans and participants the information necessary to prevent/reduce injury</p>	<p>Empower protection and prevention brochures are available and widely distributed to our client community for safeguards and tips for avoiding malicious threats, vulnerabilities, and fraud scams.</p>
<p>✓ Honoring any contractual or legal obligations with respect to the breach, including complying with agreed-upon notification requirements</p>	<p>All security breach notifications are coordinated through the Empower legal department in accordance with applicable contracts and state and federal law requirements.</p>
<p>✓ Fixing the problems that caused the breach to prevent its recurrence</p>	<p>We review and revise incident response plans on an annual basis; revisions incorporate lessons learned from exercises and previous incident detection and response activities.</p>

Empower’s 82,000 plan sponsors and their 18 million participants’ trust us with their assets and identities, and that is not a responsibility we take lightly. We safeguard the retirement assets of some of the world’s largest financial, technology, healthcare, government, franchise, and educational organizations, defense contractors, and airlines. A partnership with Empower is built on a foundation of trust — the security of plan and participant information is critical to the success of our business. That’s why in addition to extensive security measures, Empower’s Security Guarantee affirms our promise to restore account losses resulting from unauthorized transactions that occur through no fault of the participant. Information regarding Empower’s Security Guarantee appears on the participant website so participants are aware of the commitment and how it works.



## Tips for hiring a service provider

The following guidance from the DOL is intended to help plan sponsors and fiduciaries select a retirement plan service provider with strong cybersecurity practices. Each item from the DOL document, [Tips for Hiring a Service Provider with Strong Cybersecurity Practices](#), is accompanied by a response detailing Empower's protocols.

### 1. What are Empower's information security standards, practices and policies, and audit results, and how do they compare to the industry standards adopted by other financial institutions?

Empower's comprehensive information security program includes regular assessments of our controls and extensive security testing, both with the aim of reducing risk to our organization. Empower's information security policies are aligned with NIST 800-53, and third-party auditors attest to the effectiveness of our policies and controls via our SOC 2 type 2 reports. We continually validate the controls of our comprehensive security program with unannounced tests and assessments, including penetration testing from multiple sources and internal and external security assessments. Our audit reports have unqualified opinions (clean reports) from our independent auditors.

#### Does Empower follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity defense in depth?

Empower uses several third-party services to provide independent evaluations of our network and systems security controls to test our defense-in-depth strategy. A sampling of these includes third-party external auditors performing annual attestations to produce AICPA SOC 1 type 2 and SOC 2 type 2 reports and Verizon Business Enterprise Risk Group, whose certification program addresses all aspects of proactive cybersecurity measures and controls. Yearly results of these evaluations have been excellent, and relevant findings are remediated immediately.

### 2. How does Empower validate your practices, and what levels of security standards have you met and implemented? What audit results can we review to demonstrate compliance with the standard?

Within the secure plan sponsor website provided by Empower, we provide documentation that supports and informs the plan sponsor about Empower's current security program and practices. These documents are referred to as the Security Assurance Package (SAP), which currently consists of the following items which are updated annually: Cybersecurity Assurance Reference Guide Outline (CARGO), SOC 1 type 2 report, SOC 2 type 2 report, available IT certification reports (e.g., Verizon CRP), and a completed SIG-Lite (Standardized Information Gathering) questionnaire with related supporting materials. The SIG-Lite is a standardized document template created by the Shared Assessments Program, a consortium of leading financial institutions, the Big 4 accounting firms, and companies from a wide array of industries. Empower's Data Security Addendum and Privacy Addendum are available upon request.

### 3. What is Empower's track record in the industry, including public information regarding information related to your services?

Empower is a leader in the retirement plan recordkeeping industry and remains committed to maintaining the security of the accounts we service. We are dedicated to giving all our clients the best customer service and the best cybersecurity protection regardless of plan size.



- Value for price<sup>2</sup>
- Web tools and functionality<sup>2</sup>
- Plan design flexibility<sup>2</sup>
- Payroll integration<sup>2</sup>
- Advisor sales and marketing support<sup>2</sup>
- Fee structure for advisors<sup>2</sup>

**planadviser.**

### 4. Has Empower experienced past security breaches, what happened and how did you respond?

Empower has not experienced a security breach of our internal systems or unauthorized access to client data.

Fraudulent activity and identity theft are major threats in today's computing environment. Empower has developed an online security guarantee to restore participant account losses resulting from any unauthorized transactions that occur through no fault of the participant. Information regarding the security guarantee appears on the participant pre-login website so participants are aware of the commitment and how it works.



**5. Does Empower have any insurance policies that cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participant's account)?**

Empower maintains cyber liability insurance policies that include coverage for items such as the following:

Cyber incident response costs (legal and regulatory), IT security, forensic, crisis communication, privacy breach management (including the accidental or deliberate actions of a rogue employee or contractor); system damage and rectification costs; system business interruption; network security and privacy liability; management liability; regulatory fines; and media liability. Identity theft could lead to third-party hijacking of client funds and may be covered under our Security Guarantee and bond program, which includes social engineering and fraudulent transfer instructions.



Please note that Empower is its own first line of defense for fiduciary matters and supplements its capital with various insurance policies as an industry best practice. Empower is backed by the full faith and financial strength of its parent company, Empower Annuity Insurance Company of America, which is AM Best rated A+, Stable, XV (rating as of January 25, 2024).\* Empower doesn't cap its liability for account losses arising from unauthorized activity, whether in case of fraud against an individual or a cyber breach of an organization.

The insurance is intended to be additional protection and does not limit Empower's liability. The aggregate of these insurance policies is \$100 million plus \$75 million (Canadian currency). Empower strives to purchase the broadest coverage available in the insurance markets.

\*AM Best: Superior (highest of seven rating categories and second highest of 13 possible ratings).

As of January 2024. Ratings are subject to change and represent the opinions of the rating agencies regarding the financial strength of our primary insurance companies, Empower Annuity Insurance Company of America, Empower Life & Annuity Insurance Company of New York (ELAINY), and Empower Annuity Insurance Company, and their ability to meet ongoing obligations to their respective policyholders. Ratings do not pertain to any offered product or any affiliates or subsidiaries. Empower Financial Services, Inc. is a subsidiary of EAICA and an affiliate of ELAINY.



**6. When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards — and beware of contract provisions that limit the service provider’s responsibility for IT security breaches. Also, try to include terms in the contract that would enhance cybersecurity protection for the plan and its participants, such as:**

#### **Information Security Reporting**

Empower is fully prepared to discuss with plan sponsors the specific processes and practices we follow in protecting data and accounts. Empower maintains AICPA SOC 1 and SOC 2 reports on an annual basis from third-party auditors. Empower’s Data Security Addendum and Privacy Addendum are available upon request.

#### **Clear Provisions on the Use and Sharing of Information and Confidentiality**

Empower’s contracts contain confidentiality and nondisclosure provisions that fully address these obligations. In addition, these provisions also address the organizational, technical, and procedural safeguards used to protect the confidential information of our clients. Empower handles participant data in accordance with all applicable privacy and data protection laws.

#### **Notification of Cybersecurity Breaches**

Plan sponsor notification of security breaches is coordinated through the Empower legal department in accordance with applicable contracts and state and federal law requirements.

#### **Compliance with Records Retention and Destruction, Privacy, and Information Security Laws**

Personal identifiable information is stored in the U.S. and is encrypted at rest and in transit when on public networks. Records are retained for up to seven years in accordance with corporate policies and regulatory compliance laws as well as contractual agreements. All workstation and server hard drives are wiped by Empower personnel, then destroyed by a contracted disposal vendor.

#### **Insurance**


Empower carries Commercial General Liability, Financial Institution Bond and Electronic and Computer Crime Policy, Insurance Company and Asset Management/ Investment Company Professional Liability (also known as errors and omissions), and Cyber Liability Insurance.



## ONLINE SECURITY TIPS

The [DOL's Online Security Tips](#) provide guidance for plan participants and their beneficiaries to reduce the risk of fraud and loss in their retirement accounts:

- 1 Register, set up, and routinely monitor your online account.
- 2 Use strong and unique passwords.
- 3 Use multi-factor authentication.
- 4 Keep personal contact information current.
- 5 Close or delete unused accounts.
- 6 Be wary of free Wi-Fi.
- 7 Beware of phishing attacks.
- 8 Use antivirus software, and keep apps and software current.
- 9 Know how to report identify theft and cybersecurity incidents.



*Empower has long believed in the importance of providing participants the tools to adequately protect their accounts and private information.*

*Each of the nine security tips listed by the DOLs are comprehensively addressed on Empower's Security Tips web page.*



► For additional questions on our compliance with the DOL cybersecurity best practices, please contact your Empower representative

1 As of September 30, 2023. Information refers to all retirement business of Empower Annuity Insurance Company of America (EAICA) and its subsidiaries, including Empower Retirement, LLC; Empower Life & Annuity Insurance Company of New York (ELAINY); and Empower Annuity Insurance Company (EAIC), marketed under the Empower brand.

2 PLANADVISER, Retirement Plan Adviser Survey, November 2022.

For more information regarding account security, including the Empower Security Guarantee, visit [empower.com](https://empower.com) and, from the list of additional links at the bottom of the page, click *Security center*.

**Securities, when presented, are offered and/or distributed by Empower Financial Services, Inc., Member FINRA/SIPC.** EFSI is an affiliate of Empower Retirement, LLC; Empower Funds, Inc.; and registered investment adviser Empower Advisory Group, LLC. This material is for informational purposes only and is not intended to provide investment, legal, or tax recommendations or advice.

"EMPOWER" and all associated logos and product names are trademarks of Empower Annuity Insurance Company of America.

The credit bureaus listed are not affiliated with Empower, LLC and its affiliates.

These best practices are for informational purposes only. They apply to U.S. residents. Security risks and recommendations change frequently. Follow the alerts, recommendations, and announcements from your service providers, law enforcement agencies, and consumer protection agencies.

**Unless otherwise noted: Not a Deposit | Not FDIC Insured | Not Bank Guaranteed | Funds May Lose Value | Not Insured by Any Federal Government Agency**

©2024 Empower Annuity Insurance Company of America. All rights reserved. GEN-FBK-WF-1220861-0224(3112652) RO3359693-0224