TRA
The Retirement *Advantage*

Cybersecurity: What We Do to Align with DOL Guidelines

In 2021, the Department of Labor's (DOL's) Employee Benefits Security Administration (EBSA) issued twelve points for cybersecurity risk mitigation in the retirement industry. Constantly strengthening our cybersecurity is a primary focus and perpetual endeavor at The Retirement Advantage, Inc. (TRA). Here are the ways we work continuously to stay in alignment with the DOL guidelines and protect the security of our clients' assets and personal information.

Guideline 1. Have a formal, well documented cybersecurity program.

What we do:

TRA has strong security policies, procedures, guidelines, and standards that we review regularly to ensure compliance with applicable laws, regulations, and alignment with industry standards.

TRA maintains a well-documented Written Information Security Policy (WISP), which is based on industry-recognized frameworks and best practices. The program supports the implementation and maintenance of administrative, technical, and physical safeguards to protect personal and other sensitive information that TRA collects, creates, uses, and maintains in connection with its operations. The program also protects TRA's systems and operations from unauthorized access, breach, and interruption.

Guideline 2. Conduct prudent annual risk assessments.

What we do:

TRA has a risk assessment program that identifies internal and external risks to the security, confidentiality, integrity, and availability of our information systems and data.

The program's processes and controls apply across all technology and information assets used for business or IT support purposes, including IT services provided by third parties.

Guideline 3. Have a reliable annual third-party audit of security controls.

What we do:

TRA partners with independent, industry leading vendors to evaluate and assess our security controls at least twice a year and determine cybersecurity goals and priorities. We take security seriously here, we conduct annual penetration tests and have plans to undergo a third-party audit of our security controls in 2023.

Guideline 4. Clearly define and assign information security roles and responsibilities.

What we do:

TRA's Director of IT and Security establishes and maintains the vision, strategy, and operation of the cybersecurity program and IT team.

IT team members maintain current knowledge of changing cybersecurity threats and countermeasures and receive updates and training on cybersecurity risks. They also stay up to date on a variety of information security topics, including cybersecurity, intelligence, threat controls, information risk, cybercrime, forensics, encryption, network and physical security, identity management, and counter measures.

Guideline 5. Have strong access control procedures.

What we do:

We govern and control access to TRA systems by logical access control policies and standards to manage the authorization, administration, authentication, and timely termination of all access rights. We provision access based on the principle of "least privilege" and "need to know." We document all access requests and follow a defined approval process.

User access management procedures ensure that access to systems and services is authorized and restricted to appropriate individuals and that we regularly review access. In addition, we have implemented risk-based policies, procedures, and controls to monitor the activity of authorized users and detect unauthorized access, use, or tampering with nonpublic information.

TRA maintains authentication standards which require multi-factor authentication when accessing systems and data.

Guideline 6. Ensure that any assets or data stored in a cloud or managed by third-party providers are subject to appropriate security reviews and independent security assessments.

What we do:

TRA employs security standards that cover both our on-premises as well as cloud-based hosting environments. These security standards consider location, availability, visibility, and control over the data and services. We have default security policies and controls, which we review and modify to ensure they comply with TRA security standards. We risk assess all third-party service providers prior to use and again periodically throughout their life cycles.

Guideline 7. Conduct periodic cybersecurity awareness training.

What we do:

TRA has developed a custom cybersecurity training course based on TRA's security standards and policies and industry specific risks, which all TRA team members are required to complete as part of the onboarding process, in addition to third-party cybersecurity training modules.

Everyone must also complete periodic online information security training.

Guideline 8. Implement and manage a secure System Development Life Cycle (SDLC) program.

What we do:

TRA has several key controls that are part of a SDLC. These controls cover development, quality assurance, change management, testing, and implementation. TRA's dedicated, highly experienced programming staff enhances our system continually. Management approves all requirements, and we document all changes within our change management control system, which also allows audits as needed. We have a quality assurance process to carefully review enhancements before they go into production.

TRA maintains documented vulnerability management and collaborates closely with our technology partners to identify, assess, prioritize, and re-mediate vulnerabilities. We conduct vulnerability scanning at both the infrastructure and application level using standard industry tools.

Guideline 9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

What we do:

TRA maintains a Business Continuity Plan which documents the procedures to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels in the event of a disruption.

We have an extensive Disaster Recovery Program that includes off-site backups with immutable storage, in addition to third-party hosted Disaster Recovery as a Service for critical systems. TRA also maintains an Incident Response Policy that establishes how we respond in the event of a cybersecurity incident.

Guideline 10. Encrypt sensitive data, stored and in transit.

What we do:

TRA uses current, prudent standards for encryption keys, physical security, message authentication, and hashing to protect the confidentiality and integrity of data.

We utilize the following best practices:

- Self-encrypting drives to store data at rest
- Endpoint encryption
- Enterprise-grade firewalls to encrypt data in transit
- Access controls to secure our sites and servers

These encryptions utilize the 256-bit Advanced Encryption Standard. We scan messages for sensitive data and handle them based on their classification.

Guideline 11. Implement strong technical controls in accordance with best security practices.

What we do:

TRA utilizes documented security configuration baseline standards which establish the controls required to safeguard operating systems, software, network, and cloud to “harden” these systems against cyberattacks. These standards leverage the Center for Internet Security (CIS) Benchmarks, National Institute of Standards and Technology (NIST), or other relevant industry guidelines. TRA applies a “defense-in-depth approach” to protect sensitive, nonpublic information.

Guideline 12. Appropriately respond to any cybersecurity incidents or breaches.

What we do:

TRA maintains an Incident Response Policy which establishes how we respond in the event of a cybersecurity incident. It also outlines an action plan that we use to investigate potential incidents and to mitigate damage if a breach were to occur. This policy is in place to both minimize potential damages that could result from a data breach and to ensure that we inform all affected parties about the ways they can best protect themselves.

CYBERSECURITY IS IMPORTANT TO YOU... IT’S IMPORTANT TO US, TOO.

As you know, cyberattacks are on the rise and no one is immune. That is why it’s vital to understand what the service providers you choose to do business with are doing to address threats to you and your employees.

With TRA’s comprehensive cybersecurity strategy and protocols, we continuously monitor for attacks and vulnerabilities to protect your data and give you comfort when doing business with us.

To learn more, visit our website’s **Cybersecurity** page.

The
Advantage
Is Yours