U.S. Department of Labor and Cybersecurity

Ameritas Retirement Plans Best Practices

Ameritas retirement plans is committed to protecting your confidential plan participant information. The U.S. Department of Labor (DOL) also is concerned about cybersecurity and has published guidance for plan sponsors, plan fiduciaries, recordkeepers, and plan participants — providing best practices and tips on protecting retirement benefits. This guidance, issued in 2021 and updated in 2024, also provided best practices for plan service providers to protect plan participant data. Ameritas, as a plan service provider, is committed to these best practices.

Inside this document is an outline of the DOL cybersecurity program best practices and how Ameritas meets them.

Ameritas®
fulfilling life®

1 Have a formal, well documented cybersecurity program.

Ameritas has implemented an Information Security Program to ensure the confidentiality, integrity, and availability of Ameritas information systems and data. The program is led by the VP and Chief Information Security Officer (CISO), who reports to the Senior VP, Risk and Compliance of Ameritas. The CISO reports the security and risk posture of the organization on a regular basis to executive management.

Ameritas maintains information security polices to clearly define requirements Ameritas must adhere to in support of the Information Security Program. These policies and supporting standards are aligned with the NIST Cybersecurity Framework (CSF), as well as the requirements of applicable federal and state laws, rules, and regulations, and reflects industry best practices such as those defined in the U.S. Department of Labor's Cybersecurity Program Best Practices.

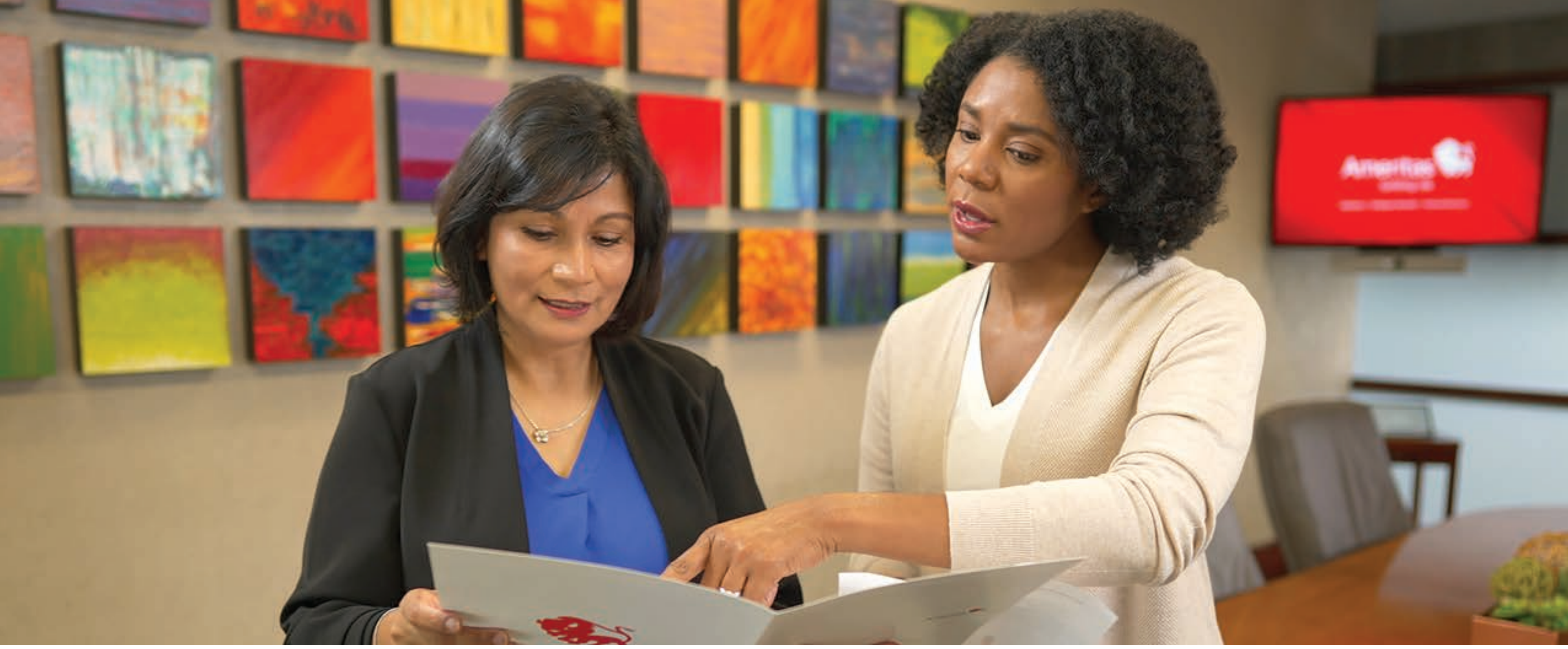
2 Conduct prudent annual risk assessments.

Security risk assessments are conducted no less than annually to identity threats to assets, operations, and security posture. Risks are documented and ranked according to likelihood and impact, which drive the design and implementation of corrective actions. Results are reported through the CISO to executive management.

The Information Security Risk assessment framework and focus was built using the NIST Cybersecurity Framework (NIST CSF) and is aligned to and supports the Ameritas Information Security Policy. The assessment also meets requirements laid out by current regulations such as those under HIPAA, DOL and the New York State Department of Financial Services.

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

In addition to routine internal audit and risk assessment activities, Ameritas also conducts external risk and compliance assessments, which enables Ameritas to continuously improve the Security Program process controls. Annually, a third-party auditor conducts a SSAE18 SOC-1 Type II audit of Ameritas' controls. Ameritas also reviews our vendors' SOC-1 and SOC-2 audits on an annual basis.



4 Clearly define and assign information security roles and responsibilities.

The Ameritas Information Security Program is led by the VP and Chief Information Security Officer, who reports to the Senior VP, Risk and Compliance of Ameritas. The program is composed of qualified employees who maintain industry standard certifications, have completed background checks and regularly attend and participate in updates and continuing education to keep them up to date on cybersecurity risks and trends.

5 Have strong access control procedures.

Ameritas has clearly defined authentication and authorization controls to protect the personal data of our participants. Access to systems and data is based upon the principal of least privilege. Key controls include documented access control policies and standards, strong password requirements, multi-factor authentication for administrative and remote system access, and encrypted VPN for remote systems access. At least annually, management conducts a review of all employees' systems access to ensure that access to systems, especially those that contain personally identifiable information (PII), is limited to employees in roles that have a specific business use and have authorization in accordance with their assigned job responsibilities.

Systems are monitored by a dedicated security operations team 24/7 to detect and respond to system threats and security incidents, including unauthorized access to sensitive data.

6 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.

Ameritas maintains the Third Party Risk Management program (TPRM) to assess and monitor the security risk of external vendors, cloud service providers, suppliers, and service providers who process, store, and/or transmit Ameritas non-public data on behalf of Ameritas. Third parties are assessed upon onboarding and periodically based on the risk they present and the continued adequacy of their cybersecurity practices.

Contracts with third parties that hold sensitive data have cybersecurity addressed with agreed-upon measures to protect our clients and Ameritas in any instance of a breach.

7 Conduct periodic cybersecurity awareness training.

Ameritas associates are required to complete mandatory security awareness, privacy, and fraud awareness training annually. They are also educated throughout the year during management meetings and various other meetings. Additionally, Ameritas conducts regular email phishing campaigns that are unannounced and actively monitor the success rate.

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

Ameritas maintains a secure development life cycle for the development and maintenance of application systems. It provides for the analysis, design, building and testing, quality assurance, installation, and maintenance of application systems.

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

Ameritas recognizes that a major disruption of business operations could have a serious impact on financial and customer service operations. Ameritas maintains a Business Continuity and Disaster Recovery Program, which is managed by the Risk Management team and IT team respectively. Business continuity plans and IT recovery plans are developed to allow for continuous business operations in the event of a disruption or disaster.

Recovery strategies have been developed for three scenarios – loss of location, loss of resources and loss of people. Business continuity and technology recovery exercises are conducted at least annually to support the continuous improvement of recovery capabilities.

10 Encrypt sensitive data, stored and in transit.

Ameritas has implemented controls, including encryption, to protect sensitive data held or transmitted by Ameritas both in transit over external networks and at rest.

Transmission of Ameritas non-public data/personal information on a public Internet network or wirelessly must be encrypted.

Data is encrypted at rest at the storage level (e.g., on endpoints as well as enterprise storage).

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

Ameritas has strong controls and security practices which are tested in our SOC audit and internal audits that are conducted at least annually. We have technology and security personnel that manage cybersecurity controls in accordance with applicable laws and regulatory requirements. Key technical controls include:

- A vulnerability and patch management program, assessing vulnerabilities in the environment and patching systems based upon risk.
- System hardening in line with CIS benchmarks.
- Industry standard boundary protection capabilities, including firewalls and data-loss protection.
- Anti-malware and EDR software on endpoints and servers.
- Routine data backups.

12 Appropriately respond to any past cybersecurity incidents.

Ameritas takes cybersecurity incidents seriously and has established a formal incident response plan designed to promptly respond to, and recover from, cybersecurity events affecting the confidentiality, integrity or availability of Ameritas information systems and data or the continuing functionality of our business or operations. This plan defines the organizational roles and responsibilities for incident response and steps for incident detection and analysis; containment, eradication and recovery; and post incident activity. The plan is reviewed and tested at least annually.

Ameritas®

fulfilling life®