CAPTRUST

CAPTRUST CYBERSECURITY BEST PRACTICES:
Executive Summary Response to Department of Labor Guidance

The intense spotlight on information security has increased demands on plan fiduciaries and affiliated service providers to protect client data against cyberthreats and breaches. In April 2021, the Department of Labor (DOL) emphasized the requirement for plan sponsors to exercise increased cybersecurity due diligence for all fiduciaries and service providers with access to plan or participant data. The DOL has laid out precise instruction for plan fiduciaries to follow when assessing service providers.

CAPTRUST meets the DOL's guidance and regularly assesses its performance against the same robust framework (NIST 800-53) used by the DOL in developing its assessment methodology. CAPTRUST addresses each of the 12 information security actions as follows:

1. A Formal, Well-Documented Cybersecurity Program

CAPTRUST's Information Security Program is aligned to the NIST 800-53 framework and is governed by the following policies:

- Information Security Policy
- Information Technology and Security Standards
- Incident Response Plan

These policies offer broad coverage on how CAPTRUST identifies and protects its information assets and systems, then detects and responds to threats to those assets and systems.

2. Prudent Annual Risk Assessments

CAPTRUST employs a nationally recognized information security vendor to perform an annual security risk assessment (SRA) to assist in identifying and prioritize information security risks.

3. Reliable Annual Third-Party Audit of Security Controls

CAPTRUST uses multiple recognized information security vendors to perform network and web application penetration tests, providing a clear and unbiased report of existing risks, vulnerabilities, and weaknesses. These reports provide the basis for remediation and ongoing improvement in CAPTRUST's security posture.

4. Clearly Defined and Assigned Information Security Roles and Responsibilities

CAPTRUST's information security program is managed and executed by vetted, seasoned, and credentialed personnel. Spearheading these efforts are a chief technology officer with 31 years of industry experience and a senior manager of IT information security with 11 years of industry experience. Security roles are clear, and responsibilities are appropriately distributed across the team. Regular formal and self-directed personnel training is driven by proactive departmental values of inquiry and investigation to maintain a clear understanding of the changing threat landscape and appropriate countermeasures.

CAPTRUST CYBERSECURITY BEST PRACTICES:
Executive Summary Response to Department of Labor Guidance

5. Strong Access Controls

CAPTRUST has robust access controls spanning devices (NAC via Cisco ISE), user accounts (Active Directory; MFA enforced via Okta), user access reviews (SailPoint), and privileged access management (CyberArk PAM) that protects privileged user/administrator accounts through daily credential rotation of random 25-to-32-character passwords. Service accounts are being retrieved from CyberArk (CyberArk CCP) using certificates obtained through Azure KeyVault (in the process of implementation).

6. Assets and Data Stored in a Cloud or Managed by a Third-Party Service Provider are Subject to Appropriate Security Reviews and Independent Security Assessments

CAPTRUST performs robust due diligence on key cloud suppliers who store, handle, or process nonpublic personal information (NPII) of CAPTRUST clients or supply critical services. A third-party security firm is employed to assist in the risk assessment process. It performs external vulnerability scans of each providers' public-facing technology infrastructure and administers risk assessments. SOC audits, which are completed by recognized CPA firms, are also reviewed by certified internal staff to complete an overall risk assessment.

7. Cybersecurity Awareness Training Conducted at Least Annually for All Personnel and Updated to Reflect Risks Identified by the Most Recent Risk Assessment

CAPTRUST holds Lunch-and-Learn training sessions on a quarterly basis. Information security awareness training is also administered through a third-party and is offered more than a dozen times each year.

8. Implement and Manage a Secure System Development life cycle (SDLC) Program

SDLC program standards are intended to provide security assurance through the following activities:

- Daily reviews of change requests (CRs) to code, software configurations, and infrastructure
- Development standards that adhere to OWASP
- White-box code reviews (Sonarcloud) and manual and automated QA testing prior to rollout to production
- Two annual penetration tests by independent, nationally recognized information security vendors
- A vulnerability management program that includes daily scanning of information assets and responsive patching

CAPTRUST CYBERSECURITY BEST PRACTICES: Executive Summary Response to Department of Labor Guidance

9. A Business Resiliency Program that Effectively Addresses Business Continuity, Disaster Recover, and Incident Response

The firm maintains a comprehensive business continuity plan, a critical incident response plan, and incident response plans for technology, information security, facilities, and personnel disruptions. A summary of the firm's business continuity plan is published on our website and focuses on how we will serve clients through a variety of disruptive events. (CAPTRUST performs annual disaster recovery tests to validate preparedness in the event of a business continuity event.

10. Encryption of Sensitive Data Stored and in Transit

CAPTRUST employs encryption that meets or exceeds federal (FIPS) standards, ensuring that sufficient protections are in place to preserve the confidentiality and integrity its data assets. Encryption is applied in the following data states:

- At-Rest
- In-Transit
- Backups

11. Strong Technical Controls Implementing Best Security Practices

CAPTRUST utilizes industry-leading technical controls that include monitoring, endpoint protection, email protection, education and awareness, and access control management. CAPTRUST's security strategy is comprehensive, proactive, thoughtful, and implemented in a complementary manner to policy and procedure. This approach creates sustainable tailwinds, propelling CAPTRUST's security efforts.

12. Responsiveness to Cybersecurity Incidents or Breaches

Time is a precious commodity during a cybersecurity incident, and how a company responds may spell the difference between a minor incident and a major one. CAPTRUST employs a comprehensive set of security measures spread across administrative and technical controls that aid in the phases of prevention, detection, response, and recovery. CAPTRUST's preparedness and ability to respond is based on a team approach between the information security, network, server, and infrastructure teams.

Should an event warrant external assistance, CAPTRUST also has immediate access to its regional FBI office and nationally recognized incident response and forensics companies to further aid in the identification, containment, investigation, eradication, recovery, and follow-up steps of incident response.