Prudential's information privacy and data protection

Staying ahead of the risks

What Prudential customers need to know

Ensuring that personal, confidential information remains private and secure is a critical concern for plan sponsors, advisors, participants and providers. As customers seek the convenience of having their information available across multiple online platforms, the threat of a cyber security incident or potential identity theft/fraud has intensified.

While these risks can never be eliminated, a carefully designed and executed Information Privacy and Data Protection program is the best defense against malicious activity. To that end, and in our ongoing effort to ensure the best protection to our customers, Prudential has designed its Cyber Security program to adhere to regulatory requirements and to align to several industry standards and best practices. Some of those requirements and standards include:

- National Institute of Standards and Technology
- NYDFS Cybersecurity Regulation (23 NYCRR 500)
- State of Connecticut Insurance Data Security Act
- SPARK Data Security Best Practices
- ISO27001
- Employee Benefits Security Administration of the U.S. Department of Labor Cybersecurity guidance for retirement plans

Design and controls

The proliferation of online risks and threats means that privacy and security must be embedded into the design specifications and architecture of technologies, business practices and physical infrastructures.

Prudential has adopted a layered Information Security Program, which includes the following defenses:

- Multiple built-in firewall protections
- End point blocking and data loss prevention protocols
- Risk-based multi-factor for employees and customers
- Layered network, database and operating system defenses, including an industry-leading tool set
- "Least privileged" user access to data and applications
- Secured data sharing using industry-standard encryption solutions

Our control environment is further strengthened by requirements within our business processes around the collection, and use and storage of personal information, which are regularly assessed.

Continuous monitoring and education

In conjunction with the defenses listed above, Prudential performs real-time monitoring to test the strength of its systems. This includes:

- Risk-based vulnerability scanning and remediation across both the external and internal network and in all environments including DevOps
- Deployment of intrusion detection / intrusion prevention systems throughout the network, with monitoring by Prudential's Centralized Security Operation Center (CSOC) 24 hours a day / 7 days a week
- Malware detection and infected device quarantine procedures
- Security and Privacy awareness education

Finally, ongoing dialogue and Q&A sessions with new and existing clients contribute to our extensive knowledge base, allowing Prudential to better understand key points of concern and adjust our approaches based on feedback.

Awareness and training

Establishing a business environment that values and rewards integrity is the best foundation to ensure the successful implementation of data security and privacy principles. Prudential takes this a step further by making sure all employees – and employees with access to personal, confidential information in particular – are aware of the threat of malicious activity and well-trained in how to avoid situations with a heightened risk of exposure.

At Prudential, all employees are held to the standards outlined in the following policies:

- Prudential's code of conduct, Making the Right Choices, which requires that we protect information as a critical component in meeting our obligations to customers, employees and shareholders.
- Prudential's privacy policy, Confidentiality of Personal Information, which requires that we keep personal information confidential.
- All employees are required to attest that they are following Prudential's code of conduct and ethics standards on an annual basis.

From a best practice standpoint, we promote awareness of trends in cyber fraud and threats to privacy through regular articles on our intranet site and through leadership and team discussions of our responsibilities to our customers.

Continuous program growth

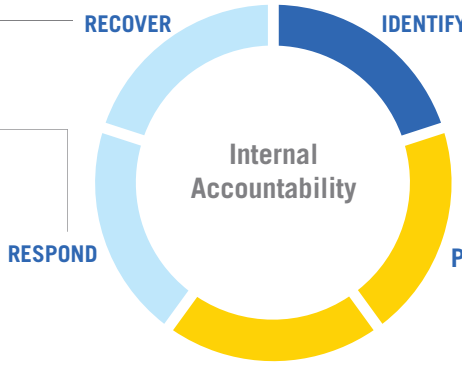
We understand that in order to continuously protect our customer assets, we need to stay a step ahead of industry vulnerabilities.

Through ongoing assessments, we have information security program initiatives to continue to enhance the security on our websites and internal applications. The Information Security and Privacy initiatives roadmap is designed to continuously improve each program. It's never-ending because the threats and landscape continue to change. As an organization, we understand that, so we budget, source and educate as an ongoing requirement.

Prudential's commitment is that, in addition to maintaining its Information Security and Privacy programs, the company is continually investing in new security tools and controls to all access points, external and internal, as new information becomes available or new threats or patterns of suspicious activity are identified.

Our program is modeled after the National Institute of Standards and Technology (NIST) framework:

- Collaboration across Prudential to track, report and respond to threats
- Documented and tested incident response plans
- Dedicated cyber forensics team



- Internal and external audits
- Peer and industry assessments
- Regulatory oversight
- Risk management

- 24/7 Cyber Security Operations Center
- External threat intelligence
- Defenses tested through Red team exercises and penetration testing
- Enterprise training and awareness

Prudential's framework aligns with industry standards

Employee Benefits Security Administration United States Department of Labor Cyber Security Program Best Practice

ISO 27001

THE SPARK Institute

NIST National Institute of Standards and Technology U.S. Department of Commerce

Best practices – Employee Benefits Security Administration of U.S. DOL (April 2021)

Because Prudential's cyber security program is already aligned with ISO27001 and other industry recognized standards, Prudential is already well-positioned to align with EBSA's cybersecurity principles:

1. Have a formal, well-documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
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.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.*
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

*Data transmissions protected via trusted network with dedicated devices and peripherals. Our self-contained, secure computing facility secures all data transmissions including those possible in the event of a dynamic routing update.

For more information about Prudential's information privacy and data protection program, contact your Prudential representative.

1049007-00001-00
For Plan Sponsor Use.
NOT01_FL_RE177_01 06/2021