Information Security

Protecting your information

We protect your information in many ways—from ensuring that our buildings are secure, to proactively preparing for disasters and business interruptions, to using secure computing practices. Safeguarding your information's confidentiality, integrity, and availability is one of our highest priorities.

One of our highest priorities is safeguarding your information's confidentiality, integrity, and availability.

Our program

We have a comprehensive written Information Security Program that safeguards information against unauthorized or accidental modification, disclosure, fraud, and destruction.

- Security policies, standards, and procedures are documented and available to employees.
- Collection of personal information is limited to business need and protected based on its sensitivity.
- Employees are required to complete privacy, security, ethics and compliance training.
- Work area assessments are completed to ensure protection of information and information systems.
- Risk management processes and procedures are documented and communicated.

Our online security features

Customer access to web and mobile applications requires the use of unique usernames and strong passwords. We use adaptive authentication systems to evaluate a customer's location at the time of authentication and monitor historical patterns of login locations. Additional login security features in place are:

- Security questions and answers.
- Verification codes.
- Timed log-off.

For accounts that support it, we recommend two-factor authentication, which requires both your password and an additional code to log in to your account. This helps protect account information when logging in even if your password is compromised.

Incident management

We have detailed processes to track, manage, and resolve all incidents.

All incidents are investigated. If a data security incident is discovered, an incident response plan is promptly initiated and thoroughly executed. We adhere to all applicable state and federal disclosure laws.

Antivirus protection

All Windows servers and workstations have antivirus software installed, and updates to definitions are applied frequently.

Our information technology managers review recurring reports to ensure compliance levels are met. All alerts are reviewed by staff in the cyber defense operations center.

Security software

We use secure communications solutions called Transport Layer Security (TLS).

All modern browsers support TLS, but if your browser does not, you will receive a message indicating that your session cannot be completed because of the security risk. We require customers use a TLS-enabled browser to communicate with the secure area of our site. We recommend using the most current browsers to ensure a high level of security. Web browsers supported by Microsoft, Mozilla, Apple, and Google support TLS 1.2, the latest encryption technology.

Information Security

Business Continuity (BC) and Disaster Recovery (DR) programs

We have a BC and DR program. Critical business functions, processes, and supporting applications have been identified and are regularly reviewed. Appropriate response and recovery plans have been developed. Testing is completed annually.

The basis for the program is professional best practices established by the Disaster Recovery Institute International (DRII), Business Continuity Institute (BCI), and International Organization for Standardization (ISO). The technology recovery plan leverages geographically distant data centers, while the incident management process facilitates response and recovery activities appropriately implementing plans if a disruptive event occurs.

Access

We have a formal, documented process to grant and revoke access to company resources (systems, data, mobile, etc.) that is supported by administrative, technical, and physical controls.

Our employees may not access or disclose personally identifiable information for any purpose except as authorized for company-related business purposes.

Industry collaboration

Principal is a member of the Financial Services—Information Sharing and Analysis Center (FS-ISAC).

FS-ISAC is an industry forum for collaboration on critical security threats facing the global financial services industry.

Cyber security insurance

We have cyber security insurance.

Our policy provides Network Security and Privacy Liability insurance coverage. It includes any network security or privacy event discovered during the policy period affecting a majority owned member company of Principal® and events originating from our third party service providers.

Patch management

We monitor for significant new vulnerabilities and attacks that have the potential to affect our systems and apply patches and mitigations as appropriate.

We have a vulnerability management practice that regularly tests our systems to ensure that they are not open to attack.

Additional security practices

- **Call centers have procedures to help validate the identity of callers.**
- **Social Security numbers are eliminated from all correspondence unless legally required.**
- **Regular training is conducted with employees on detecting fraudulent activities.**
- **Strict standards that limit access to data are followed.**
- **Regular testing of our security technology is performed.**

Vetting third party service providers

We have a defined Supplier Management Program which includes processes for vetting, selecting, and monitoring third party service providers.

Third party security profiles are completed when certain types of data are provided to and/or stored at a third party location. A separate detailed risk assessment is completed if the third party is granted access to our networks, systems, or data.

Principal Life Insurance Company, Des Moines, Iowa 50392-0002, www.principal.com
EE11699-02 | 01/2019