Information Security

Protecting Your Information

Principal protects 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. Doing so is one of our highest priorities to ensure your information's confidentiality, integrity, and availability.

One of our highest priorities to ensure your information's confidentiality, integrity, and availability.

Our Program

Principal has 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 customer information and compliance with company policy.
- Risk management processes and procedures are documented and communicated.

Security Protocols

Customer access to web and mobile applications requires the use of unique usernames and strong passwords. Principal also uses adaptive authentication systems to evaluate a customer's location at the time of authentication and historical patterns of login locations. Plus the following:

- Login image and phrase.
- Security questions and answers.
- Timed Log-off.

Incident Management

Principal has 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 servers and workstations have antivirus software installed, and updates to definitions are applied frequently.

Information Technology managers review recurring reports to ensure compliance levels are met.

Encryption

Company laptops and desktops are required to be encrypted, and dual authentication is required before laptops can be accessed remotely. Confidential data in transmission is encrypted.

Encrypted data is transmitted via secured connections, such as:

- HTTPS (HTTP over TLS).
- Secure File Transfer Protocol (SFTP) over the Internet
- Pretty Good Privacy (PGP) encryption via SFTP.

Information Security

Business Continuity (BC) And Disaster Recovery (DR) Planning

Principal has 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.

Professional best practices established by the Disaster Recovery Institute International are utilized as the basis for the program. The technology recovery plan leverages geographically distant data centers. The incident management process facilitates response and recovery activities appropriately leveraging plans if a disruptive event occurs.

Access

Principal has 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.

Access is restricted to those with a business need. Employees may not access or disclose personally identifiable information for any purpose except as authorized for company-related business purposes.

Patch Management

Updates, patches, and fixes are quickly communicated to affected areas to address critical security issues (e.g., vulnerabilities).

Systems are consistently monitored to identify vulnerabilities and threats and updated when needed.

Cyber Security Insurance

Principal has cyber security insurance.

Our policy provides Network Security and Privacy Liability insurance coverage and 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.

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.

Third Party Service Providers

Principal has 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

EE11699-01 | 04/2016