Protecting you and your information

Your personal information is important to you. It's important to us, too. That's why we do so much to protect your information, while continually providing service you can count on. One of our highest priorities is maintaining the privacy and confidentiality of customer information.

While no one can guarantee absolute information security, we protect your information in many ways – from working to ensure that our buildings are secure, to proactively preparing for disasters and business interruptions, to using safe and secure computing practices. We continuously review and make enhancements to how we safeguard and protect customer information.

We continuously review and make enhancements to how we safeguard and protect customer information.

Privacy and security are a priority

We take privacy and the confidentiality of our customers' information very seriously at The Principal. We are committed to maintaining your confidence in us. We apply industry best security practices and have

procedures in place to protect data entrusted to us. These procedures and related standards include limiting access to data and regularly testing and auditing our security practices and technologies. Employees and temporary workers are required to follow policies and procedures plus complete confidentiality training to understand

the requirement of maintaining the confidentiality of customer information. If they fail to do so, they are subject to disciplinary action. Personal information about employees or customers is only disclosed as required or permitted by law and in accordance with established company procedures.

We have a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. A full time dedicated security team helps ensure the security of information we process and store.

Protected and prepared

Disasters and business interruptions can occur without warning. We are committed through our Business Continuity Planning Program to protect and preserve our business records and financial and informational assets through continuous business operations. Our Business Continuity Planning Program is based on the professional practices established by Disaster Recovery Institute International. Regular simulation exercises are held across the organization to be action ready for any disasters or business interruptions. Employees are trained to report data breaches immediately. We have a data incident response plan in place to promptly investigate and respond to any breach of data.

Protecting your data on-site

Our Global Physical Security Standards program helps all areas of our company reduce risk and work to ensure compliance with corporate standards. This program includes controls such as physical risk assessments, access control, physical security technology, staff, policies and procedures. Our Global Security Operations Center provides security services and response 24 hours a day, seven days a week.

Proactive protection via systems

Virus protection

Files coming into the company network are scanned for viruses and other malicious software. We deploy anti-virus software in our email management system, Web and application servers, as well as on all desktops. Our standard procedures require updating of virus signature files each day. In addition, we have a Corporate Incident Management Plan that provides emergency procedures designed to quickly contain any virus outbreaks. Employees are trained to recognize signs of potential computer infections in addition to recognizing phishing scams as preventive measures to decrease risk of an outbreak.

Intrusion detection

Intrusion detection systems monitor network traffic both to and from the Internet. These systems are designed to note and intercept or block suspicious activities. In addition, we have a top-tier security event management solution that supports real-time incident response and facilitates further investigation.

Proactive risk protection via processes

Risk management

We use multiple risk management processes and procedures. We perform security reviews of vendors who may store or process company information. We require a risk review in projects that touch all business lines. Perimeter and infrastructure reviews are completed regularly. Reviews of work areas are completed in each of our business units annually. We require all vendors to conform to defined security requirements.

Cybersecurity Protocols

We utilize a set of industry standards and best practices developed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework to align our risk management processes.

Independent security assessment

We partner with various external consulting firms to test our defenses and report on any vulnerability detected. This helps ensure your personal information is protected from malicious code (viruses, spyware, adware, ransomware, etc.) and other online threats.

Encryption

We have encryption tools to enhance the integrity and confidentiality of confidential information. Documents and email that include sensitive information are encrypted prior to being sent over public networks. Company laptops and desktops are required to be encrypted, and dual authentication is required before laptops can be accessed.

Records retention and destruction

We retain business records for the period of time necessary to meet business requirements and legal obligations. We destroy business records in a manner designed to protect confidential information. All paper documents are shredded or otherwise rendered unreadable upon disposal. Electronic media is also rendered unreadable prior to destruction.

People you can trust

One of our most important assets is our employees. And they take action to protect your information. All employees are required to complete privacy, security, ethics and compliance training. We also offer a wide variety of other training to all employees and temporary workers that help us achieve our goal of protecting your information.

For the most current version of this document, visit www.principal.com.

Principal Life Insurance Company, Des Moines, Iowa 50392-0002, www.principal.com

EE10128-05 | 10/2016