



## 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.



## 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](http://www.principal.com).

## 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.