

Cybersecurity and data privacy

We take data privacy and security seriously. We maintain policies and procedures designed to comply with applicable state and federal rules as well as employ the following measures:

<p>Information security</p>	<p>We have policies and procedures for identifying, assessing and managing material risks associated with cybersecurity threats. To help protect our information technology (IT) resources, we have instituted administrative, physical and technical controls and processes and commissioned third-party assessments. The technical defense measures we have implemented are designed to address vulnerabilities that may arise, including from a security control failure. These measures currently involve a combination of artificial intelligence (AI); machine learning computer network monitoring; malware and antivirus resources; firewall systems; and endpoint detection and response. We also utilize cloud service defenses; Internet address and content filtering monitoring software intended to secure against known malicious websites and potential data exfiltration; and enterprise gateway security for workforce mobile devices and applications. Additionally, a variety of cyber intelligence and threat monitoring sources provide us with ongoing updates on potential or emerging risks. For all these measures, we rely on third-party providers that we believe are capable of performing the service for which they have been engaged or on certain governmental agencies. Before we engage a third-party provider for these types of services and resources, we typically conduct a security review involving, as relevant to the service or resource, discussions with the provider’s security personnel, evaluation of auditor reports, and other requested information and documentation.</p>
<p>Employee education and awareness activities</p>	<p>To support the ongoing identification and management of cybersecurity issues, all employees are required to complete cybersecurity awareness training, including social engineering and phishing, Internet security, physical security and insider threats, and additional AI-enabled cyber threats and deepfakes, with additional training for handling of customer personal information. We also publish a monthly security awareness newsletter along with performing ongoing internal phishing assessments.</p>
<p>Customer privacy</p>	<p>We do not sell our mailing or contact lists to unaffiliated third parties. KB Home may share customer email addresses and contact information with our selected service providers for home-related offers and other information that we believe may be of interest to our customers; however, customers are able to indicate on the guest information, registration card or other materials that they do not wish to be contacted.</p>
<p>Leadership oversight</p>	<p>Our Board of Directors, through its Audit and Compliance Committee, monitors cybersecurity risks and our evolving physical, electronic and other protection strategies and initiatives. Our management executives periodically review our cybersecurity practices and risks with the committee, most recently in January 2026.</p>

