

INFORMATION SECURITY POLICY

AIA Holdings, Inc., Allegheny Casualty Company, Associated Bond and Insurance Company, and affiliates – Information Security Policy for Web and EULAs

Cybersecurity Practices

As technology becomes more complex and sophisticated, so do the cyber risks that businesses and organizations face. We have implemented technologies and tools to implement cybersecurity protections and maintain a cyber risk management strategy related to information security that includes monitoring emerging security threats and assessing appropriate responsive measures.

Policy & Governance

AIA Holdings, Inc., Allegheny Casualty Company, Associated Bond and Insurance Company, and their affiliates, maintain a comprehensive set of information security policies and standards, which are modeled to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Our information security policies and standards have been developed in collaboration with groups across the enterprise, such as Legal, Compliance, HR and each of our business segments. Our policies include, for example, Information and System Use policies for employee and non-employee system users.

We perform an annual information security assessment as part of our Information Security Management Program (ISMP).

Technology

We use various technologies and tools, as appropriate, to enhance information security, such as multifactor authentication, encryption, firewalls, intrusion detection and prevention, vulnerability scanning, and patch management.

In addition, our CISO team is actively engaged within the information security community in order to monitor emerging trends and developments and acquire intelligence for identifying and mitigating cyber threats. Additionally, the company's Cybersecurity team investigates suspicious events.

As the workforce, the work environment and the threat landscape continue to evolve, we continue to evaluate related risks and implement appropriate controls.

Training & Awareness

To help manage risks from potential cybersecurity threats, as part of our annual cybersecurity training, all employees receive data protection and privacy training, which focuses on the need to appropriately protect and secure confidential company information. We also provide regular targeted training on topics such as phishing and secure application development, among others. In addition to online training, employees are provided with cybersecurity related information through a number of different methods, including event-triggered awareness campaigns, recognition programs, security presentations, intranet articles, videos, system-generated communications, email publications and various simulation exercises.

Third-Party Relationships

As part of our supplier risk management program, using a risk-based approach, the information security team works with our vendor management team to conduct assessments with respect to our third-party service providers based upon the risk of each third-party.

Where appropriate, we seek to incorporate contractual language with third party service providers that includes clear terms involving the collection, use, sharing and retention of user data, as well as compliance with appropriate security terms.

Incident Response

We have a Security Incident Response Plan in place. The Incident Response team, under the direction of the CISO, executes on the IR plan with the goal of ensuring timely and accurate resolution of information security incidents.

Additional Information Additional information regarding privacy and security, including our Privacy Statements, is available on our website.