AXIS Statement on Data Privacy and Cybersecurity

April 2025

Statement on Data Privacy

AXIS is committed to complying with applicable data privacy and protection laws and regulations in all jurisdictions where we operate and to implementing leading data protection standards to protect our customers' and users' privacy. It has adopted a suite of policies and procedures that apply to the whole enterprise and to all business lines to ensure the transparent use and security of individuals' personal information.

AXIS' Privacy Notices, accessible here (https://www.axiscapital.com/who-we-are/privacy-notice), reflect the scope of our policies and include details of when, why and how we collect and use personal information, share it with third parties and keep it secure. The Notices explain the rights of individuals, which include access, correction, and deletion, and how individuals can exercise those rights. We also pledge to minimize the amount of data collected to only what is necessary, for as long as necessary, and do not sell data to advertisers or marketing companies.

Data protection, privacy and security at AXIS is overseen by the Data Protection Officer and Chief Information Security Officer, who regularly report to the management Operational Risk Committee (ORC). AXIS has processes and procedures for undertaking due diligence on third parties and vendors with whom we share personal information. AXIS also has established contract review policies, which aim to ensure that third party and vendor contracts address data privacy and protection wording if applicable. In addition, AXIS has procedures for responding to data incidents and the exercise of individual rights.

All employees and contractors are required to complete an annual privacy and data protection training program. This training is designed to ensure that all understand and are aware of the principles of data minimization and purpose limitation, their responsibility for protecting both personal information and non-personal commercially sensitive information, and how to recognize and respond to a data incident or the exercise of individual rights.

Statement on Cybersecurity

Understanding and managing evolving cybersecurity risks is an integral part of our business. Our cybersecurity program uses controls to prevent, detect, and respond to threats against our users, systems, and information. To date, no cybersecurity incidents have materially impacted the Company, including the Company's business strategy, results of operations, or financial condition.

Key components of the program include the following:

- **Industry Standards.** Our security program is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the industry standard used

by several governments and a wide range of businesses. The NIST Cybersecurity Framework includes adoption of Zero Trust principles to protect digital assets.

- **Security Awareness.** As our staff and vendors are the front line of defense against advanced threat actors, all users of our internal systems, including part-time staff and contractors, must complete annual cybersecurity awareness training.
- **Risk Mitigation Services.** As a provider of cyber insurance, we also offer our distribution partners and policyholders access to a range of risk mitigation services delivered by partner organizations and vetted by our Cyber underwriting team. These services include cyber awareness training, risk assessment tools, network security and monitoring tools and incident response services. In addition, we periodically send customers and users communications regarding cyber resilience best practices and alerts based on our claims insights.
- **Third-Party Risk Management.** We review the security of our critical vendors used across our organization to assess whether their cybersecurity programs meet our standards. We closely manage our connectivity to third parties and reassess their security measures to protect our systems and data against a constantly evolving threat landscape.
- **Security Monitoring & Response.** Our Security Operations Center (SOC) monitors security events 24x7x365, deploys preventative and detective controls throughout our environment, and promptly responds to potential security threats.
- **Network & System Security.** We protect our networks and sensitive customer information behind robust firewalls, intrusion prevention, and other advanced security technologies. Our systems are kept current through rigorous vulnerability and patch management practices.
- **Access Management.** We manage access to information systems and data using industry standard identity and access management lifecycle controls. These controls provide authorized users access to the resources they need and help to prevent unauthorized users from obtaining sensitive information through fraudulent means.
- **Security Assurance.** We proactively identify and remediate cybersecurity threats to our environment and our partners through advanced penetration testing, systems hardening, and other activities used to continuously strengthen our cybersecurity posture.
- **Business Continuity and Notification.** In the event of a manmade or natural disaster, whether cybersecurity in nature or other, our Business Continuity Program is prepared to continue conducting critical business activities in a secure manner. We also have comprehensive backup procedures to enable the recovery of our data in the event of a system failure.
- **Cybersecurity Incident Response Plan.** AXIS has a cybersecurity incident response plan that includes procedures for responding to various types of cybersecurity incidents and tested through periodic tabletop exercises. This approach aligns with the NIST Computer Security Incident Handling Guide. The CIRP addresses the necessary processes

and legal requirements pursuant to rules and regulations promulgated by the SEC, GDPR and the various state cybersecurity regulations.

Board Governance

The Board, together with the Risk and Audit Committees, oversees our information security program. In 2024, our Board and Risk and Audit Committees received periodic updates throughout the year on cybersecurity matters, and these updates are part of their standing agendas. These updates include reports regarding items such as cybersecurity strategies, program effectiveness, key risks and performance metrics related to the Company's information security program and the Company's mitigating controls.