ALPHAWAVE SEMI

IT Policies and Cybersecurity

In 2022, the Company went through a period of accelerated expansion both organically and through acquisitions. As a result, in 2022 we started a review of the IT policies across the business to align and prioritise IT investment with evolving business needs and to maintain compliance and controls.

Group wide Security policies and IT controls are being reviewed and updated by a newly established Security Council which is chaired by the IT Director. The policies seek to address the regulatory environment, including data privacy regulations, and to mitigate the evolving cyber security threat. We are ensuring that all relevant policies are aligned with the NIST 800-53 framework and ISO 27001.

Our efforts are managed by our IT Director, who oversees a comprehensive, multidisciplinary program involving information security, IT, and physical security.

Our IT Director reports directly to our Senior Vice President, Engineering, and regularly updates our Board of Directors on our cybersecurity performance and risk profile. All our existing policies and procedures are assessed regularly by our external auditors as well as third-party consultants.

We maintain cyber-liability insurance that covers certain liabilities in connection with security breaches or related incidents. In 2022, Alphawave did not experience any material information security breaches.

We also address cybersecurity scenarios in our resiliency planning and document them through business continuity plans. Our Incident Response Program facilitates integrated response to potential cybersecurity events.

In order to support these activities, during 2022 the Company expanded the IT Team.