Virgin Galactic Holdings, Inc.

Cybersecurity Overview

At Virgin Galactic, we take a risk-based approach to cyber security and customer data privacy that is intended to identify and address the highest priority information risks applicable to our business. Our information security department executes rigorous oversight of our data and the data entrusted to us across all our internal and external systems and applications. This includes regular in-house and third-party testing, auditing, patch management, identity and access management, and data loss prevention. We use several market leading tools and services to support our security program, which is oriented around compliance with industry standard control frameworks including NIST 800-171 and ISO 27001. Our data privacy program is led by a dedicated internal privacy team and supported by a privacy management technology platform. It is aligned with all applicable U.S. Federal and State privacy laws, as well as with the more stringent European General Data Protection Regulation ("GDPR"). We have experienced no material data breaches in the last 3 years, nor have we been notified of any breaches at our major third-party suppliers during this period.

We extend our high data security and privacy standards to our vendors and partners as part of a broader third-party risk management program. Where applicable, we seek vendor compliance with industry standards such as ISO 27001 and SOC 2 Type II. Due to the nature of our business, we often default to the most secure and robust cloud platforms available (e.g., Microsoft Government Community Cloud High; FedRAMP compliant), which in turn benefit our commercial business as well.

Our information security governance program is structured to ensure alignment with business objectives and has visibility by senior leadership. Our Board of Directors is briefed on our information security program on a quarterly basis.

We communicate regularly with our employees regarding the importance of data security and privacy. In addition to direct updates about Internet safety, phishing, and other topics, we require annual mandatory security training and more frequent training for select employee groups.