Veeco Instruments Inc.
Sustainability Report

Interim Update – Information Security (March 2021)

Veeco's Information Security function is tasked with proactively monitoring, identifying and mitigating risks to Veeco's assets, data and confidential information. These risks include unauthorized access to customer data, theft of company intellectual property, compromise of company systems impacting normal business operations, and compliance with regulatory requirements in a complex global regulatory landscape.

To mitigate these risks Veeco retains dedicated information security resources to monitor and address all identified risk through the application of layered security controls in alignment with the National Institute of Science & Technology ("NIST") Cybersecurity Framework ("CSF"). Veeco periodically retains external services to assess its maturity within the NIST CSF and to further identify technology risks within its environment.

In addition, Veeco requires that its employees undergo annual information security awareness training and operates quarterly phishing exercises to ensure that employees understand their information security-related responsibilities.

Veeco supplements its information security program with a cyber insurance policy.

Veeco's Chief Information Officer delivers regular quarterly reports on the information security program to the Audit Committee. These reports include the status of risk identification and mitigation efforts, projects to strengthen the company's security poster and improve resiliency, and updates on the evolving threat landscape.

Veeco previously disclosed an information security breach on November 1st, 2018 which has since been remediated. Expenses directly related to this breach totaled approximately US$687,000 in 2018 and US$624,000 in 2019. The company has suffered no known breaches before or after the 2018 breach and has not incurred any penalties or entered any settlement agreements regarding information security breaches.

Dated: March 8, 2021