Benchmark's Cybersecurity Statement

At Benchmark Electronics, cybersecurity is an important element of our sustainability efforts. Benchmark is committed to protecting the confidentiality, integrity, and availability of data across our global operations, ensuring trust with our customers, employees, suppliers, and shareholders.

Our commitment includes:

Governance and Oversight: Cybersecurity risk is overseen by our Board of Directors and is integrated into our enterprise risk management framework. The Audit Committee is responsible for reviewing the Company's policies, guidelines, and processes concerning cybersecurity risk exposures and the steps management has taken to monitor and control any such risks.

Security Frameworks: Our information security policies and practices, including our Information Technology Disaster Recovery Plan, are designed to comply with DFARS/NIST 800-171 controls and CMMC requirements. Our controls are continuously evaluated and updated to address evolving and potential threats.

Incident Response and Resilience: We have formalized incident response protocols and conduct regular exercises to ensure preparedness. We assess and monitor the cybersecurity posture of our vendors and partners, incorporating security requirements into our procurement and onboarding processes.

Employee Awareness and Training: All employees receive cybersecurity training, including phishing simulations and secure data handling practices. We foster a culture of security awareness across all levels of the organization.

Data Privacy: We prioritize the protection of personal and customer data in compliance with applicable laws and regulations. This commitment underscores our focus on responsible digital practices and ongoing enhancement of cybersecurity governance, aligning with our broader sustainability commitments.