



**H.B. Fuller**

Connecting what matters.™

## **H.B. Fuller Statement on Confidential Information, Information Security and Data Privacy**

The Company's Confidential Information is among its most vital assets. The Company is committed to protecting its Confidential Information, including its Trade Secrets, from unauthorized disclosure, whether externally or internally, whether deliberately or accidentally. Employees, and others who are under an obligation to protect the Company's Confidential Information, must not disclose Confidential Information to anyone outside of the Company except pursuant to an appropriate confidentiality agreement. Likewise, Confidential Information may be shared within the Company with other employees only on a business need-to-know basis. Just as the Company places great importance on protecting its Confidential Information, the Company respects its competitors' and business partners' confidential information, and Company employees shall not disclose any confidential information obtained from prior employment or other sources.

We rely on information technology to record and process transactions, manage our business and maintain the financial accuracy of our records. In today's business environment, information technology security threats are increasing in frequency and sophistication. Therefore, we include information security, also known as cybersecurity, in our annual review of significant risk factors that impact our Company and its businesses. In addition, we manage cybersecurity risk on an on-going basis through a security vulnerability management program and through periodic third-party cybersecurity risk assessments. Based on the results of these assessments, we prioritize efforts to address the highest ranked cybersecurity risks at the Company. We also maintain Information Technology Security Risk insurance policies to cover certain losses related to cybersecurity breaches of our systems.

Our Board of Directors receives a review of Information Technology and Cybersecurity on an annual basis, while the Audit Committee of our Board of Directors reviews cybersecurity at the Company at least twice per year. In addition, we provide a cybersecurity training program that includes yearly information technology and cybersecurity training for all employees and periodic "anti-phishing" exercises twice a year. The Company has not experienced a material information security breach during the last three years.

We have in place a Global Data Privacy Policy that articulates the privacy and data protection principles followed by the Company with regards to the personal information of its employees, job candidates and business partners. As a global company with a tradition of upholding the highest ethical business standards, we respect and are committed to protecting personal data in a manner that is consistent with both business needs and the laws of the countries in which we operate.