Training, Annual Certifications and Cyber-Security

Training Generally

Employees are provided with a wide range of training and development opportunities such as classroom instruction, tuition reimbursement, leadership development programs, eLearning courses, and one-to-one mentoring programs. These are designed to develop and prepare our employees for expanded roles within our company, including future leadership roles. In 2025, our employees received on average approximately 15 hours of training.

We also enable employee development and growth by offering full-time U.S. employees who have at least 12 months of service the ability to participate in the tuition reimbursement program. Through the program, employees can have specified expenses from secondary institutions reimbursed.

Cyber-Security Training

We deploy cyber-security training monthly.

In 2025, we trained all employees who use email regarding how they can help AMETEK mitigate cyber-security risks by deploying twelve courses to over 13,000 AMETEK employees with a completion rate of over 97%.

In 2025, we also conducted at least ten simulated phishing attacks against all employees who use email. The simulations were designed to entice employees to disclose confidential information using social engineering techniques. Employees that do not pass the simulations receive reinforcement training.

Specialized personnel, including Finance and Customer Service, receive targeted training periodically to educate them on the techniques used by external parties to create fraudulent transactions that may result in a financial loss to AMETEK.

Cyber-Security

We have experienced, and may in the future experience, whether directly or through third-party service providers, information security breaches. These events have not caused material disruption to our business in the last three years. Additionally, AMETEK has not incurred any expenses from information security breach penalties or settlements in 2023 – 2025. The impact of future information security breaches cannot be predicted.

As we rely on third-party service providers and platforms, we use a variety of processes and tools to address cyber security threats related to the use of third-party technology and services, including diligence, imposition of contractual obligations and performance monitoring. As part of our monitoring, we regularly obtain System organization and Control Reports (SOC Reports) for key third-party financial systems.

Several of our UK businesses are externally audited and certified by UK Cyber Essentials and UK Cyber Essentials Plus, which are considered top information security standards.

Annual Certifications

All full-time employees who interact with vendors, customers or have access to financial records are required to certify annually as to their compliance with key AMETEK policies including the code of conduct, conflicts of interest and anti-corruption. In 2025, compliance surveys were sent to over 17,000 AMETEK employees with a response rate of over 96%.

February 11, 2026