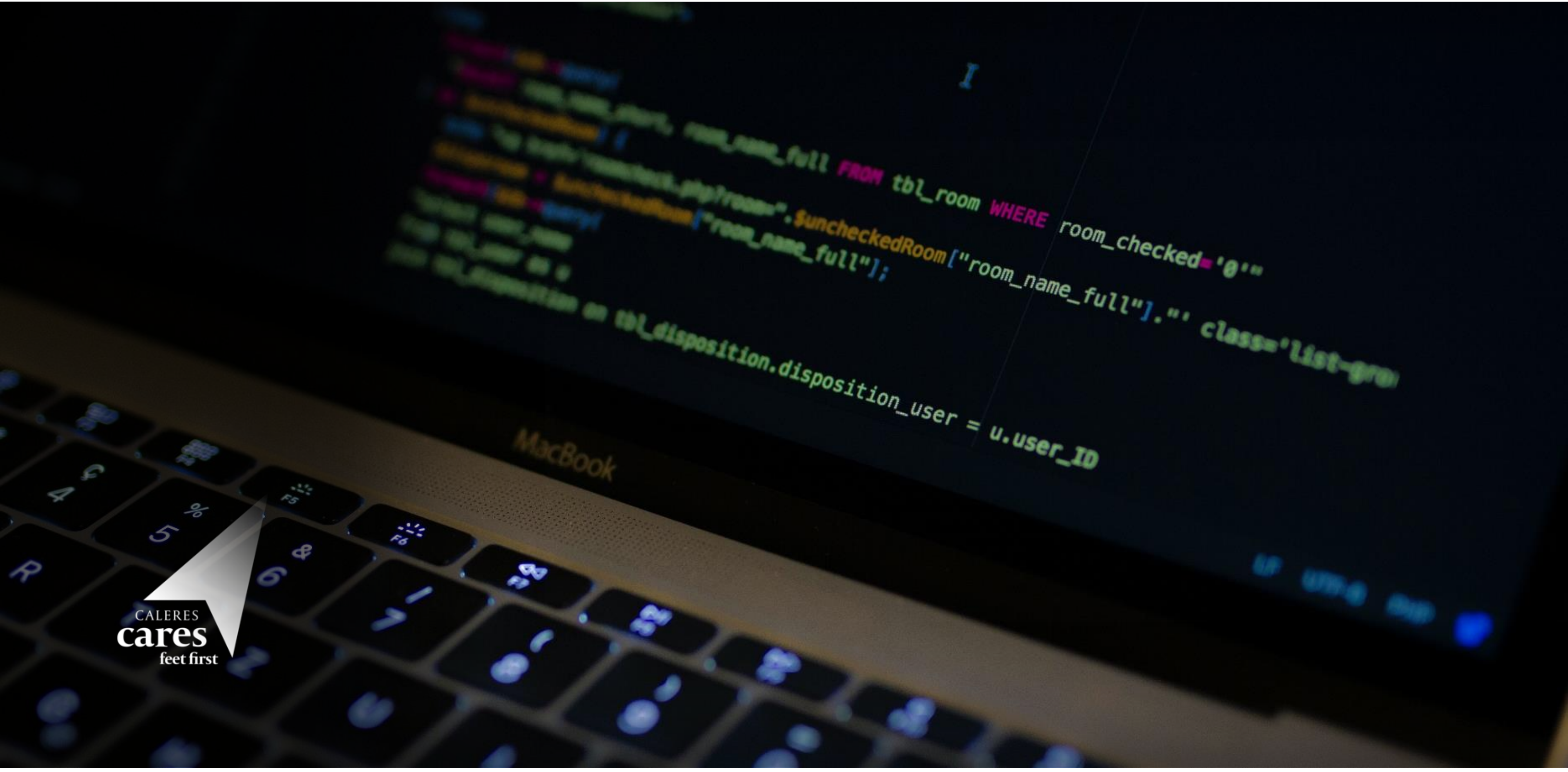

Cybersecurity and Data Privacy

Today's digital environment presents a continuously evolving threat to cybersecurity and data privacy. At Caleres, we use a broad mix of controls that encompass people, process, and technology to help us achieve our two main objectives: Reduce the attack surface, and quickly detect and defend against cyberattacks.

CYBERSECURITY

SAFEGUARDING CONSUMER DATA

Like many organizations, we experience frequent attempts at malicious cyberattacks. We utilize trusted threat intelligence and observable trends to ensure our tools are appropriately configured and updated to defend our environment.

In the retail industry, cyberattacks often target consumer payment information. We follow the Payment Card Industry Data Security Standard (PCI DSS), a framework of security controls that, when followed, optimizes the security of credit and debit card transactions to help us protect consumers.

Consumer purchases made in both brick-and-mortar stores and online are protected via PCI DSS-approved devices and payment solutions to protect cardholder data. Caleres does not store cardholder data.

DEFENDING INFORMATION INTERNALLY

Our "defense in depth" strategy includes a robust set of security tools designed to protect sensitive data and alert upon detection of abnormal or suspicious behavior. Associate access is granted based upon role assigned; roles are based on the principle of least privilege. Technical solutions are in place to manage and monitor the use of elevated rights and privileged accounts.

DATA PRIVACY

EDUCATING ASSOCIATES

Associates are typically our first defense against data privacy concerns. For this reason, all new hires complete a security awareness training program that Associates must complete annually. This training arms Associates with the knowledge and skills needed to understand and respond appropriately to potential threats.

We also execute monthly internal phishing campaigns and analyze results to develop targeted trainings as needed. Our IT team works diligently to communicate specific threats, publishes a monthly newsletter, and produces videos for our learning management platform.

Caleres also offers ongoing training and seminars for Associates specific to their roles.

COMPLIANCE AND CONTINUED MATURITY

Caleres submits to the following assessments to ensure appropriate protection of all sensitive data contained within the environment:

- **Annual Payment Card Industry (PCI) Assessment:** A third-party quality security assessor will use evidence, interviews and artifacts to validate compliance with the PCI DSS framework. In addition to the administrative review, a technical assessment is performed using the same tools hackers would use.
- **Third-Party Security Assessment:** We engage a third-party security partner on a recuring basis to assess the maturity of our cybersecurity program. This assessment is used to identify gaps and inform our cybersecurity strategy.

MAINTAINING HIGH STANDARDS FOR SUPPLIERS

We apply the same level of safeguards across our vendors and suppliers. When sensitive consumer and Associate information is exchanged, all third parties undergo a vendor risk assessment, which is designed to evaluate whether appropriate physical, technical, and administrative safeguards are in place, and sign a data processing agreement, which details the rights and obligations of each party concerning the protection and processing of data.