# Data Security

***Our governance policies, including the Information Security Policy, outline high level information security objectives designed to meet compliance and regulatory requirements.***

## Data Security

Costco identifies and addresses data security risks based on several frameworks, including the NIST Cybersecurity Framework (CSF), CIS 18 Critical Security Controls, and the Payment Card Industry Data Security Standard (PCI DSS). The company's governance policies, including the Information Security Policy, outline high level information security objectives designed to meet compliance and regulatory requirements. We have standards, procedures and programs to guide the management of data security risks.

Costco has implemented several technology measures, leveraging third-party security providers when needed and engages in multiple activities to seek to identify and mitigate vulnerabilities and risks in systems (e.g., scanning for common vulnerabilities and exposures, penetration tests on internal and external networks, code scans on applications, employee awareness and training, and internal and external audits). We also review on a risk-based priority third parties with whom we do business, in an effort to reduce the likelihood of security incidents or business interruptions.

## Defense in Depth Strategy

Costco employs a "defense in depth" strategy to address the attack chain and safeguard our systems and information. Some of the measures utilized by Costco include phishing detection and mitigation, multi-factor authentication, information system protection systems such as anti-malware, anti-ransomware, endpoint detection and response, file integrity monitoring, and other system hardening techniques.

Networks are protected using network detection and response capabilities, are segmented, and provide flow level visibility into lateral movement potential; e-commerce systems are protected by a web application firewall. This layered defense concept combined with our detection and response capabilities helps us reduce the potential risk of unauthorized access to our systems and information.

While our cybersecurity and compliance efforts seek to mitigate risks, there can be no guarantee that the actions and controls we and our third-party service providers have implemented and are implementing will be sufficient to protect our systems, information or other property. Our Vice President of Information Security reports regularly to the Board of Directors and senior management concerning our security practices.