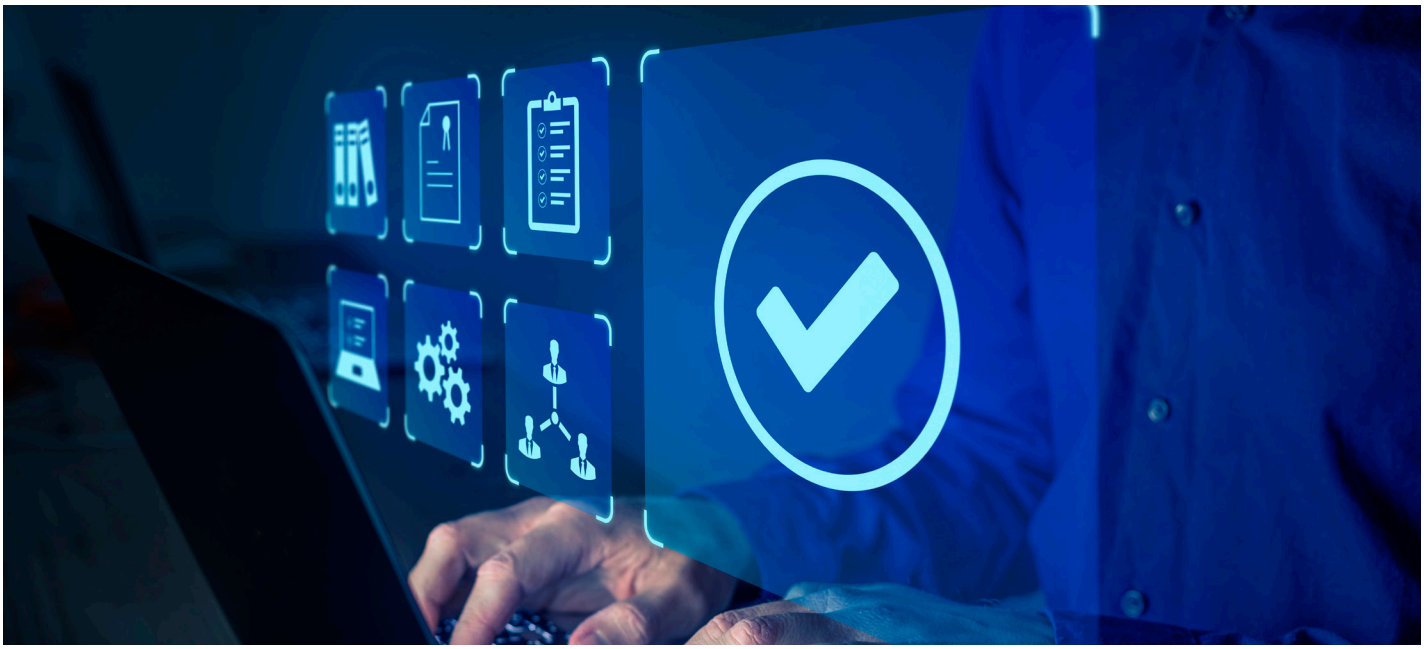
DELL Technologies

Overview

Personnel and Risk Management Overview

Dell Technologies is focused on a culture of trust and security across our global workforce. We recognize that actions from any of our team members could present a security risk, whether intentional or not. We have therefore devised, and continually improve, extensive programs to help prevent, detect, and deter security concerns within our workforce.



Training and Awareness

Our team members are a key part of our overall security approach. From onboarding to monthly newsletters, to annual training, to special awareness campaigns and more, we regularly educate team members about threats which could target them, how to detect and respond to those threats, and the consequences of behaviors which increase security risk. We encourage team members to recognize and report security issues throughout their career. Role-specific training is required for team members with specialized roles or access, like developers and IT administrators. Just in time training is provided to team members who are part of events which put them at a higher security risk. Progressive discipline is enforced for those whose actions increase security risk, including financial impact and potential employment termination.

Security Throughout the Employee Lifecycle

Our security programs mandate high standards for selection and training of our team. All employees receive an in-depth background screening before joining our team. Carefully building a trusted workforce helps serve the security requirements of both Dell and our customers. Additionally, we use advanced technology and analytics to alert our security team if unusual insider activity is observed for anyone with trusted access to our systems and information, underpinned by our advanced 24x7 security operations center.