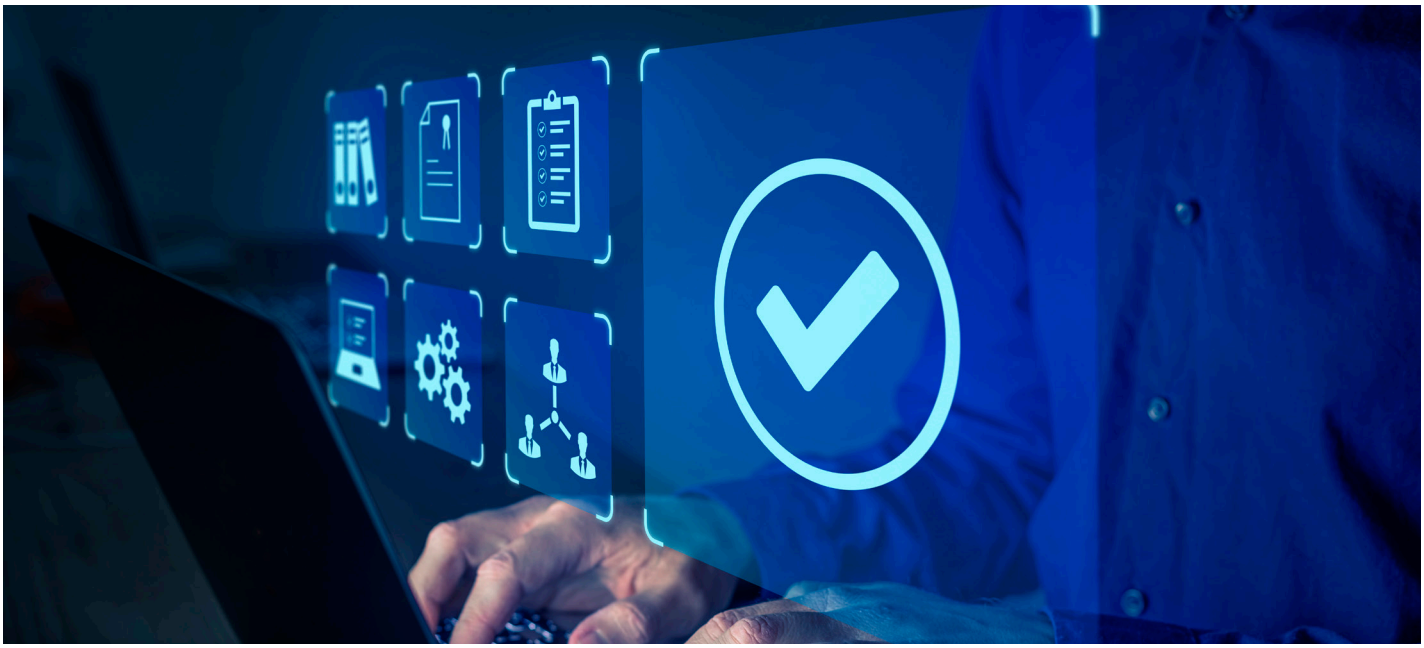
概览

人员和风险管理

Dell Technologies 注重在全球员工队伍中打造信任和安全文化。我们认识到可信的“内部人员”可能会有意和无意造成哪些风险，并制定了大量计划来检测、阻止和预防这些类型的安全事件。



培训和认知

团队成员是我们整体安全方法的关键组成部分。从入职培训到每月简报、年度培训以及特别宣传活动，我们定期教育团队成员，让他们了解成为不知情的内部人员的风险、如何预防这种危险，以及高风险安全行为的后果。我们鼓励团队成员在整个职业生涯中识别并报告安全风险。

对于具有特殊角色或访问权限的团队成员（如开发人员和 IT 管理员），需要接受特定角色的培训。如果团队成员参加的活动可能面临更高安全风险，我们会提供及时培训。对于表现出不安全行为的成员，我们将采取渐进式纪律处分，包括经济处罚，甚至可能解雇。

整个员工生命周期内的安全性

招聘合适的员工至关重要。在加入我们的团队之前，所有员工都会接受深入的背景调查。精心构建值得信赖的员工队伍有助于满足戴尔和客户的安全要求。

此外，在高级全天候安全运营中心的支持下，如果我们发现任何拥有系统和信息的可信访问权限的人进行异常内部人员活动，我们还会使用先进的技术和分析功能来提醒安全团队。