DELL Technologies

戴尔的企业安全性和弹性

概览

Dell Technologies 安全性和弹性部门 — 版本 1.1 — 上次更新时间：2023 年 4 月 5 日

对于如何建立信任并保护已然互联的世界，Dell Technologies 一直审时度势、深思熟虑。随着全球的互联化和智能化、5G 以及人工智能和机器学习等先进技术的出现，我们所能做的早已今非昔比，远超过去想象。我们要能适应不断变化的世界，并确保自身的安全性和弹性。而且，我们还将继续履行我们的重要使命 — 通过将安全性和弹性融入戴尔的各项工作，保护 Dell Technologies 并赢得客户的信任。

首席安全官 John Scimone

安全性与弹性部门

通过将安全性和弹性融入戴尔的各项工作，
保护 Dell Technologies 并赢得客户的信任。

网络安全

保护客户和公司数据

提供高级威胁情报，洞察新出现的威胁

身份和访问管理

管理网络风险，保持合规性并通过适当的方式保护环境

企业弹性、全局调查和公司安全性

企业弹性与安全性

企业安全性：管理对人员、信息、资产和声誉的各项保护措施，使他们免受物理和环境攻击，规避各类事件的影响

危机管理：管理可能对 Dell Technologies 产生负面影响的意外事件

业务连续性：确保能及时恢复业务关键型流程和运营

灾难恢复治理：确保能及时恢复业务关键型数据和系统

全局调查：管理盗窃、欺诈和工作场所暴力等实体安全事件

产品和应用程序安全性

漏洞响应：及时响应已报告的漏洞，确保部署的产品和应用程序安全无虞

安全的开发生命周期：通过确保整个开发生命周期的安全性，开发更安全的产品和应用程序

监管、风险和合规性

创建及维护 Dell Technologies 安全性和弹性策略、标准和流程，并确保它们的合规性

确保遵守外部法规，如萨班斯-奥克斯利法案 (SOX) 和支付卡行业数据安全标准 (PCI DSS)

执行审核，续订合同（其中阐明 Dell Techonologies 是客户的供应商）并向客户提供介绍戴尔产品和服务的安全规则和协议的相关信息。

Dell Federal | Dell Technologies Services | 戴尔金融服务

网络安全

网络安全部门为安全计划和技术设定标准，并对这些计划和技术进行实施和维护，从而帮助 Dell Technologies 管理和降低风险，抵御高级攻击者的侵害，保护我们的信息、业务、客户和品牌。

Dell Technologies 的网络安全部门负责：

- 保护客户和公司数据
- 提供高级威胁情报，洞察新出现的威胁
- 身份和访问管理
- 管理网络风险，保持合规性并通过适当的方式保护环境

为何关注网络安全?

4.5 小时

攻击者在入侵后，深入公司网络内部所需的平均用时

6 万亿美元

预计到 2021 年全球因数据泄露产生的成本

78 天

检测到复杂入侵所花费的平均时间

产品和应用程序安全性

产品和应用程序安全性部门的工作包括确保提供给客户的产品受到保护，能够抵御网络攻击，并且没有漏洞。

Dell Technologies 的产品和应用程序安全性部门负责：

- 安全的开发生命周期 — 通过确保整个开发生命周期的安全性，开发更安全的产品和企业应用程序
- 漏洞响应 — 及时响应已报告的漏洞，确保部署的产品和应用程序安全无虞

为何关注产品和应用程序安全性?

90%

的安全性事件是利用产品缺陷所致

100 倍

在维护阶段修复软件缺陷的成本是在设计阶段修复的成本的 100 倍

~60%

的数据泄露事件中，所涉及的漏洞已经有了针对性的修补程序

全球安全运营

全球安全运营部门的工作包括保护人员、信息、资产和声誉，使他们免受物理和环境攻击，规避各类事件的影响。Dell Technologies 的全球安全运营部门负责：

- 保护我们世界各地的员工、流程、资产和 Dell Technologies 品牌
- 管理防护措施和安全摄像头，调查员工和犯罪分子对公司实施的犯罪和非网络安全事件

全球安全运营的示例和措施：

- 危机管理
- 业务连续性
- 灾难恢复
- 内部人员风险管理
- 对犯罪和违反行为准则的事件进行调查
- 统一的安全保护服务
- 设施安全系统
- 事件安全性
- 针对高风险人员加强保护
- 保护关键人员和资产的运输
- 管理通过 Security@Dell.com 获悉的所有安全相关事务

为何关注全球安全运营？

9000 美元

计划外数据中心停机的每分钟成本

21%

每年，21% 的安全漏洞均为物理失窃和内部盗窃所致

逾 200 万

美国每年有超过 200 万次工作场所暴力事件

78%

的工作场所杀人事件为枪杀

组织安全

Dell Technologies 要确保我们的全球团队成员都能意识到，他们有责任遵守安全性和弹性实践和标准。为促使企业遵守这些实践和标准，我们信息安全部门的职能包括：

1. 提供战略以及策略/标准和法规的合规性、认知和教育、风险评估和管理、合同安全要求管理、应用程序和基础架构咨询、保证测试，推动公司向着安全方向发展。
2. 对安全解决方案进行安全测试、设计和实施，以在整个环境内采用安全控制。
3. 对已实施的安全解决方案、环境和资产进行安全运营，并管理事件响应。
4. 借助用于调查（包括 eDiscovery 和 eForensics）的安全运营、法律、数据保护和人力资源，进行法证调查。

信息透明，值得信赖

Dell Techologies 自身的数字转型之旅和我们为客户提供支持的转型之旅一样，都涵盖以下几个方面：业务转型、IT 转型、生产力转型和安全转型。对于我们业务流程中使用的各种系统和解决方案，我们都采用并遵循“固有安全性”原则；我们还调整了久经考验的框架和方法的应用方式，以确保契合我们的企业战略。除了重视安全控制措施（如互联网安全中心 (CIS) 和 SANS 研究所推荐的控制措施），我们还密切关注客户最关心的问题。下面是我们的客户最想了解的前 20 项控制措施。我们根据 NIST 网络安全框架 (CSF) 中定义的五个最高级别功能对这些控制措施进行了分组。

识别

资产管理

戴尔的工作是跟踪和管理物理和逻辑资产。Dell Technologies IT 部门可能跟踪的资产示例包括：

- 信息资产，例如已确定的数据库、灾难恢复计划、业务连续性计划、数据分类、归档信息。
- 软件资产，例如已确定的应用程序和系统软件。
- 物理资产，例如已确定的服务器、台式机/笔记本电脑、备份/归档磁带、打印机和通信设备。

Dell Technologies 非常重视对信息、软件和物理资产的识别、跟踪和管理。

Dell Technologies 拥有完善的资产管理计划，会将规则和活动传达给所有人员。所有资产都会落实，有指定的所有者，并会得到调配和监控，直到折旧和返还。

这些资产根据业务关键程度进行分类，以确定机密性、完整性和可用性要求。针对个人数据处理的行业指导为技术、组织和物理安全措施提供了框架。这些安全措施可能包括访问管理、加密、日志记录和监控以及数据销毁等控制措施。

公司资源使用策略适用于公司拥有的所有信息技术资源（无论位于什么位置），其中列出了多项要求，确保 Dell Technologies 员工清楚地了解该如何使用这些资产。

合规性

我们的安全性和弹性部门的策略、标准和控制措施组合与 NIST 和 ISO 框架保持一致。这些基本规则涵盖了数据的整个生命周期，囊括了我们的物理和网络环境，规定了每个团队成员都有责任为我们的安全文化做出贡献。信息安全、法律、隐私和合规部门会共同努力，确定所有适用的当地法律和法规。这些要求涵盖了方方面面，诸如：公司和我们客户的知识产权、软件许可证、员工和客户个人信息的保护、数据保护和数据处理过程、跨境数据传输、财务和运营流程、关于技术的出口管制条例和取证要求。

我们制定了多种机制来确保遵守这些要求，包括：信息安全计划、执行隐私委员会、执行风险指导委员会、全球风险与合规委员会、内部和外部审计/评估、内部和外部法律顾问咨询、内部控制评估、内部渗透测试和漏洞评估、合同管理、安全意识、安全咨询、策略例外审查和风险管理。此外，根据地理和业务需求，还制定了各种经过独立审核和认证的安全认证，包括 SOX、ISO 27001、SOC1、SOC2 和 PCI DSS。

我们的行为准则可以指导我们如何根据我们的文化和价值观，以及我们工作和服务所在国家/地区的所有适用法律的条文和精神在 Dell Technologies 开展日常活动。

风险管理

我们拥有成熟的风险管理计划，提供了适当的流程来识别、评估和处理与组织重要信息有关的风险。它消除了与这些资产相关的不确定性，可确保实现所需的业务成果。

我们的风险管理计划利用一个集成的控制和风险框架，重点关注与信息技术和信息安全相关的可用性、访问权限、准确性和敏捷性等关键业务需求。它提供了结构和行为准则，确保以主动、经济高效的方式持续评估和解决我们的信息技术和信息安全风险，包括人员、流程、数据和技术方面的风险。我们制订了管理行动计划/修正流程 (MAP) 来记录和管理风险，每个计划和流程都分配有风险负责人，由他们负责修正工作。

供应链

我们有一整套全面的方法来保护供应链，并提供客户可以信赖的解决方案。我们的“深度防御”和“广度防御”战略包含多个控制层，以减轻可能引入供应链的风险。这些控制措施有助于建立供应链保障，让大家相信整个供应链和产品生命周期中使用的一系列流程和控制措施可以排除非预期因素，实现产品、流程和信息的生产和交付，并且它们能按照设计和预期发挥功能。

我们的供应链风险管理框架与美国基础架构保护计划 (NIPP) 的全面风险管理框架相似，体现了政府和私营部门如何共同努力降低风险并实现安全目标。我们的框架包含一个开放的反馈流程，有助于持续改进。风险缓解计划在整个解决方案生命周期中将处于优先地位，并视具体情况实施。

供应商治理对于保障供应链的绩效和完整性至关重要，因此，在吸纳潜在供应商和合作伙伴前，我们会先开启供应商治理，即对他们进行彻底审查。确定合作关系之前要进行分析，可能包括初步的现场调研和制造资格评估，此外还需完成特定产品的信息征求 (RFI) 或报价 (RFQ)。我们具有独特的优势，因为 Dell Technologies 产品组合打造了卓越、值得信赖且受人尊敬的品牌，我们可以从中汲取见解、最佳实践、技术和专业知识。我们认为，必须倾听客户、供应商和合作伙伴的意见并与之合作，才能不断改进 Dell Technologies 提供供应链保障的方式。

保护

访问管理

要保护戴尔网络和系统就必须审视数字身份的生命周期及其对戴尔资源的访问，这是一个关键因素。数字转型已经快速走出传统数据中心，走入云端，这也使得勒索软件攻击愈演愈烈，数据丢失风险越发高涨。我们的身份和访问管理策略采用自动化的方式并根据风险确定优先级，有助于改善安全态势并确保监管合规性和顺畅运营。

严格的身份管理、“最低权限”用户访问和多重身份验证有助于应对与混合、多云和边缘环境相关的风险。对于员工和承包商的入职/加入、调动和离职/解约，戴尔所采用的方法都会进行适当的管理。强大的实时分析和报告功能可进一步为运营提供协助，并保障团队能够提供现代化的用户体验，同时确保数字身份（人员、设备和应用程序）能够“在适当的时间以适当权限访问适当的资源”。

数据治理

我们拥有成熟的企业信息治理框架，对硬拷贝和电子数据与信息的生命周期存在要求。它涵盖正常业务过程中使用的所有信息（无论何种格式或媒体）的创建、接收、管理、处理、存储和处置。根据信息安全和隐私准则，我们会对得到批准的存储库/存储位置中的所有应用程序/数据库和文档进行识别、分类保护、保留和处置。

- 信息资产的识别和清点要视其位置和在整个生命周期中的移动情况而定。
- 结构化和非结构化数据会根据采用的数据类别（公开、内部使用、受限和严格受限）进行分类。如果信息分属多个类别，则使用限制性最高的分类标签。资产分类要视业务关键性而定，以确定机密性要求。
- 根据数据的价值、使用情况和用途，每个数据分类类别都会设有保护要求，从创建时到生命周期结束，贯穿始终。针对个人数据处理的行业指导为技术、组织和物理安全措施提供了框架。
- 信息将根据法律或法规要求的保留期要求来保留，分为依法保留和根据运营业务需求保留。
- 到达要求的保留期后，会以安全的方式对信息进行处置。

戴尔人才招聘

我们实施的控制措施包括对所有职位候选人进行背景调查和能力调查，确保我们的员工和承包商都了解自己的责任，并适合他们要入职的岗位。我们会根据相关法律、法规和道德规范执行这些调查，且调查力度视业务需求、要访问的信息的分类以及感知到的相关风险而定。

在招聘流程中，我们所有的员工和分包商都必须签署保密协议，并根据当地法律接受相关的筛选流程。

加密

我们的加密策略符合行业最佳实践。此外，我们策略所依附的标准和控制措施也在不断变化，并始终与利益相关者要求的业务和法律要求保持一致。

我们会根据组织规定的秘钥生成、分发、存储、访问和销毁要求，为信息系统内使用的加密方式建立和管理加密秘钥。对于特定分类的数据，我们会根据所采用的相关策略和标准执行加密。我们的无线网络使用出色的行业标准加密方法来提供保护。

我们的加密流程和系统为静态数据、使用中的数据和动态数据提供服务，这些数据遍及基础架构、数据库和应用程序。此外，我们强大的加密密钥管理流程可确保密钥、证书和数字签名在其生命周期内得到保护，包括秘钥的生成、分发、存储、备份、轮换、过期、存档和销毁。

网络管理

Dell Technologies 实施必要的网络保护措施，例如采用技术和管理控制措施来管理网络和支持性基础架构的安全性。

我们的控制措施符合 NIST 和 CIS 的要求，可保护和强化网络设备。网络管理提供互联网连接、本地网络连接、对资源的远程访问和网络设计标准，这些设计为保护提供给用户的网络服务奠定了基础。通过我们依照行业最佳实践实施的管理、物理和技术控制，我们可确保建立一个基于多层保护的安全环境，不同的保护措施相互支持、互为补充，以提高整体安全性。

密码管理

Dell Technologies 认识到，我们的用户必须恪尽职守，使用不易猜到或推断的密码保护其用户帐户，才能访问我们的系统。密码是计算机安全的一个重要方面，是用户帐户的第一道防线。密码选择不当可能会导致整个公司网络受到威胁，因此所有有权访问系统的员工、承包商和第三方都有责任采取适当的步骤来选择和保护他们的密码，并通过双因素身份验证来访问我们的内部网络。

我们制定了符合行业标准的密码策略和标准，确保所有用户都维护安全做法，且支持受保护的信息基础架构战略。这些策略和标准包括创建强密码、保护密码以及更改频率等。此外，我们还利用日志记录、监控、自动化和警报系统来实施密码策略并提供额外的安全保护。

修补程序管理

我们实施着一项全局修补程序管理计划，该计划遵循行业标准并满足法规和合规性要求。我们的修补程序管理流程符合安全最佳实践，并包括：

- 维护有关可用修补程序的新知识。
- 列出需要使用自动监控工具修补的所有资产清单。
- 确定哪些修补程序适合特定系统，以确保经过相应测试。
- 按变更控制管理计划进行安装。
- 查看修补流程和结果，并记录所有相关过程，例如所需的特定配置、标准和紧急修补过程。

我们的应用程序以及新旧系统都会得到维护，达到最新的安全修补程序级别。

物理安全性

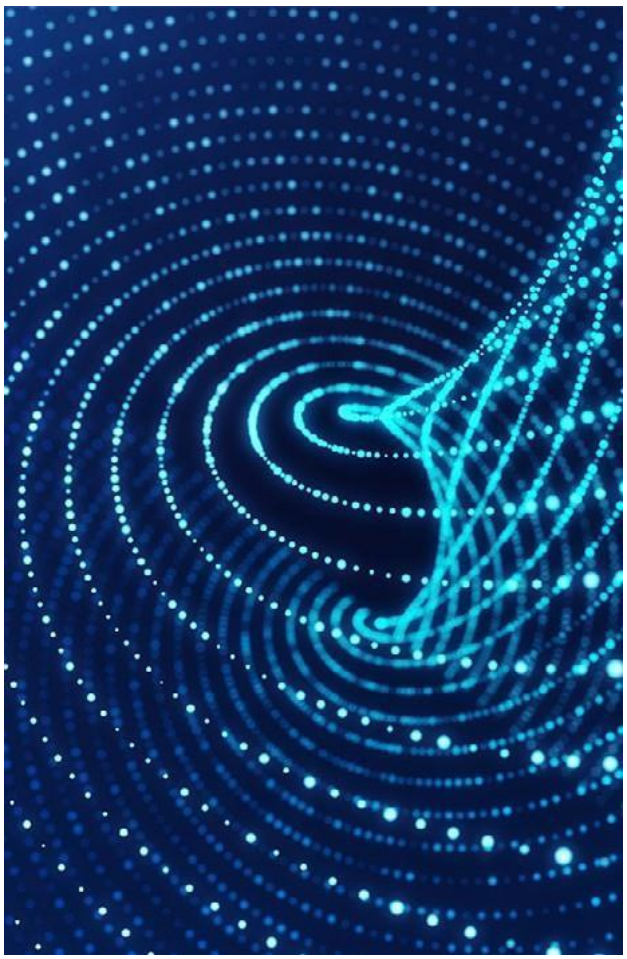
计算设备是我们的宝贵资产之一，必须加以保护。仅限授权人员的物理访问限制以及可靠的环境控制，可在各种威胁之下保护我们的数据和计算环境的机密性、完整性和可用性，从而确保业务连续性、尽可能减少业务影响并更大限度地提高投资回报、增加业务机会。

我们的物理安全计划遵循行业安全最佳实践和法规要求，可确保通过安全入口控制进入我们运营场所的人员，防止未经授权进入运营场所并对信息进行访问、损坏和干扰。对于包含关键或敏感信息的场所，进出都会受到控制，仅限具有业务需求的授权人员进入，而且会对这些人员进行定期审查，确保只有适当的人员可以进入。

安全的开发生命周期

我们的系统开发生命周期稳定而可靠，可对必须采取的各个步骤进行控制，确保分发给客户（内部和外部）的所有硬件、软件和固件均已在正式治理计划的控制下根据开发生命周期的定义进行适当设计、开发和封装。

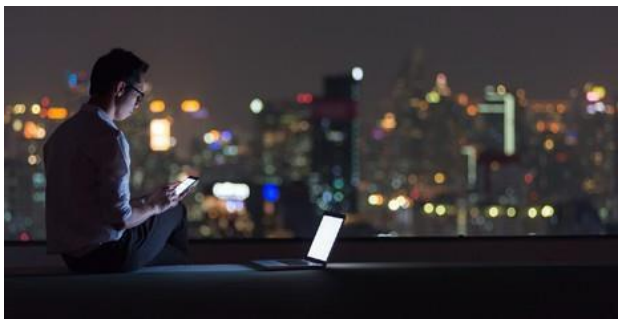
我们力求将安全性贯穿于产品或应用程序的整个生命周期，确保每一款产品和应用程序都能安全开发并且始终安全。戴尔安全计划中包括威胁建模、静态代码分析和安全测试等多项分析活动，旨在发现并解决整个开发生命周期中的安全缺陷。



戴尔的安全开发生命周期计划符合 ISO/IEC 27034“信息技术、安全技术、应用安全”中规定的原则。Dell Technologies 还与 SAFECode、BSIMM 和 IEEE Center for Secure Design 等多家行业标准组织合作，确保遵守行业惯例。

此外，许多 Dell Technologies 员工还积极参加各类专注于制定安全标准和定义业界安全做法的组织，其中包括：

- 云安全联盟 (CSA)
- 分布式管理任务组 (DMTF)
- 事件响应论坛 (FIRST)
- 信息技术标准国际委员会 (INCITS)
- 国际标准化组织 (ISO)
- 互联网工程任务组 (IETF)
- 国际开放标准组织 (The Open Group)
- 结构化信息标准促进组织 (OASIS)
- 卓越代码软件保障论坛 (SAFECode)
- 存储网络行业联盟 (SNIA)



我们会定期审查公开发布的第三方漏洞，以确定它们在我们环境中的影响和适用性。根据它们带给业务和客户的风险，我们安排了预先确定的修复时间表。此外，我们通过基于风险的主动式方法，定期对应用程序和基础架构进行漏洞扫描和评估。在开发过程中以及在发布到生产环境之前，我们还会使用安全代码审查和漏洞扫描程序，主动检测编码漏洞或风险。

检测

防范恶意软件

我们实施了多种检测、预防和恢复方面的控制措施，并结合适当的意识培养计划，以保护环境免受任何恶意软件和病毒的侵害。

我们采用集中管理的多级防病毒和端点检测与响应 (EDR) 保护模型，包括来自三家一流供应商的三级网关保护。我们有一套经过定义的标准解决方案，所有相关设备都会安装。这些设备必须保持运行状态，并遵守通过管理策略服务器和流程提供的配置设置（如适合操作系统）。此外，我们的防恶意软件程序要求扫描所有入站和出站邮件以查找垃圾邮件、病毒、DLP 策略、附件保护、网络钓鱼和批量电子邮件。

变更管理

我们实施了行业最佳实践变更管理流程，以确保生产线资产稳定、可控且受到保护。

我们的变更管理流程可确保以可控的方式管理对 IT 资源的更改，从而尽可能减少业务中断。变更管理提供了管理这些变更所需的要求、指导和工具，以确保这些变更经过适当的审查、批准并有效地传达给用户。

下面列出了部分优势：

- 尽量降低必要变更的操作风险
- 尽量提高已实施变更的有效性
- 便于对环境中的所有变更集中排列优先级和进行调度
- 通过清晰的文档和明确定义的流程简化未来变更
- 为所有类型的环境变更提供一致、可预测的服务级别
- 提高处理大量变更的能力
- 通过中央调度程序防止变更冲突

日志记录和警报

我们建立并维护了一个日志记录和警报管理计划，它遵循行业标准、法规和合规性要求，用于记录事件并跟踪授权和未经授权的活动以及对系统、应用程序和数据的访问。

我们的日志记录和警报计划可确保根据业务分类和关键性来捕获、跟踪和管理系统、应用程序、平台和网络设备的安全事件，并发出通知。通过该计划，我们实施了控制措施来实现日志及其保留的标准化，以保护日志免受未经授权的更改。此外，日志中捕获的详细信息还规范了格式，有助于按类型、位置、主题、用户、日期时间戳甚至访问的数据进行事件管理以及识别。

最后，我们使用实时监控方法来监控，并在有可疑活动或发生审核日志错误时生成警报，甚至触发已知事件的自动修复。

漏洞管理

为了实现企业的业务目标并确保有效保护我们的环境和运营，我们制定了全球安全修补和漏洞管理策略。我们采取了许多控制措施，以确保我们的环境得到精心管理，能够有效抵御内部和外部威胁。我们按照行业标准保护数据、应用程序、基础架构、客户数据的完整性、可用性和机密性。

根据漏洞管理战略，我们从可信赖的资源收集网络威胁信息，并与主要供应商结成联盟。我们会扫描资产和系统以查明是否存在漏洞。我们还会根据我们的策略、优先事项和潜在风险影响执行修补和修正。

响应

业务连续性

Dell Tchnologies 快节奏的全球业务需要灵活的方法来实现运营弹性，这样我们才能积极应对风险，尽可能缩短停机时间，并提供适应性强的基础架构以实现增长，同时保护客户、员工、业务合作伙伴和利益相关者的利益。我们整合了全球业务连续性计划，该计划定义了运营弹性标准的框架，可协助 Dell Tchnologies 业务部门规划和降低风险，以确保我们在瞬息万变的世界中满足客户的需求。

企业弹性计划的设计以风险为基础，符合公认的国际行业标准，包括 ISO 22301。业务部门会根据该计划来指定在丢失关键功能依赖项时使用的替代和恢复程序。这种做法能够使公司在不影响服务级别、恢复点目标 (RPO) 和/或恢复时间目标 (RTO) 的情况下，根据与客户的协议持续提供服务。我们还使用业务影响分析 (BIA) 定义关键功能。

安全实践

戴尔计划的总体指导由全球业务连续性办公室 (GBCO) 提供，并由经过认证的业务连续性实践主题专家领导。GBCO 能够在如何避免业务中断、做好相关准备以及从中恢复方面为企业提供指导，还能提供与一级供应商相匹配的一流业务连续性计划。业务部门会根据该计划来指定在丢失关键功能依赖项时使用的替代和恢复程序，使公司能够在不影响服务级别、恢复点目标 (RPO) 和/或恢复时间目标 (RTO) 的情况下，根据与客户的协议持续提供服务。我们还使用业务影响分析定义关键功能。

戴尔的业务连续性规划流程包括一项公司策略，该策略表明了对全球业务运营方法的承诺，并得到了高级管理层的支持。业务连续性计划涉及关键方案规划，包括连续性和从以下损失中恢复：

- 人力资本和主题专业知识
- 关键基础架构
- 设施
- 包括重要文档、IP、关键数据在内的资产
- IT 应用程序和基础架构
- 内部和外部的关键依赖项
- 供应商托管的服务和第三方服务

Dell Technologies 要求所有关键业务部门每年都更新和测试其业务连续性计划。

沟通

我们制定了沟通计划，确保关键决策者和主题专家能够在业务中断的威胁下进行协作。沟通计划包括在公司面临业务中断的威胁时联系可能会受此影响的客户。

风险评估

我们每年进行风险评估，以找出最有可能影响业务运营的自然和人为事件并做好准备。

供应商/第三方

Dell Technologies 策略要求对供应商执行业务弹性标准，办法是评估供应商能力、定期监控合规性、安排备选供应商以及制定处理假冒、被盗或非法物品的计划。

监管合规性和相关计划

Dell Technologies 建立了必要的程序和策略，来确保对适用的产品和运营相关法律法规的合规性，例如工作场所安全、产品安全、环境保护、劳工标准、建筑规范和进出口合规性。此外，关键营运场所和/或业务流程已通过相关标准的认证（自愿获得），包括 ISO 9001，ISO 14001，OHSAS 18001，ISO 20000 等。戴尔的程序和流程会根据需要进行调整，以反映内部运营和外部因素的变化（例如气候变化、人口增长以及能源和水的获取）。

安全

我们实施了物理安全控制措施和程序，用于监视、阻止、检测以及保护关键资产，支持 Dell Technologies 服务的部署，从而避免物理威胁。这些程序与评估的风险和资产价值相对应，并且我们会定期检查其有效性。我们建立了相关的数据安全控制措施，包括访问控制、加密和信息分类，以保护 Dell Technologies 和客户数据。此外，我们还制定了一项计划，以确保员工的安全，并减轻因不可预见的员工减少而可能造成的停工所带来的影响。

持续而不间断的改进

Dell Technologies 要求管理层至少每年审查和批准一次连续性和恢复策略。公司策略要求 Dell Technologies 业务部门分析运营流程的风险和单点故障，并实施策略以填补任何不可接受的缺口。

如果您对 Dell Tchnologies 的业务连续性计划有其他疑问，请联系您的 Dell Tchnologies 客户代表。

事件管理

网络安全事件响应计划的主要目标是减轻和控制与计算机安全事件相关的风险。

保护我们的声誉和合作关系对公司至关重要。有效的端到端网络安全计划可以帮助保护公司的信息和资产，在建立这种保护方面发挥着关键作用。我们的网络安全事件响应计划是这类安全计划的重要组成部分，旨在概述我们如何识别、评估、响应和补救网络安全事件。该计划还定义了参与我们应对网络安全事件的各个利益相关者的角色和责任。

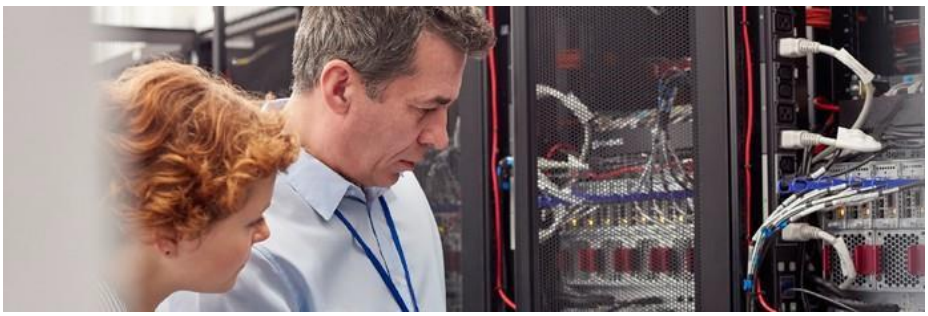
我们制定了公司网络安全事件响应计划，概述了安全事件的目的、范围、识别、评估、响应和补救措施，包括根据需要向监管机构、控制方和/或数据当事人发出通知。

恢复

灾难恢复

我们认识到，在充满不确定性和挑战的全球环境中运营，采取一致、可扩展、灵活和协调的方法来实现弹性十分重要。

如果某个事件会严重影响我们的正常营业，我们的灾难恢复计划将及时恢复支持我们关键运营的业务关键型流程、应用程序、数据和系统。



灾难恢复计划会建立标准、流程和控制措施，以便及时恢复用于管理和支持业务功能的关键业务数据、应用程序、系统和基础架构。这些要求确保了支持关键业务部门的资源的连续性。

我们的计划和方法可确保为客户服务的应用程序和基础架构具有恢复能力，且符合合同规定的服务级别协议、RTO 和 RPO。我们已经预先建立了指定的恢复站点并准备好了 IT 灾难恢复人员，能够在发生业务中断时快速调动。此外，当新应用程序联机或 IT 环境发生变化时，我们会修订和测试灾难恢复计划，如无变化，则每年至少修订和测试一次。测试方法与应用程序/系统的关键程度相对应。