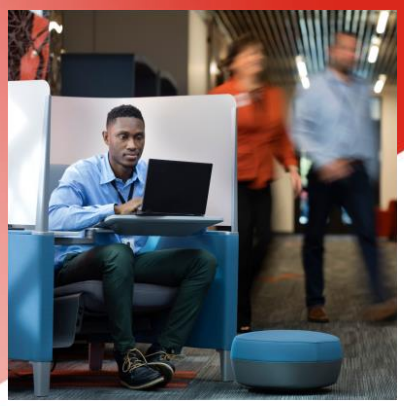
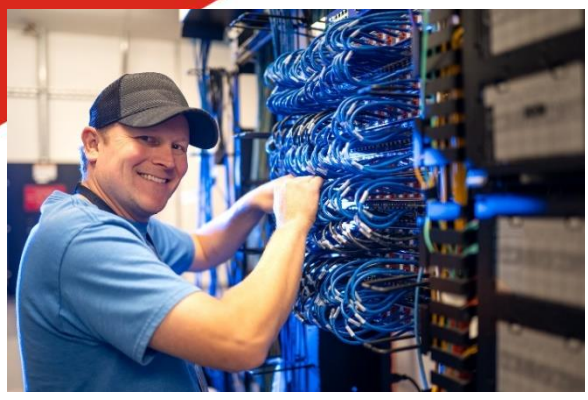
W. L. GORE & ASSOCIATES

使用限制政策

戈尔合作伙伴





引言

戈尔资产为我们提供了与客户、合作伙伴和彼此开展业务的能力。在戈尔，我们相信同事和合作伙伴将负有责任感的开展业务，并以谨慎的方式保护我们的资产。本 "可接受使用政策 "和我们对满足其要求的承诺对于我们作为企业取得成功至关重要。

目的

本《使用限制政策》（以下简称 "政策"）旨在规定访问或使用 W. L. 戈尔公司（以下简称 "戈尔 "或 "公司"）资产的 戈尔合作伙伴 的责任 。本政策旨在保护戈尔的信息资源，并指导戈尔合作伙伴适当使用这些资源。

本政策将取代先前的 "使用限制政策"。 戈尔合作伙伴 应在本政策上签字，以确认他们已阅读、理解并同意遵守本文件中规定的内容。

范围

本政策适用于使用戈尔资产的所有 戈尔合作伙伴 。

所有使用戈尔信息资源或访问戈尔信息的行为，无论是使用公司配发的硬件、个人拥有的受管设备还是个人拥有的非受管设备（须经批准），均须遵守本政策。

本政策中未尽事宜并不一定构成相应的许可。如果您对本政策未涵盖的方面或潜在冲突有任何疑问，请联系您的联系人或信息技术援助中心 (ITAC)。

定义

与本政策相关的定义概述如下。请参阅企业信息技术术语表(Enterprise IT Glossary)，了解更多定义。

人工智能（AI）工具 - 任何利用人工智能算法执行特定任务和解决问题的软件应用程序。AI 工具包括但不限于：

- *机器学习工具（ML）*——分析数据以确定模型并做出预测，帮助戈尔完成需求预测、客户细分和欺诈检测等任务。
- *自然语言处理工具（NLP）*——处理和分析人类语言，从而优化聊天机器人、情感分析和自动客户支持等应用程序。
- *计算机视觉工具*——允许计算机解读视觉数据并据此做出决策，可用于质量控制、面部识别和自动检查等领域。
- *机器人流程自动化工具（RPA）*——自动执行重复性任务，例如数据录入和发票处理。
- *预测分析工具*——使用统计算法和机器学习技术，根据历史数据预测未来结果，从而辅助决策过程。
- *大语言模型（LLM）等生成式人工智能*——根据输入数据生成文本、图像或代码等内容，可用于内容创作、营销等方面。
- 具有*检索增强生成（RAG）*技术的应用程序——使用个人数据生成内容，而这些数据并非源于 AI 模型本身，而是来自输入内容，例如同事曾输入的交互信息或咨询过的其他数据源。
- *翻译管理系统（TMS）*——利用自动化技术，并可能结合一些 AI 元素，以此增强翻译工作流程，例如检查之前的翻译记录，并将新内容融入原始文档布局。

资产 - 支持戈尔业务运营且由戈尔拥有、许可、使用或运营的任何硬件、软件（由戈尔发放或管理）或戈尔环境内的其他组成部分。

- *硬件*包括但不限于计算机、笔记本电脑、平板电脑、计算机硬盘、网络硬件、闪存盘和其他存储设备、工作站、电话、移动设备、视频会议设备、打印机、扫描仪，和/或任何其他支持业务运营的物理技术设备。
- *软件*包括但不限于操作系统、网络软件、信息应用程序（如电子邮件、语音邮

件）、协作工具、文字处理工具、电子表格及其他数据应用、数据库、网络应用程序和/或任何其他程序、应用或软件平台。

内容 – 基于运营、法律或监管需求对企业具有价值的数据、信息或记录。

数据 – 以象征性方式表示某些事物的内容，而这些事物的含义在一定程度上取决于元数据。数据是一系列客观存在（如数字、文字、测量值、观察结果或对事物的描述）的集合。

数据保护专员 – 欧洲的《通用数据保护条例》(GDPR) 确立了“数据保护专员”(DPO) 这一概念。DPO 致力于确保遵守所有相关的数据保护法律、监控特定流程并与相应的监管机构合作。

戈尔电子邮件账户 – 与戈尔域名关联的用户账户（包括其他所需的软件、存储和硬件），让您能够收发邮件。

信息 – 具有短期业务价值的内容。信息是指特定背景下的数据。

互联网访问 – 所有能够实现电子通信（尤其是从互联网检索数据）的资源，包括相关的硬件和软件。

内联网 – 由戈尔提供、允许在戈尔内部网络上进行电子通信的所有资源，包括相关的硬件和软件。

记录 – 作为商业行为、决策或交易证据的内容。记录是任何形式（纸质或电子）的完整且最终确定的信息，必须根据法律、监管或运营要求在规定的时间期限内予以保留。

受管设备 – 用于访问戈尔内容或戈尔网络的个人移动设备，其中已安装并激活戈尔设备管理软件。

- 请参阅《移动设备使用指南》(Mobile Device Use Guidelines)

合作伙伴 – 承包商、第三方等。

戈尔资产的使用

戈尔业务必须通过经批准的应用程序或受管设备来进行。未遵守这一规定可能会导致戈尔内容面临维护不当和安全性降低的风险。

每个戈尔合作伙伴都有责任 保证戈尔内容的安全，除非是经授权的有关连人士或合作伙伴，否则不允许访问任何资产 。

访问权限

戈尔合作伙伴只能使用获准访问的资产。

戈尔合作伙伴在访问或被授权访问戈尔资产时应采取以下步骤：

- 戈尔合作伙伴应根据 ″需要了解 ″原则访问或授权访问戈尔资产。
- 戈尔合作伙伴应仅在必要时被授予戈尔资产访问权限，并在业务要求得到满足或承诺发生变化时撤销访问权限。
- 必要时，戈尔合作伙伴必须通过适当渠道（应用程序所有者、信息安全等）申请访问权限。
- 仅允许通过戈尔授权的方法和设备远程访问戈尔网络。

处理

戈尔合作伙伴应遵守安全分类政策和记录与信息管理政策中规定的准则，以安全的方式管理戈尔资产。

禁止的用途

戈尔合作伙伴不得

- 以非法或恶意的方式使用戈尔资产，尤其是如果此类使用可能损害戈尔的声誉或导致公司承担责任或财务损失的情况下。

- 访问、下载、展示或传播可能被视为淫秽、种族主义、性别歧视、威胁、冒犯、歧视或辱骂性质的资料。
- 使用威胁性、骚扰性或辱骂性的语言或内容。
- 展示被认为不适合工作场所的内容。
- 试图规避信息安全部门或戈尔物理安全团队设置的任何安全机制。
- 使用其他同事或合作伙伴的登录凭据。
- 使用非受管个人设备连接至戈尔网络。
- 在戈尔设施内设置未经授权的无线网络并将其连接到戈尔网络，或访问戈尔设施内未经授权的无线网络。
- 安装或改动现有资产，或参与故意损害戈尔资产或导致戈尔资产发生故障或失灵的活动。
- 篡改或禁用戈尔的防病毒软件或加密功能。
- 在戈尔资产上安装个人或非标准软件（智能手机或平板电脑上的个人应用程序除外）。

- 在个人拥有的设备（电脑、手机、云存储等）上存储戈尔数据或信息，除非该设备已安装戈尔软件来管理存储在该设备上的信息（请参阅《自带设备用户协议》），或 存储在未经戈尔信息安全评估的云或网络中。

监控

除非法律禁止，为确保遵守戈尔的政策和标准，戈尔保留可能在未事先通知的情况下采取相关行动的权利，包括查看、拦截、阻止或以其他方式调查（“监控”）任何同事或合作伙伴对戈尔资产的任何使用情况或记录相关活动日志。

在监控过程中，戈尔将尽一切合理方式遵守特定国家/地区的法律，确保将个人信息（“PI”）仅用于明确和特定的目的。

在可能的情况下，监控会以自动化方式进行。监控过程会捕获特定信息。有关在特定情况下为了特定目的而可能收集的信息类型，请参见随附的附录 B。

为遵守法规，或保护戈尔的品牌声誉和公司的竞争优势，在当地法律允许的情况下，戈尔可能会监控某些敏感信息（如出口管制信息、个人信息或戈尔机密技术等）。

在监控方面可能还要遵守其他地区程序或当地法律。 关于如何对同事进行监控的更多信息，请参见随附的附录 A。

在适用法律允许的范围内， 如果戈尔有理由认为戈尔合作伙伴违反了本政策或其他相关政策，戈尔可能会尝试识别该合作伙伴。经与相关数据保护官协商后，戈尔公司可进行有针对性的监控。

如果戈尔通过监控怀疑存在违反本政策的行为：

- 戈尔公司保留取消戈尔合作伙伴访问戈尔资产的权利 。戈尔公司还将酌情删除或阻止访问个人设备上的任何公司信息（请参阅《自带设备用户协议》）。
- 在遵守适用法律的前提下，戈尔公司可储存通过监控活动获取的任何内容副本，这些内容反映了戈尔合作伙伴对戈尔资产的不当使用 。如有必要，戈尔公司还可在诉讼或调查中披露此类内容副本或包含此类内容的设备。

个人设备

戈尔可能允许戈尔合伙伙伴使用个人拥有的设备（如智能手机或平板电脑）开展与戈尔有关的业务。在这种情况下

- 戈尔合作伙伴必须通过 ITAC 申请程序签署用户协议，并允许戈尔 IT 部门安装移动设备管理软件。移动设备管理软件允许

戈尔 IT 部门控制设备上的戈尔内容和应用程序，或
- 在有限的情况下，可根据下文概述的例外程序批准访问。

电子通讯

除非当地法律或法规另有规定，否则戈尔电子邮件系统和其他消息服务（如 Teams 或其他戈尔管理的即时通讯(IM) 工具）以及这些工具中的所有相关信息均明确属于戈尔的财产。戈尔电子邮件和即时通讯账户仅用于公司业务。在所有电子通讯中，我们都需要根据《安全分类标准》确保敏感信息和个人信息的机密性（一般通过使用加密技术）。

即时通讯应用程序

戈尔认识到通过即时通讯应用程序进行内部和外部沟通的必要性。只要有可能，我们强烈鼓励使用由戈尔提供和维护并在戈尔认可的设备上使用的应用程序、平台或工具。

如果必须通过 WhatsApp 等外部即时通讯应用程序进行沟通，切勿传输机密或敏感信息，包括个人信息或知识产权。

通讯内容应当以联系沟通性质为主。切勿将戈尔业务记录存储在任何即时通讯或消息传递应用程序中。所有业务记录（如批准和交易支持文件）必须根据既定的业务流程进行维护。

录制

戈尔合作伙伴可以使用工具（微软团队或其他设备/软件）记录或转录会议和互动。戈尔合作伙伴必须在会议开始前（最好在会议邀请函中）告知与会者将进行录音/转录，并允许他们选择退出。如果会议正在进行中，Microsoft Teams 会显示会议正在录制，任何与会者都可以在此时选择退出，即使他们很晚才加入。

对于混合会议和自动录音会议，主持人应在会议邀请或会议聊天中告知所有与会者将使用录音。在休息或非业务讨论期间，录制必须暂停。

涉及敏感个人信息或主题的会议不应被记录。例如病人数据、贡献/报酬。

戈尔 AI 工具

我们鼓励戈尔合作伙伴利用戈尔提供的人工智能工具提高工作效率、简化工作流程并支持决策过程。在将公司或个人数据输入人工智能工具时，戈尔合作伙伴必须确保数据的准确性和相关性，并遵守数据隐私和安全协议。戈尔合作伙伴不得上传或共享非戈尔提供的人工智能工具中的任何机密、敏感、专有或受法规保护的数据，除非领导明确授权并经信息安全部门评估。此外，戈尔合作伙伴应了解人工智能生成的结果有时可能会误导或不正确。因此，在根据人工智能输出结果做出决策或采取行动之前，必须验证其准确性和可靠性。戈尔合伙伙伴对人工智能工具产生的结果负责，并应准备好解释和说明这些结果。严禁滥用人工智能工具，例如生成误导性信息、侵犯知识产权或在没有适当监督的情况下自动执行任务，违者将受到纪律处分，最高包括解雇。

合规与报告

- 戈尔合作伙伴应完成与本政策相关的任何培训，包括强制性隐私和信息安全培训。
- 戈尔合作伙伴如发现任何实际或可疑的安全事件或未经授权使用或访问戈尔资产，必须立即通知 ITAC。
- 根据适用法律，违反该政策可能会导致面临纪律处分，情节严重者包括终止雇佣关系和/或在必要时采取法律行动。

附录 A - 地区差异

第 1 节	意大利地区适用的监控信息	阐明与意大利同事相关的附加条款。

第 1 部分 - 意大利地区适用的监控信息

本政策中描述的监控活动仅由戈尔在意大利雇佣法和隐私法的限制范围内并按照其规定的方式执行。

首先，根据 1970 年 5 月 20 日颁布的第 300 号法律第 4 条第 1 款，戈尔不得以监控同事在工作场所的活动为目的而开展任何此类活动，除非是为了遵守意大利数据保护法的要求。

不过，戈尔安装了可能触发远程监控同事活动的间接可能性的安全工具。
此类安装是为了有效保障戈尔组织及其资产的安全。如上所述，它旨在识别并解决对戈尔的组织和资产构成风险的安全、敏感数据泄露、欺诈检测、适用法律的合规性以及数据滥用等方面的问题。

戈尔公司尽可能以自动和/或随机方式进行监控。然而，如果戈尔有理由相信戈尔合作伙伴 实施了不当行为，且此类不当行为可能危及戈尔的组织、安全或资产，戈尔可能会尝试识别 该戈尔合作伙伴。

附录 B - 监控戈尔合作伙伴使用戈尔资产所形成信息的类型、情形和目的。

第 1 节：监控过程中可能捕获和记录的信息

网络活动，包括：

- 日期/时间
- 用户 ID、设备 ID、工作站 ID、IP 地址和其他唯一标识符
- 数据流的物理和逻辑路径，包括起点和终点
- 数据量
- 操作
- 关键词（如“机密”、“仅供内部使用”等）。

互联网活动，包括：

- 日期/时间
- 用户 ID
- 原始 IP 地址
- 目标地址（允许情况下）
- 传输的数据量

接收和发送的电子邮件：

- 日期/时间
- 发件人和收件人地址
- 消息 ID
- 邮件大小
- 主题
- 敏感数据关键词（如“机密”和“仅供内部使用”等）
- 仅适用于触发“标记内容”的电子邮件：电子邮件正文和附件。

数据丢失预防工具搜索数据中的关键词（如“患者 ID”）和模式，以检测敏感数据（如客户、医疗保健患者或戈尔敏感数据）的潜在泄漏。这些工具监控来自笔记本电脑、台式机和云使用情况的外送邮件和外发流量（发往网络、云、USB/CD/DVD、打印机和网络驱动器的流量），并对指定项目进行标记。

处理后的数据（可能包含唯一的用户、设备和/或位置标识符）仅用于以下目的：

- 技术错误的分析和纠正。
- 确保系统安全；包括维护被阻止的互联网页面列表（“阻止列表”）。
- 网络的优化和访问控制。
- 数据保护控制。

第 2 节：监控的具体示例及其目的：

- 保护戈尔的信息资产免遭未经授权的披露、删除或篡改。
- 按照法律规定和戈尔政策，遵守调查和执行要求。

- 保护其系统和网络免遭病毒、木马和其他恶意软件的侵害。
- 保护其系统和网络免遭未经授权的访问和/或未经授权的操纵。
- 保障戈尔及其他各方的合法权利和安全；以及
- 依照法律、法规、法院命令的要求，或有关当局或执法机构的规定。