

7. **图片和录音录像。**未经公司明确同意，禁止员工使用由公司持有或拥有的电子和其他业务系统以外的任何设备对公司财产或公司开展业务的办公场所拍摄图片、视频或其他录音录像。该项禁止包括但不限于：

- 使用个人相机、手机或其他设备拍摄公司财产，无论照片是数码格式还是其他格式。
- 使用录音机、手机或其他设备记录谈话。
- 使用录像机、手机或其他设备拍摄视频。

公司有权检查、观看、收听和从员工处获取员工对公司财产或公司办公场所拍摄的，或公司有理由怀疑包含公司或与 Stryker 有业务来往的公司的保密或专有信息的所有图片、视频和其他录音录像。

8. **关于 Stryker 电子和其他业务系统政策的问题。**有关本政策的问题应向相应部门、附属公司或运营单位的总裁、人力资源主管、信息技术主管提出，或向 Stryker 法律总顾问或 Stryker 主管人力资源的副总裁提出。

9. **违反公司政策。**如有任何违反本政策的行为，员工应通知所在部门、分公司或运营单位的总裁、人力资源主管、信息技术主管、Stryker 法律总顾问或 Stryker 主管人力资源的副总裁。违反本政策可能导致包括（直至）解雇在内的处罚。

Joint Replacements

Trauma, Extremities & Deformities

Craniomaxillofacial

Spine

Biologics

Surgical Products

Neuro & ENT

Interventional Spine

Navigation

Endoscopy

Communications

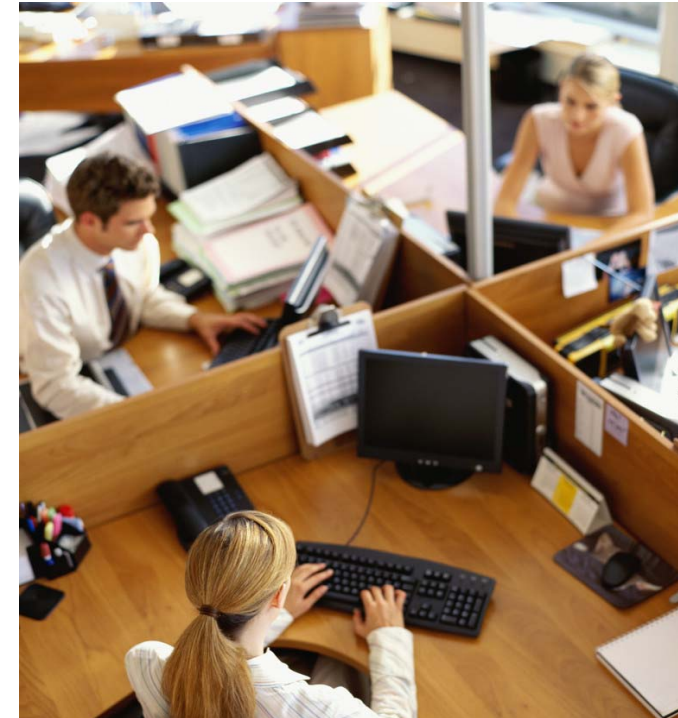
Imaging

Patient Care & Handling Equipment

EMS Equipment

电子和其他业务系统

第七号公司政策



**Copies of all Corporate Policies
may be found on
www.stryker.com/corporatepolicies**

2825 Airview Boulevard
Kalamazoo, MI 49002
t: 269 385 2600 f: 269 385 1062

目的：

阐述 Stryker Corporation 关于使用 Stryker 电子和其他业务系统的政策，包括但不限于笔记本电脑、台式和掌上电脑；电子邮件；语音邮件；电话；照片（数码照片和其他格式照片），个人数码助理；录像设备；因特网接入，无线和远程系统接入；音频、视频和网络会议；传真机；电子计时系统和相关的员工卡；以及 Stryker 向员工提供的其他电子或业务设备和服务（本文件中统称为“电子和其他业务系统”）。

范围：

该政策在适用法律允许的范围内适用于 Stryker 在各地的办公场所的每位员工。如果政策条款不符合适用于 Stryker 个别业务单位的当地法律，则该业务单位应修改政策，与可适用的当地法律保持一致或实施与当地法律相符合的单独政策，但是修改后的政策应在最大限度内与本政策的原则保持一致。本政策与当地法律一致的条款的效力不受影响。

详述：

1. **电子和其他业务系统属公司财产。** Stryker 拥有多种电子和其他业务系统。公司向员工提供这些系统，以协助其办理公司业务。所有此类系统和系统生成、处理或存储的文件、档案、备份、通信、图片和录音都是 Stryker 的财产，必须适当使用，妥善保护，不得有任何非故意的泄露和非经授权的查阅。
2. **公司查阅权限。** Stryker 有权随时并以公司认为恰当的任何理由，在通知或不通知员工的情况下，拦截、查阅、监控、检查、复制、修改或删除

Stryker 员工在电子和其他业务系统中生成或保存的任何材料。前述理由包括但不限于，开展公司业务、监测员工所提供服务的质​​量、确保对公司政策的遵守、确保员工个人信息控制的安全性，以及调查对不当或非法行为的指控。本条款中涵盖的材料包括但不限于电子邮件、语音邮件、图片、电话交谈、录像和电脑文件和文档。

3. **公司员工查阅电子邮件、语音邮件和电脑文件的权限。** 未经员工本人或其主管同意，任何其他员工不得查阅或试图查阅其他员工的电子通信、语音通讯或信息、或电脑文件。除非相关当地 IT 部门的书面政策明确许可，否则任何员工不得与他人分享其密码或登录许可证，或对该密码或许可证不采取任何保护措施，使非授权的人员可以接触到该密码或许可证。除非拥有业务授权，否则任何员工不得查阅、使用或篡改公司系统存有的保密信息或个人信息。
4. **语音邮件或谈话录音的披露。** 除非公司明确同意，否则任何员工不得披露公司电话系统、语音邮件或其他电子和业务系统记录的谈话内容。
5. **对保密的非公开信息的保护。** 使用电子和其他业务系统的员工，应尽审慎职责保护属于 Stryker 或由 Stryker 保管的敏感的员工个人信息和保密的非公开信息，以免其遭受未经授权的查阅、披露、破坏、丢失或更改。
6. **电子和其他业务系统的滥用。** 除了员工主管或所在部门的要求外，员工还不得以以下方式使用 Stryker 的电子和其他业务系统：

- 进行进攻性、骚扰、淫秽、诋毁或威胁性的通讯；
- 下载、传播、观看、公开、拍摄、打印或发送有关色情、淫秽、性、种族、宗教、种族或其他形式的骚扰性、进攻性或不适宜的材料；
- 未经相关 IT 部门许可，从互连网或其他外部渠道安装、下载、传播或发送任何类型的程序、文件或软件，包括但不限于连锁信、游戏或电脑病毒或蠕虫；
- 安装、下载、传播、拍摄或发送违反著作权法、商标法或专利法的材料；
- 未经相关 IT 部门或其主管许可，私自将公司电脑系统与家用/个人电脑系统相连接或使用家用/个人电脑或非 Stryker 电子邮件办理公司业务；
- 代表外部组织招揽生意或劝诱他人；
- 从事与 Stryker 业务无关的商业或盈利活动；
- 发送来自公司外部的可能破坏公司或公司商业伙伴声誉的媒体广告、互连网主页、电子布告栏通告、电子邮件、图片、语音邮件或其他公开陈述或信息；
- 实施未经公司授权或非公司发起的慈善举措；
- 未经 Stryker 事先授权，转移员工的个人信息或属于 Stryker 或与 Stryker 有业务来往的公司的非公开专有和/或保密信息；
- 未经公司事先授权，代表 Stryker 签订合同或协议；
- 将系统用于不合理的个人用途，或会扰乱或妨碍其本人或其他员工工作职能之用途；
- 出于非法目的或违反 Stryker 行为准则或公司政策使用业务系统。