

信息处理与分类指引

简介

本文档详细介绍了信息处理（包括根据信息分类进行处置），并为公司信息处理政策提供支持。

Trinseo 信息分类旨在帮助保密。分类表明了信息对 Trinseo 的价值及保护信息所需的控制措施。

Trinseo 信息分类是内部产生的信息的始发者，或依法取得的非 Trinseo 信息的首个 Trinseo 接收人的责任。首个 Trinseo 接收人是取得并有意使用信息的员工，可能并非打开邮件、电子文件、录像带等的人员。

当 Trinseo 信息不受限制地在外部共享（例如，发表在期刊、报纸等出版物上）时，该文档必须移除 Trinseo 分类标签。

注意：

在提到公司或法人实体的名称时，请勿将 TRINSEO 全部以大写字母表示。全部大写仅限 CALIBRE™ 聚碳酸酯等产品商标。

接下页

存储及使用 Trinseo 信息

要求

拥有 Trinseo 信息的个人，不论是信息的创建者还是受托者，都有责任以符合信息的保密程度及相应的信息分类的方式保护信息。不论是标记、书面、口头还是电子信息，这项要求都适用。

每个人都有责任存储 Trinseo 信息以便信息受到保护。不论是物理形式还是电子形式的信息，每个人都必须了解信息存储环境的安全程度。（例如，让您没有密码保护的电脑或 PDA 处于开启状态就像您把文件柜打开一样。）

具体的存储要求如下

Trinseo 受限

可以存储在实体办公室或工作区，无需其他特殊保护。

信息可以存储在 Trinseo 电脑、可移动存储介质或托管服务器上。

不支持的设备如用于同步 Trinseo 信息（如日历、任务和联系人），必须在最多 60 分钟不活动后自动启用密码保护。

Trinseo 保密— 未经许可不得共享

在 Trinseo 拥有和经营的设施中使用信息时，确保信息不被他人随意观察到。在其他设施（租用的办公场所、家庭办公室等）中，信息应由用户拥有并在使用时不被他人随意观察到。

在不使用时，确保信息放在上锁的房间或家具内。其中包括存储在 CD 等可移动存储介质或其他存储介质上的信息。不支持的设备不应用于同步电子邮件或存储任何类型的 Trinseo 敏感信息。这种同步可能造成许多技术问题，并产生 Trinseo 信息丢失的巨大风险。对分类为个人及保密的电子邮件和其他信息、Trinseo 保密、或律师—当事人特权 / 律师工作成果的访问只应通过完全支持的 Trinseo 设备和服务来完成，包括 Trinseo 工作站及 / 或 Trinseo 智能手机。

在以电子方式存储此类信息时，必须存储在实施适当的安全访问的托管服务器上。在法律允许的情况下，信息可以存储在加密的 Trinseo 工作站硬盘驱动器或可移动存储介质上。

Trinseo 保密— 从第三方来源获得

与 Trinseo 保密—未经许可不得共享相同

接下页

存储及使用 **Trinseo** 信息，接上页

律师—当事人特权	与 Trinseo 保密—未经 Trinseo 律师许可不得共享相同。参与的 Trinseo 律师应确定信息分发的对象和方式。
----------	---

律师工作成果	与 Trinseo 保密—未经 Trinseo 律师许可不得共享相同。参与的 Trinseo 律师应确定信息分发的对象和方式。
--------	---

个人及保密	与 Trinseo 保密—未经许可不得共享相同。
-------	--------------------------

接下页

分发或传递 Trinseo 信息

要求

Trinseo 信息必须以符合其分类等级的方式分发。分发或传输 Trinseo 信息存在两个相关问题。首先是确保接收人了解如何处理信息。其次是在信息传输及存储在接收人所在地期间妥善保护信息。

在分发 Trinseo 信息时，必须表明其分类。在许多情况下是通过在文档或信息中添加分类标签的方式来表明。在以口头方式提供 Trinseo 信息时，应事先以口头方式表明保密性，并随后提供一份书面提醒。唯一的例外情况是公共事务或法律部已批准发布的信息。

无论是在公司设施还是其他地方，在讨论 Trinseo 信息时，请注意您的周边环境。注意您身边可能听到谈话的人员。不同的传输方式提供不同程度的保护。分发方式的安全风险必须符合待传输信息的敏感性。

分发方式的示例包括：

电话、个人对个人、视频会议、语音邮件、邮件、电子公告板、内部会议、简报、电子邮件、传真、内部网 / 互联网、闭路电视等。

具体的分发或传输要求如下

Trinseo 受限

可以使用普通邮件和电子邮件（内部或外部）。

在公共场所讨论时，注意周围的人。

Trinseo 保密— 未经许可不得共 享

在传输之前验证信息接收人或系统的地址、电话或传真号码。

除通过法律允许的加密方式外，信息不得在 Trinseo 防火墙之外通过电子邮件或任何其他方法（如通过互联网）传输。

可移动存储介质或硬盘驱动器上传送或交付的信息必须加密。

此类信息不得携带在托运行李中。

在公共场所或设施讨论此类信息时，注意可能无意中听到谈话的人。在周围有人时不进行讨论。

接下页

分发或传递 **Trinseo** 信息，接上页

**Trinseo 保密—
从第三方来源获
得**

与 Trinseo 保密—未经许可不得共享相同

律师—当事人特权

与 Trinseo 保密—未经 Trinseo 律师许可不得共享相同。参与的 Trinseo 律师应确定信息分发的对象和方式

律师工作成果

与 Trinseo 保密—未经 Trinseo 律师许可不得共享相同。参与的 Trinseo 律师应确定信息分发的对象和方式

个人及保密

内部邮件应放在注明“个人—仅限收件人开启”或类似文字的信封中。提供回信地址。未经职能或工作流程负责人许可，不得进行电子传输。

除通过法律允许的加密方式外，不得在 Trinseo 之外通过电子邮件或任何其他方法传输。

接下页

处置 Trinseo 信息

要求	<p>不再需要保存的 Trinseo 信息必须根据 Trinseo 的记录管理政策妥善处置。Trinseo 信息的处置可使用粉碎或在垃圾填埋场监督填埋等手段。处置程序将取决于您所在的工作地点。</p> <p>以下是各种 Trinseo 信息分类的处置方法：</p>
Trinseo 受限—仅供内部使用	<p>采用防止进一步分发的实用处置方法。如果您不确定您当地的处置办法，将文件撕成四份或八份并扔入 Trinseo 的废纸篓中即可。</p> <p>电脑或可移动存储介质：覆盖整个介质，随后进行“格式化”或“重新格式化”；或当不再需要时物理破坏可移动存储介质。</p>
Trinseo 保密—未经许可不得共享	<p>必须撕碎、焚烧或存放在处理此类信息规定的安全性—批准的容器中。撕碎的文件可以在垃圾填埋场处置。</p> <p>电脑或可移动存储介质：与 Trinseo 受限—仅供内部使用相同。</p>
Trinseo 保密—从第三方来源获得	<p>与 Trinseo 保密—未经许可不得共享相同。</p>
律师—当事人特权	<p>与 Trinseo 保密—未经 Trinseo 律师许可及指示不得共享相同。</p>
律师工作成果	<p>与 Trinseo 保密—未经 Trinseo 律师许可及指示不得共享相同。</p>
个人及保密	<p>与 Trinseo 保密—未经许可不得共享相同。</p>
回收计划	<p>所有纸张回收计划必须遵守处理指引。撕碎或其他销毁方法可能需要非 Trinseo 人员提供服务，因此应与参与处置 Trinseo 信息的所有承包商签订 Trinseo 保密协议。该流程应接受随机审核</p>
电子数据处理指导	<p>大量电子数据存储于电脑系统和其他电子介质中。此数据可能包含敏感信息，包括人事档案、财务数据和受保护的健康信息。此类存储设备或其中包含的数据若处置不当，可能导致数据丢失或数据泄露给未经授权的用户。电子介质被定义为用于记录信息的任何电子存储设备，包括但不限于硬盘（包括 Trinseo 工作站 (DWS)）、磁带、光盘、录像带、录音带和可移动存储设备（如软盘、压缩盘、CD、DVD 和 USB 存储设备）</p>

信息处理与分类指引

相关文档

Trinseo 信息处理政策

文档和记录管理

当前程序已归档至在管理系统下的电子文档管理系统（网络 EDMS）中。本列表不包括位于 *styron_RecordsMgmt* 文件服务器上的主电子副本。如果文档不在 *styron_RecordsMgmt* 文件服务器或以下所列的位置中，则视为不受控制。

更新 Trinseo 内部网中的版本

修订

本文档修订人：

Thereasa Alcorn, 全球 RIM 协调员

2015 年 2 月 2 日

(姓名 / 职务)

(日期)

验证

本文档验证人：

Jen Levin, 副总法律顾问

2014 年 3 月 3 日

(姓名 / 职务)

(日期)

批准

本文档批准人：

记录管理委员会

(姓名 / 职务)

(日期)

MOC

MOC 编号

批准日期: _____

文档历史记录

以下信息记录了本文档的至少 3 次变更，并列出了最近 6 个月的所有变更。

日期	修订人	变更
3/3/2014	J. Levin; T. Alcorn	创建支持信息处理政策的指导文件
2015 年 2 月 2 日	T. Alcorn	更新至 Trinseo 名称变更。