《正大集团信息管理政策和指南》

目录

《正大集团信息管理政策和指南》

1. 宗旨

信息是正大集团的重要资产，因此，必须以系统性和高效的方式进行信息监管，确保其的可靠性、准确性和完整性，预防正大集团资产损失的风险和信息的泄露，让公司可以做出更好的商业决策并提升公司的竞争力。

2. 范围

本政策和指南适用于正大集团（简称“集团”），包括正大集团所有下属公司。下文中的“公司”指所有采用本政策和指南的公司。本政策将至少每年一次或视情况而修订。

3. 目标

使董事、管理层及员工了解其在预防不当使用正大集团信息和信息泄露方面的角色和职责。

4. 角色和职责

所有人在履行职责与协调工作时的准则，包括：

4.1 董事会

4.1.1 制定《信息管理政策和指南》；

4.1.2 履行监督职责，确保本政策和指南的有效落实。

4.2 管理层

4.2.1 根据业务和公司的环境，以及当地的法律法规制定相关的工作规章制度；

4.2.2 明确信息管理和信息系统的负责部门或人员；

4.2.3 明确访问信息和信息系统的权限；

4.2.4 确保信息使用的风险管理；

4.2.5 确保公司制定本政策和指南的执行报告，包括报告信息使用的问题。

4.3 信息和信息系统负责部门或人员

4.3.1 根据第 5.2 条指南“风险管理”履行职责；

4.3.2 根据第 5.3 条指南“信息管理”履行职责；

4.3.3 根据第 5.2 条指南“外部信息交流”履行职责；

4.3.4 根据第 5.2 条指南“信息销毁”履行职责；

4.3.5 报告本政策和指南，以及相关规章制度的执行情况，包括信息使用问题的相关报告。

4.4 信息技术部门

4.4.1 维护公司信息技术系统；

4.4.2 监管信息技术系统和网络的访问情况；

4.4.3 维护信息的安全；

4.4.4 确保公司做好信息的备份和恢复。

4.5 内部审计部门

4.5.1 根据本政策和指南，对信息管理的执行情况进行审计；

4.5.2 为全体人员提供咨询和相关知识，以确保本政策和指南的正确落实。

4.6 员工

4.6.1 保护个人信息，以及正大集团、客户和合作伙伴信息的安全、不泄露；

4.6.2 以准确、可靠的原则编辑信息、记录和报告；

4.6.3 保护正大集团的知识产权且不侵犯他人的知识产权；

4.6.4 遵守本政策和指南，以及信息管理相关的法律法规和国际标准。

5. 指南

5.1 根据“PAPA”信息伦理理论，即：信息隐私权(Privacy)、信息准确性(Accuracy)、信息产权(Property)、信息资源存取权(Accessibility)履行职责，具体如下：

5.1.1 信息隐私权（Information Privacy）

个人隐私信息包括身份证号码、出生日期、账户信息（账号和密码）。

1) 对所有董事、管理层、工作人员、客户、供应商和业务合作伙伴的个人信息保密并维护其安全；
2) 禁止将任何来源的客户信息用于营销目的，或重新创建客户数据库并出售给其他公司；
3) 妥善保管与正大集团信息系统有关的账号和密码，确保其具备不可预测性；
4) 严禁将密码记录在他人可能容易获取、破解的地方；
5) 在有必要向他人告诉密码时，应在事后立即更换密码。

5.1.2 信息准确性（Information Accuracy）

1) 必须在保存任何信息前核实其准确性，并及时更新信息，以保证信息的准确性和可靠性；
2) 必须确保信息来源的可靠性和可核实性，比如政府部门等可靠的单位组织。

5.1.3 信息产权（Information Property）

1) 全部或部分员工发明创造的知识产权属于正大集团；

2) 严禁侵犯和未经允许披露在正大集团开发并未公开的知识产权和版权；
3) 严禁使用、复制、打印或公布侵权的图片、文章、书目或其他文件等。包括在正大集团信息技术系统上安装盗版软件；
4) 下载互联网上软件或更新软件时，须谨慎小心。严禁在正大集团信息技术系统上盗用他人版权或知识产权的软件；
5) 维护正大集团的知识产权，未经允许禁止披露；
6) 避免不当或不法使用正大集团的知识产权。在使用时须确保已盖章或放置商标、服务商标或版权符号，例如：®，TM，© （20XX）等；
7) 任何员工的发明或创新，比如应用软件、技术发明等创新成果，应向正大集团报备；
8) 应协助正大集团获取专利、版权。保护正大集团的知识产权、商标；

5.1.4 数据访问权（Data Accessibility）

1) 管理层应根据员工的工作和职责授予访问权，包括电脑系统、应用软件、电子邮箱、无线网络、网络系统等；
2) 管理层应至少每年或有人员变动时，如人员升职，进行审批信息和信息系统的访问权限；
3) 唯有被管理层授权人，才可以更改数据和信息系统的访问权限；
4) 记录所有数据和信息系统访问，以及权限更改的情况，包括被许可方和未经许可方的，以备发生问题时作为调查证据；
5) 记录和监督信息系统使用情况，并对可能发生的关键信息系统安全漏洞保持警惕。

5.2 风险管理指南

5.2.1 进行风险识别和评估；

5.2.2 进行风险排序，优先处置重大风险；

5.2.3 制定风险防控整改措施，并确保其有效执行落实。

5.3 信息管理指南

5.3.1 信息保密等级划分(Classification of Information)，应鉴于安全风险，影响商业价值、公司财产和形象划分，如下：

1) 绝密文件（Special Control）【紫色】，指可能影响业务战略，并严重损害市场竞争力的信息。如果此类信息泄露，可能对公司在国际上的声誉造成损害。例如：
   - 商业秘密信息（Trade Secret）；
   - 业务战略计划；
   - 市场营销、产品研发计划；
   - 公司合并方案
2) 秘密文件（Confidential）【红色】，指可能对业务运作和发展造成影响的信息。如果此类信息泄露，可能对公司在国内的声誉造成损害，被起诉支付赔偿金。例如：
   - 市场营销文件（尚未公开）；
   - 个人数据；
   - 客户数据
3) 内部文件（Internal Use Only）【黄色】，指仅限于集团旗下公司交流的信息，可能对日常工作造成影响、损害组织形象的信息。例如：
   - 内部通知、政策；
   - 规章制度、工作手册；
   - 日常工作记录
4) 公开文件（Public）【绿色】，指不会对组织造成影响、并可以向外部人员公开的信息。例如：

- 可持续发展数据；
- 宣传数据；
- 营销宣传

另外，任何打印件或复印件的保密等级，应与其原件一致，无论是完整还是部分的内容。

5.3.2 信息及相关设备的存储指南：

1) 管理层及信息负责人需根据信息保密等级，确定其存储期限；
2) 使用移动存储设备进行信息备份，并明确记录备份详情，包括相关储存软件、日期和时间、负责任的姓名；
3) 妥善保管储存公司信息的信息系统和设备，包括手机、笔记本电脑、平板电脑等。在职场外使用以上设备时须特别谨慎，使用后应放在有锁的地方保管；
4) 需要退出信息系统或完成工作后，须进行锁屏并设置密码；
5) 当正大集团信息或储存集团信息的设备丢失或被盗时，应立即向信息技术部门报告。

5.3.3 自带设备使用指南：

移动设备是业务沟通的重要工具，有助于提高工作的效率。然而，需要使用自带设备的员工，应在链接公司网络前申请批准。自带设备和软件使用批准流程，按照各公司的规定。

需要使用自带设备的员工须遵守以下指南：

1) 在员工自带开发的知识产权归正大集团所有；
2) 链接内部网络前，应请求信息技术部门设置自带设备的系统并安装基础应用软件；
3) 若在自带设备上储存正大集团的数据，须设置访问该数据的密码，以防未经授权人盗窃。另，请不要在无人看管的情况下，将自带设备放在公共场合；
4) 应定期备份正大集团相关的数据，以防丢失的情况；

5) 当储存正大集团数据的自带设备丢失或被盗时，应立即向正大集团报告；
6) 员工须承担任何与自带设备相关的费用；
7) 员工须承担自带设备上的个人数据或正大集团数据丢失的风险，不管是应用软件或设备瘫痪、被病毒或恶意软件攻击等失误的原因；
8) 离职前须提交或销毁自带设备上的正大集团的数据；
9) 正大集团保留断开员工自带设备与内部网络等其他服务的权力，且无需提前通知。

5.3.4 数据备份指南：

1) 关于应用软件和技术系统上的数据备份和恢复的流程，应制定成书面的文件；
2) 实时将正大集团信息系统和硬盘上的数据备份到其他储存设备，例如：U 盘、移动硬盘和光盘；
3) 妥善保管数据储存设备，以确保随时可以使用数据，例如：将数据备份到新的储存设备、至少每年定期检查数据储存设备，以防其退化。

5.3.5 跨部门或公司发送秘密信息和绝密信息时，应对信息进行加密。

5.4 外部人员信息交流指南

5.4.1 需要向外部人员或未经授权人发送秘密信息和绝密信息时，须与该信息负责人核实，并向管理层请示批准。此外，必须让对方签订保密协议；

5.4.2 向外部人员发送秘密信息和绝密信息时，应对信息进行加密。

5.5 网络使用指南

5.5.1 禁止在工作时间内利用公司的网络处理与正大集团不相干的私人事务；

5.5.2 禁止利用公司的网络侵犯他人的版权，例如：从互联网上未经允许地下载他人的软件、音乐、电影、图片或文字，并从中谋取个人利益；

5.5.3 使用正大集团网络时，切勿违反集团的《行为准则》；

5.5.4 使用正大集团网络时，避免造成他人网速下降的行为，例如下载大量的文件。

5.6 电子邮箱使用指南

5.6.1 禁止以隐藏邮件发送人的方式向他人发送电子邮件，以骚扰他人；

5.6.2 禁止通过电子邮件发送骚扰他人的文字或图片，包括非法、羞辱、侵犯、挑衅、仇恨或支持非法活动的内容；

5.6.3 在打开来自未知发件人的邮件时需谨慎，可能是恶意软件和网络钓鱼。当发现可疑的邮件时，应立即向信息技术部门报告；

5.6.4 点击任何链接时需谨慎，可能是恶意软件，例如病毒、间谍软件、特洛伊(Trojan)木马病毒等；

5.6.5 切勿以密送（Blind Carbon Copy: Bcc）的方式发送工作邮件；

5.6.6 确保每一封电子邮件已设置邮件签名；

5.6.7 应在工作时间外或午休时使用个人邮箱。

5.7 社交媒体使用指南

请参照《正大集团社交媒体使用政策和指南》

5.8 信息销毁指南

5.8.1 内部文件、秘密文件和绝密文件的信息的打印件，无论是纸质或任何介质，若不再使用必须用碎纸机进行销毁。公开文件则可以直接丢入垃圾桶，或用碎纸机进行销毁。

5.8.2 销毁数据存储设备前，须确保已迁移关键信息，其他信息则须永久删除。

5.9 信息泄露检查指南

当秘密文件和绝密文件的信息泄露时，负责管理层人员须成立调查委员会，进行原因、失误的检查，并改进信息储存方法，信息泄露防护系统，并向高层管理人员报告，以防信息泄露的再次发生。

6. 培训

所有公司应通过培训、会议等渠道向董事、管理层和工作人员传达《正大集团信息管理政策和指南》，并定期进行评估其效果。

7. 举报

一旦发现任何违反本政策的行为，应根据《正大集团检举政策和指南》进行举报投诉。无论是在事件调查过程中还是之后，公司须全程保护

举报投诉人，确保其不被报复和调动工作岗位，并保密其个人信息和举报投诉的内容。

8. 疑问指导

如果您发现可能违反法律、法规和本《正大集团信息管理政策和指南》的行为，并有疑问，请在做出任何决定或采取任何行动之前，向您的主管、团队或负责监督利益冲突的人员、合规部门和法务部门寻求指导。

9. 处罚办法

所有员工必须积极配合内部和外部的调查负责人。任何直接和间接违反或不遵守本政策和指南的行为将一律按照公司的规定受到纪律处分。

10. 相关法律法规和政策

10.1 泰国 2007 年《计算机犯罪法》；

10.2 泰国 2018 年《版权法》；

10.3 《中华人民共和国数据安全法》；

10.4 《中华人民共和国网络安全法》；

10.5 《正大集团社交媒体使用政策和指南》；

10.6 ISO/IEC 27001:2013 信息安全管理体系。

11. 附录

本政策和指南附有下列附件:

11.1 附录一 ：基于文件保密等级的封皮示例

11.2 附录二 ：基于文件保密等级的纸张示例

附录一
基于文件保密等级的封皮示例

绝密文件

(SPECIAL CONTROL)

公司标志

绝密文件封皮

本文件的信息可能影响业务战略，严重损害市场竞争力。并可能对公司在国际上的声誉造成损害。

本文件拥有者的职责

1. 本文件拥有者需承担本文件的安全的责任；
2. 确保有妥当的保护措施，不放在无人看管的地方，除非是安全的地方；
3. 只能向有访问权的人士披露本文件。

保管方法

使用本文件后，须放入注明是“绝密文件”的包装或文件夹，并储存在人员出入管控区域的保险箱内。

复制办法

禁止在未经允许前复制、重新编辑绝密文件，无论是部分还是全部。

销毁办法

禁止在丢入垃圾桶，仅能使用碎纸机进行销毁。

(当此封皮与本文件分开时，将不再视为保密文件)

秘密文件

(CONFIDENTIAL)

公司标志

秘密文件封皮

本文件的信息可能对业务运作和发展造成影响，以及对公司在国内的声誉造成损害、被起诉支付赔偿金。

本文件拥有者的职责

1. 本文件拥有者需承担本文件的安全的责任；
2. 确保有妥当的保护措施，不放在无人看管的地方，除非是安全的地方；
3. 只能向有访问权的人士披露本文件。

保管方法

使用本文件后，须放入注明是“秘密文件”的包装或文件夹，并储存在人员出入管控区域的带锁文件柜内。

复制办法

禁止在未经允许前复制、重新编辑秘密文件，无论是部分还是全部。

销毁办法

禁止在丢入垃圾桶，仅能使用碎纸机进行销毁。

（当此封皮与本文件分开时，将不再视为保密文件）

内部文件

(INTERNAL USE ONLY)

公司标志

内部文件封皮

本文件的信息可能对日常工作造成影响、损害组织形象，仅限于内部使用。

本文件拥有者的职责

1. 本文件拥有者需承担本文件的安全的责任；
2. 确保有妥当的保护措施，不放在无人看管的地方，除非是安全的地方；
3. 只能向有知情权的相关人员职务披露本文件。

保管方法

使用本文件后，须放入注明是“内部文件”的包装或文件夹，并储存在带锁的文件柜内。

复制办法

如需复制、重新编辑内部文件，无论是部分还是全部，须经过相关负责人的允许。

销毁办法

建议使用碎纸机进行销毁。

（当此封皮与本文件分开时，将不再视为保密文件）

公开文件

(PUBLIC)

公司标志

公开文件封皮

本文件的信息不会对组织造成任何影响，并可以向外部人员公开。

本文件拥有者的职责

本文件拥有者可视情况公布本文件。

保管方法

使用本文件后，须放入注明是“公开文件”的包装或文件夹，并储存在文件柜内。

复制办法

可视情况复制、重新编辑内部文件，无论是部分还是全部。

销毁办法

可以直接丢入垃圾桶或使用碎纸机进行销毁。

(此封皮非保密文件)

附录二
基于文件保密等级的纸张示例

公司标志

秘密文件

秘密文件

秘密文件

第 1 / .....页

公司标志

内部文件

内部文件

内部文件

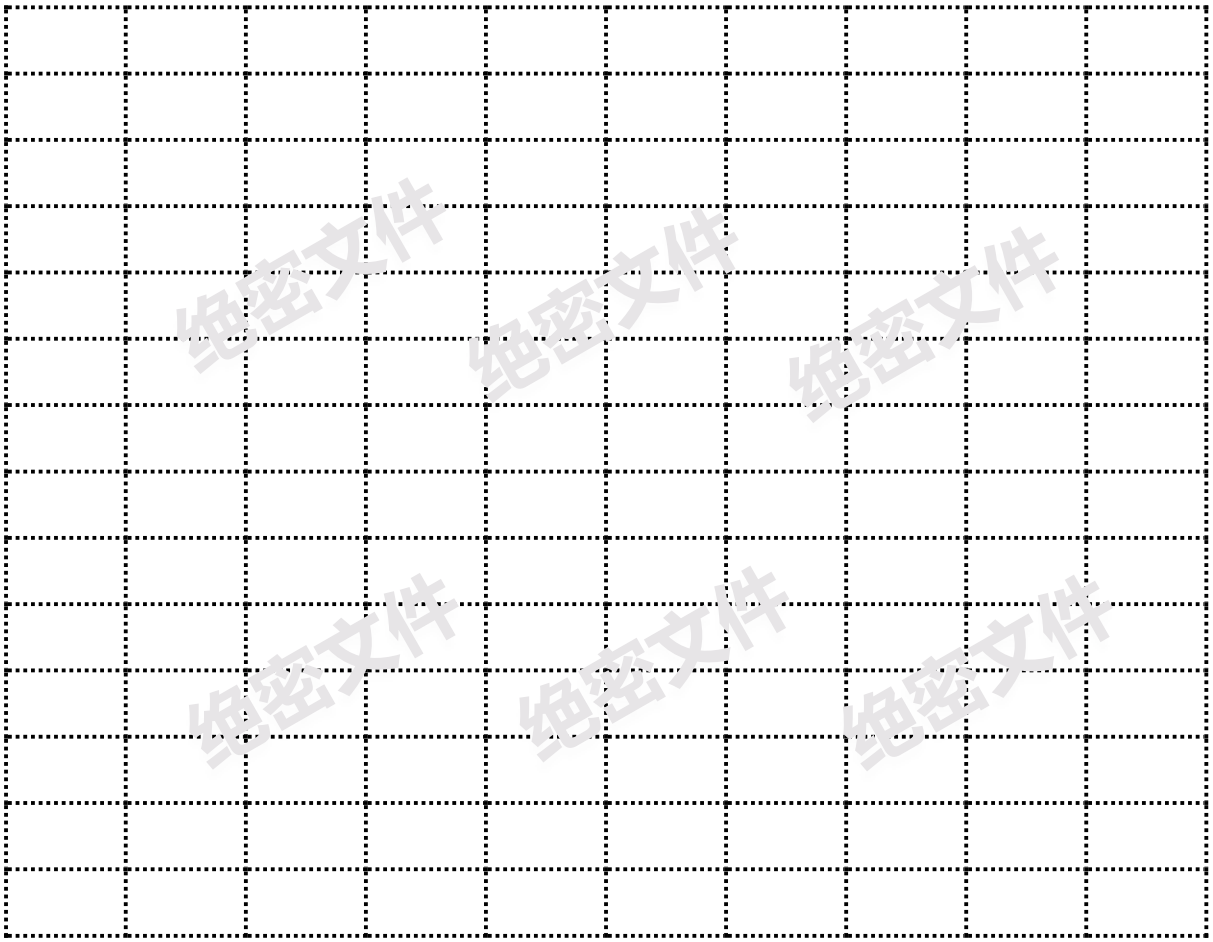
第 1 / .....页

公司标志

公开文件

公开文件

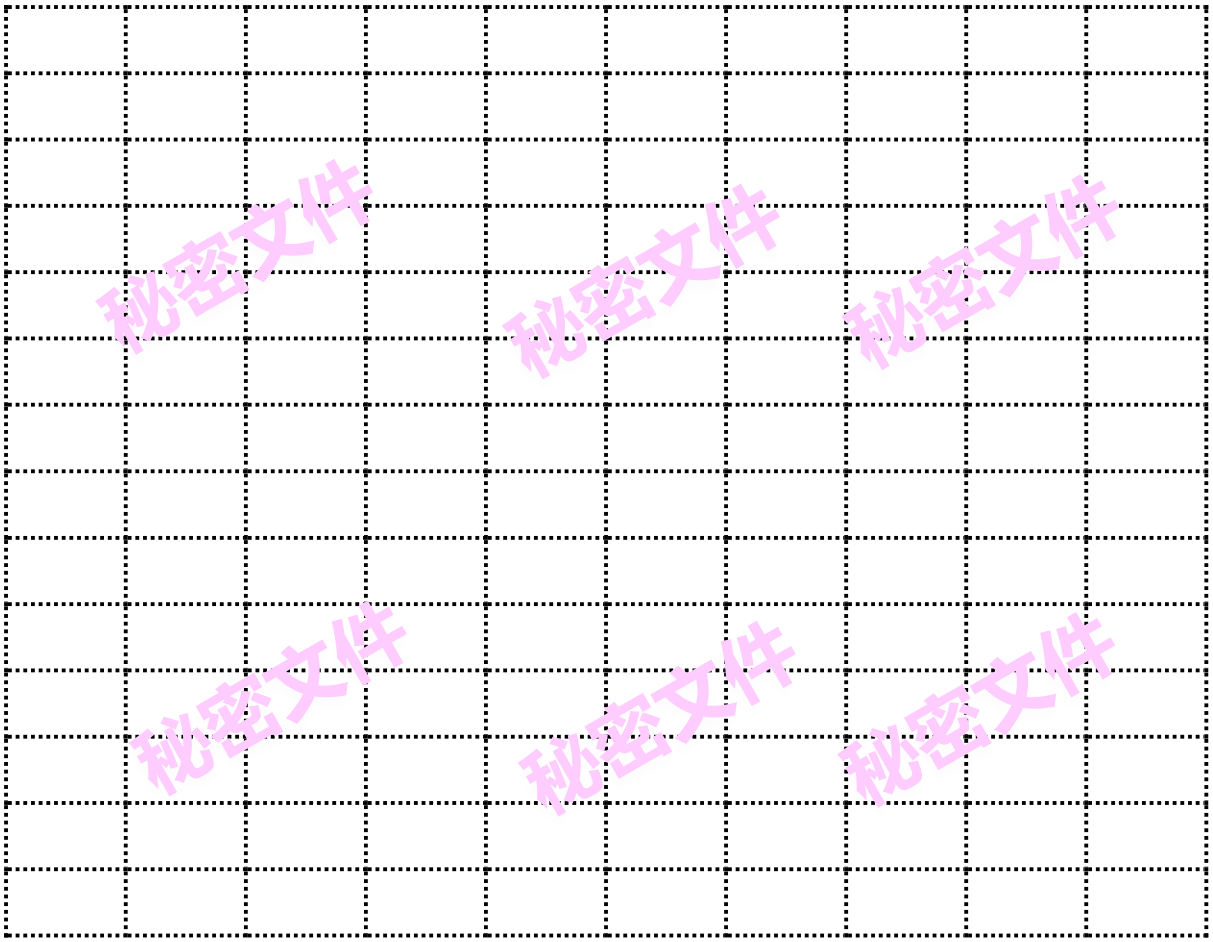
第 1 / .....页



绝密文件

公司标志

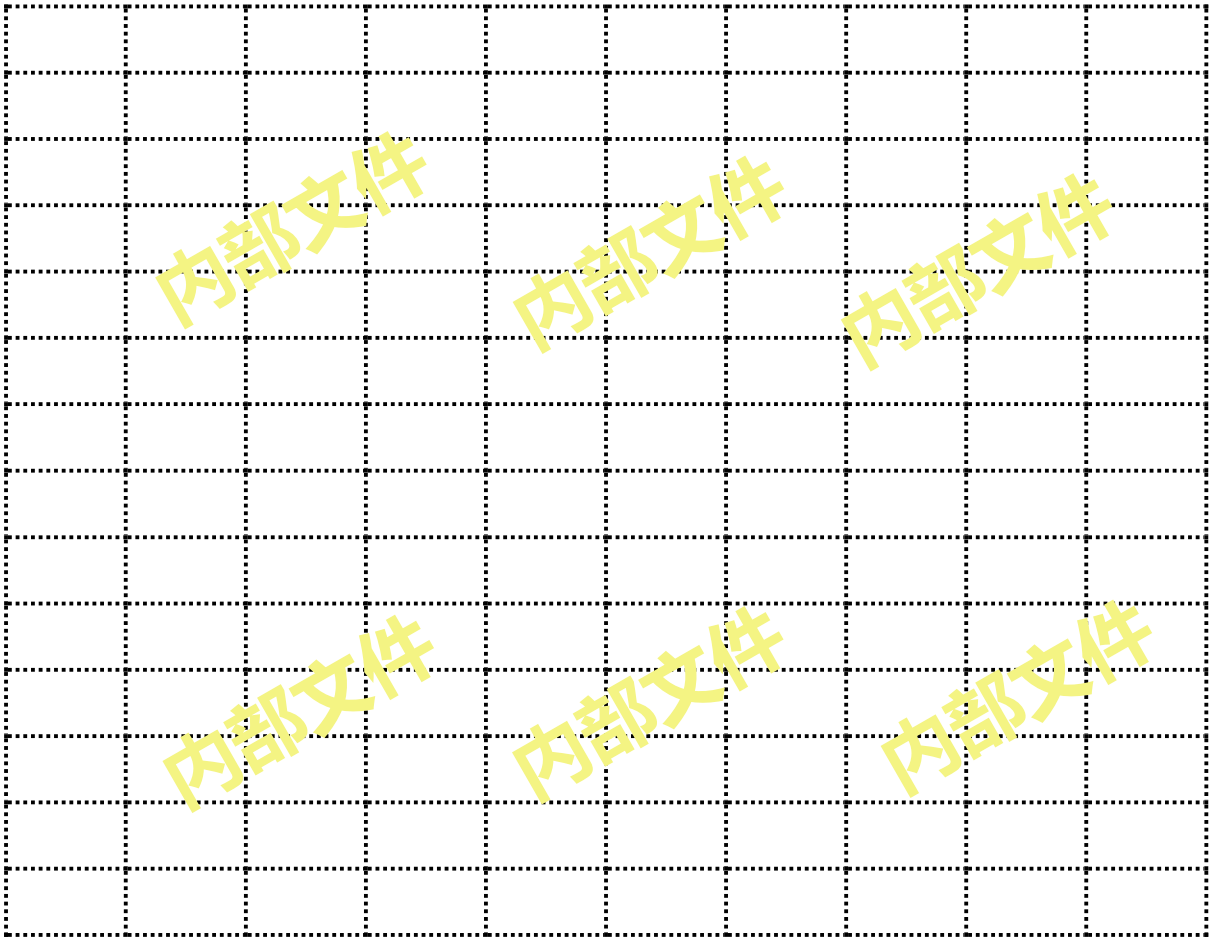
秘密文件



秘密文件

公司标志

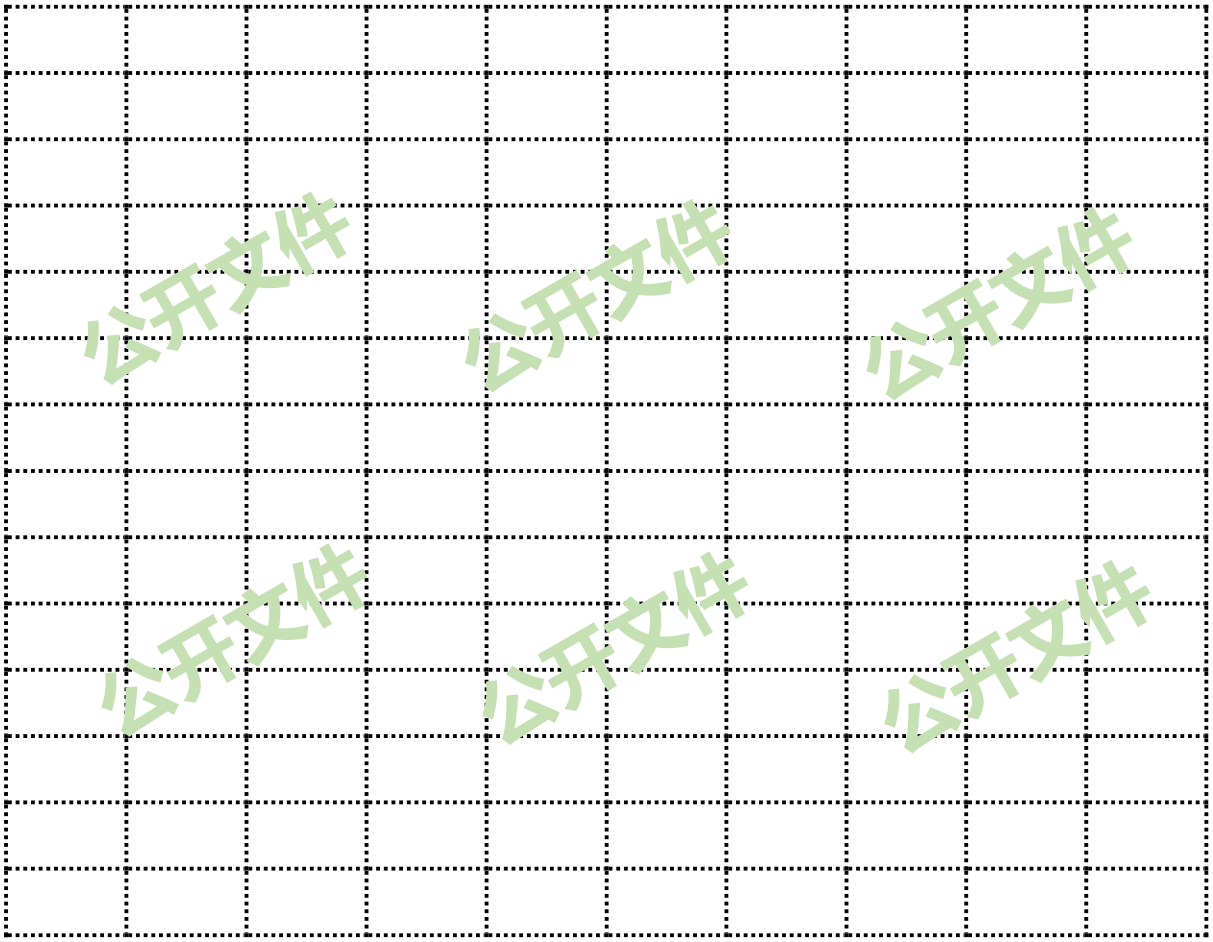
内部文件



内部文件

公司标志

公开文件



公开文件