MedTecX IT Security Guideline

骊霄 IT 安全指南

1. 办公环境安全 Keep Office Environment Secure

- 请不要为未知人员打开门禁，保证不被非 MedTecX 的用户或允许的访客进入办公场所。

  Never open the door for unknow person.

2. 外来人员防范 Prevent Attack From Strangers

- 请亲自接待您的访客。

  Never entrust others to receive your visitors.

- 访客须由 MedTecX 接待者陪同，方可进入办公区域。

  Visitors can only enter the office area accompanied by MedTecX employee.

3. 制造私密环境 Create a Private Environment

- 通过电话会议、视频会议等方式沟通公司机密信息时，需要保证不被外人（包括您的家人）听到。

  Please create an intimate environment when communicating company’ s information through phone calls, video conferences, etc.

- 在开会时，如果需要演示报价等机密信息，请拉上会议室的百叶窗或窗帘。

  Please draw the blinds or curtains when holding a meeting in the meeting room.

- 建议在公司配备的电子设备贴上防窥膜，比如手机和电脑屏幕。

  It is recommended to use privacy screen protector for electronic devices.

4. 保持桌面整洁 Keep Your Desk Clean & Tidy

- 请勿随意将重要文件存放在桌子上，必须放入带锁的柜子，钥匙请随身携带。

  Store confidential files in locked file cabinets and always keep the keys with you.

- 请不要将密码及隐私信息记录在便签纸上并贴于桌面、屏幕等办公场所。

  Never record passwords or sensitive information on sticky notes and post it on desk, screen and other office areas.

- 离开座位时，请将电脑、手机等其他电子设备锁屏。

  Please keep your electronic devices locked when leaving seats.

5. 便携设备使用安全 Keep Portable Device Safe

- 电脑笔记本，手机，等便携式设备必须设置有密码保护的锁屏。

  Please set passwords for your laptops, phones, tablets and other portable devices.

- 出差时，电脑笔记本，手机等都应随身携带。

  Please carry all your portable devices with you when travelling on business.

- 请勿将出于为锁定状态下可访问数据的便携式设备留给其他人保管。

  Never leave unlocked portable devices alone.

- 如设备遗失，请立即向您的经理报告并联系 Sinokap IT。

  If you lose your device or think it might be stolen, please report to your manager and contact Sinokap IT ASAP.

6. 文件安全传输分享 Ensure the Safe Transmission & Sharing of Files

- 进行文件传输与分享时，请对文件或文件夹加密后再通过邮件或文件服务器中的分享链接发送给对方。加设的密码需要通过第二种途径发送给对方，例如邮件对方文件后，短信告知文件的访问密码。

  Please encrypt the sharing files or the folders, and then send them to the other party via email or the share link. The password on files should be sent through the second method.

- 请使用公司标准的即时通讯工具进行业务沟通，微信（个人版）、QQ 等个人聊天工具仅作个人通讯，不得通过微信、QQ 等个人聊天工具传输业务文件。

  Please use company standard instant messaging tool for business communication. Do not transfer business related documents through personal instant messaging tool.

- 发送邮件时，请核对收件人及附件内容正确。

  Please double check if the recipient and the attachment are correct when sending an email.

7. 文件数据安全 Keep File Data Secure

- 所有工作文件必须存在公司的服务器上的相应权限的文件夹，因为服务器有备份。

  All company files must be kept on the file server which has a regular backup.

- 请勿上传未知文件到服务器上。

  Please do not upload unknown files to the file server.

- 工作文件不得随意外传。

Company files shall not be freely distributed.

- 工作文件不得用私人邮件外传。

  Please do not sent company files via private mailbox.

- 工作文件不能保存在个人的百度云等第三方的云存储介质。

  All company files should not be saved in a third-party cloud storage media.

8. **密码使用安全 Password Safe**

- IT 给您的设备或者任何账号都必须修改初始密码！请个人妥善保管，不要随意分享给他人！

  Please change the initial password ASAP. Do not share the password with others.

- 密码遗失或者重置请联系 Sinokap IT。

  If the password is lost or needs to be reset, please contact Sinokap IT immediately.

- 密码长度至少 10 位字符，包括大小写字母、数字、特殊符号。

  Passwords must be at least 8 characters long, including uppercase and lowercase letters, numbers, and special symbols.

- 密码不能包含姓名、生日、账户名等个人信息。

  Passwords cannot contain name, birthday, account info., etc.

- 不同账号请勿使用同一个密码。

  Please use different passwords for different accounts.

- 请每 90 天修改密码，新密码不能与前 5 次重复。

  Please change the password every 90 days. The new password cannot be repeated with the previous 5 times.

9. 预防网络钓鱼 Identity and Prevent Phishing

- 请勿点击或下载未知发件人发出的未知链接及未知附件，如收到类似邮件，请立即告知 Sinokap IT。

  Never click suspicious links or download attachments from the email sent by unknown sender. If you receive this kind of emails, please inform Sinokap IT ASAP.

- 请勿泄露个人信息或公司信息给未知收信人。

  Never disclose personal information to unknown recipients.

- 未经 MedTecX 允许，请勿随意下载或安装非标准化软件。

  Never download or install software without the permission of MedTecX.

- 请勿点击未知网站，如有不清楚可以联系 Sinokap IT。

  Please do not open unknown websites.

- 请勿点击连接未知 Wi-Fi，个人外出需要网络可以使用手机热点。

  Never connect unknown Wi-Fi. Please use mobile hotspot instead in public places.

10. 防范数据泄露 Prevent data leakage.

- 请勿将未知的设备插入电脑。

  Please do not insert unknown devices into the computer.

- 打印公司文件时，请使用公司打印机并在打印机旁等候打印完成。

  Please use the company printer and wait for the printing to be completed by the printer when printing company files.

- 请及时销毁含机密信息的废纸，等待纸张全部粉碎后才能离开。

Please destroy confidential waste in time.

- 请及时销毁快递单信息，可以使用涂抹笔遮盖个人信息。

  Please destroy the express information in time.