艺术家的最佳安全实践规范

安全是所有业内专业人士的责任

物理安全

拒绝他人未经授权访问设施、设备和资源。保护员工和财产免受损害或损坏。

- 只邀请经雇主授权的访客参观您的工作地点。
- 不要与他人共享您的工作证/标识卡、电子钥匙或其他钥匙。
- 对于一些敏感的实体物品（如手稿、道具和可拆卸的存储设备），如果不频繁使用，请将其存放在安全的地点。

密码安全

将未经授权访问帐户的风险降至最低。

- 不要将密码透露给他人或允许他人使用您的帐户。对于由您的个人用户帐号所进行的一切活动，您都需要承担一定责任。
- 定期更换密码，所有帐户都要使用强口令。
- 内容访问和其他服务均使用不同的密码。
- 不要将登录和密码凭证一起发送，可以将信息通过两种不同的渠道发出，例如用电子邮件发送用户名，再将密码用短信发出。
- 确保密码的安全性，不要在设备上透露密码的相关信息（例如在台式机、笔记本或加密驱动器上贴便利贴）。

内容安全

将未经授权访问或丢失数字内容的风险降至最低。

- 只使用客户或工作地点认可的安全方法传输数字内容，不要通过电子邮件或未加密的服务（如FTP）进行传递。
- 您有责任确保工作地点所用网络的安全性，不要连接任何未经授权的硬件或安装未经许可的软件。
- 将数字内容存储在合适的位置，定期备份。
- 如果您的客户或雇主明确允许您进行云存储或备份，只能使用Google Drive或Dropbox之类的云存储或备份服务来记录客户内容或其他敏感资料。

注意社交工程

让相关人员无意识地泄露机密信息。欺诈者惯用的伎俩之一。

- 认真阅读并遵守客户和/或雇主提供的安全策略。不要与未经内容所有者许可的他人共享内容，包括对其进行接收、处理或查看。只有直接参与某个项目的人员才有可能使用该内容。
- 专业资料（如LinkedIn和IMDB）中绝不应透露未发布/未出版项目的任何信息，除非您获得了明确的授权。
- 如可能，请使用代号而非实际标题指代相关项目。
- 在公共场所与同事谈论工作时应十分小心，请勿让其他不与您共事的人员听到。

安全事故

如果您怀疑发生机密泄露，该怎么办？

- 将任何内容疑似丢失的情况立即报告给雇主或内容所有者。
- 不要容忍他人的安全疏忽或泄密行为，或者睁一只眼闭一只眼；如果意识到泄密却不上报，您也负有连带责任。
- 如存在疑虑，请咨询您的主管或技术团队。

请注意：以上是VES技术委员会撰写的**一般指南**。不同的工作室、设施或制片过程可能会采用不同的安全策略，视具体情况而定。

如有任何疑虑或疑问，请立即询问您的制作人、主管或雇主的人力资源部门。

如需了解更多信息，请访问 http://www.fightfilmtheft.org/facility-security-program.html。