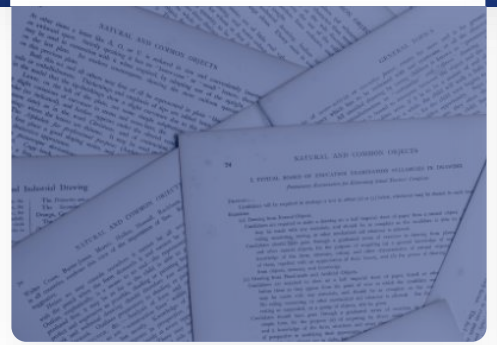
新员工信息安全培训

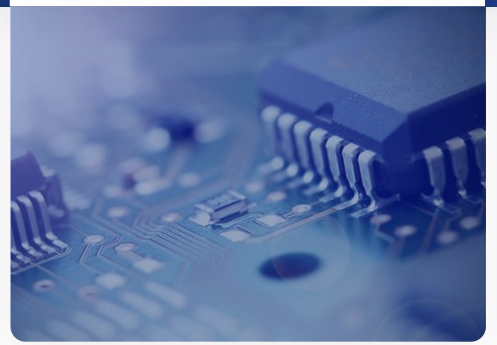
欧西爱司物流（上海）有限公司

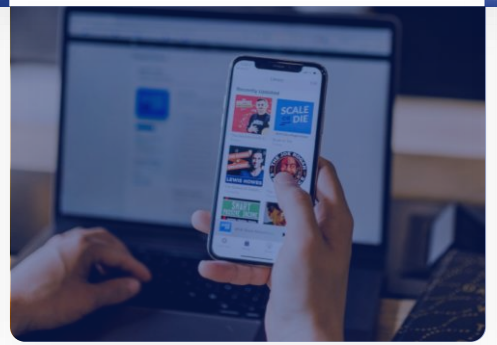
IT部

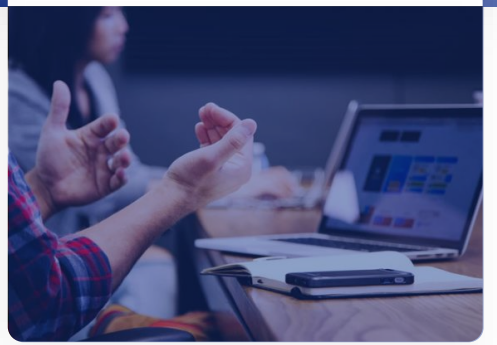
目 录

CONTENTS









目 录

CONTENTS

01

什么是信息安全

OCS ANA GROUP

1.1 什么是信息

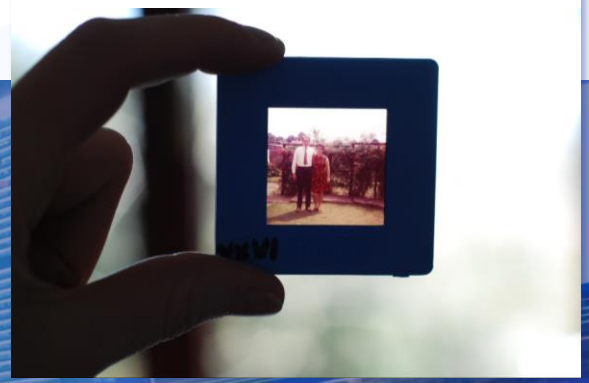
信息是一切可被存储和使用的物质与知识描述对企业具有价值的信息，称为信息资产。

纸面化信息

电子化信息

载体信息

人的记忆



1.2 什么是信息安全？

信息安全是指：保障保密信息不被泄露，在使用时可用，整个信息未被篡改。

确保信息在存储、使用、传输过程中不会泄露给非授权的用户或者实体

保密性
Confidentiality

确保信息在存储、使用、传输过程中不被非授权用户篡改；
防止授权用户对信息进行不恰当的篡改；
保证信息的内外一致性

完整性
Integrity

确保授权用户或者实体对于信息及资源的正常使用不会被异常拒绝，
允许其可靠而且及时地访问信息及资源

可用性
Availability

目 录

CONTENTS

02

信息安全的重要性

OCS ANA GROUP

2.1 信息安全威胁就在我们身边







不可抗力
（火灾、地震、临时停电、突发网络故障）

国与国之间的信息窃取

国家：从最高层次来讲，信息安全关系到国家安全（军事机密）

以企业为目标的恶意攻击

企业：对组织机构来讲，信息安全关系到正常运作和持续发展（客户资料）

针对个人身份信息的安全威胁

个人：信息安全是保护个人隐私和财产的必然要求（骚扰电话）

2.2 发生信息安全事件的危害

1

经济损失

个人信息遭冒用

2

名誉损害

个人信息泄漏，
遭遇诈骗

3

牢狱之灾

4

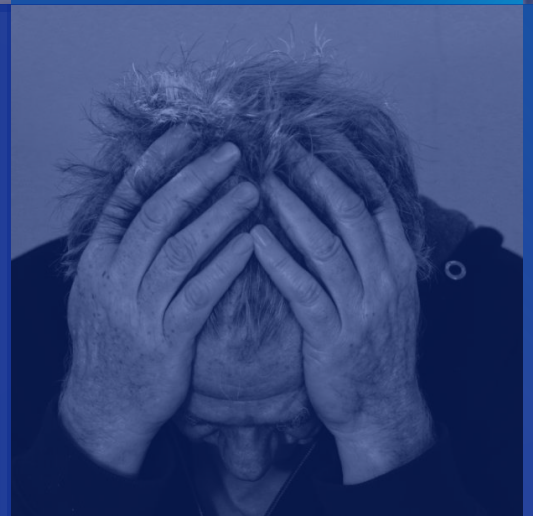
引发竞争

公司客户信息泄漏，
价格恶性竞争

5

引发战争

国家军事机密泄漏



2.3 我在信息安全中的角色

三分技术，七分管理

技术手段

是基石

人员安全意识

人：最易忽视的高风险领域，

起关键作用

信息安全制度

是保障

2.4 最常犯的一些错误

想想你是否也犯过这些错误：

将口令写在便签上，
贴在电脑监视器旁

开着电脑离开，
就像离开家却忘记关灯那样

不能保守秘密，口无遮拦，
泄漏敏感信息

轻易相信来自陌生人的邮件，
好奇打开邮件附件

使用容易猜测的口令，
或者根本不设口令

丢失笔记本电脑

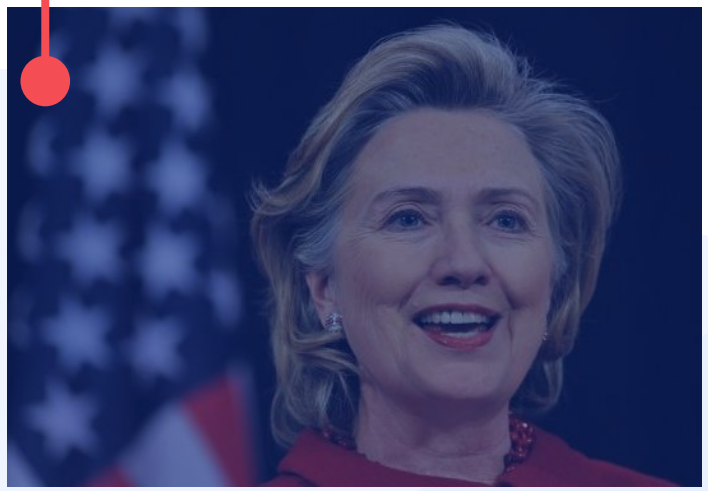
随便上网，或者随意将无关
设备连入公司网络

事不关己，高高挂起，
不报告安全事件

只关注外来的威胁，
忽视企业内部人员的问题

2.5 一些信息安全案例

2016年，在美国，希拉里作为美国历史上第一个女性候选人原本正顺风顺水，却因为“邮件门”最终丢失总统宝座（钓鱼邮件）。



2017年5月10日 “黑客”入侵某快递公司后台盗近亿客户信息。

2018年9月19日，顺丰科技数据中心的一位高级工程师（邓XX）误删生产数据库，导致某项服务无法使用并持续 590 分钟。

2.6 一些数据

《中国网民权益保护调查报告》(2015年-2016年)

- 网民因信息泄露、电信诈骗等现象导致总体损失约人民币 **805亿元**（2015），**915亿元**（2016）
- **78.2%** 的网民个人身份信息被泄露过
- **63.4%** 的网民个人网上行为信息被泄露过

2014年国际刑警组织发布

- 全球网络犯罪掘金 **3万亿美元**，已超过大麻、冰毒和可卡因贩毒之总和

据美国投资咨询机构Cybersecurity Ventures预测

- 到2020年全球每年因网络攻击和网络罪犯带来的损失将高达 **6万亿美元**

目 录

CONTENTS

3．我们应该怎么做

提高安全意识

- 安全就是“矛”和“盾”的关系
- 便捷与安全永远无法同时满足
- 知道如何去识别一个潜在风险

掌握和实行良好的安全习惯

- 在日常事务中养成良好的信息安全习惯
- 同时鼓励其他人也这么做

报告任何异常事件

- 如果您发现了某件安全事件，第一时间通知适当的联系人

目 录

CONTENTS

04

信息安全如何实现

OCS ANA GROUP

4.1 离开工位

1. 电脑锁屏 Win + L

2. 将办公桌面的文件、笔记本等收拾到柜中

4.2 重要信息的保密

各类信息，无论电子还是纸质，在标注、授权、访问、存储、拷贝、传真、内部和外部分发（包括第三方转交）、传输、处理等各个环节，都应该遵守既定策略。

凡违反程序规定的行为，公司将酌情予以纪律处分。

4.3 电子邮件系统安全使用

发送邮件（四禁止）

- 禁止发送或转发反动或非法的邮件内容
- 禁止伪造虚假邮件，不得使用他人账号发送邮件
- 禁止将公司Email用于工作以外用途
- 禁止未采取必要加密保护措施的机密信息通过Email发送

接收邮件（三绝不）

- 绝对不要打开不安全的邮件附件，常见后缀：.bat .com .exe .vbs
- 绝对不要打开任何未知文件类型的邮件附件，包括邮件内容中到未知文件类型的链接
- 绝对不要轻易相信索要敏感信息的邮件（钓鱼邮件），应该仔细核对发件人邮件地址，并当面或电话核实

4.4 病毒防范

所有计算机部署指定防毒软件

不得以任何理由私自关闭或卸载防毒软件

不得以任何理由对防毒软件的安全设置进行任何更改

发生任何病毒事件，相关人员应及时向IT部门汇报

4.5 移动介质安全

禁止在公司电脑上使用 U盘、移动硬盘 等移动存储介质

若确有文件需要通过移动介质方式进行传输，
请联系IT部门协助处理

4.6 口令安全

用户名+口令是最简单也最常用的身份认证方式

针对口令的攻击简便易行，口令破解快速有效

口令是抵御攻击的第一道防线，防止冒名顶替

由于使用不当，往往使口令成为最薄弱的安全环节

口令也是抵御网络攻击的最后一道防线

口令与个人隐私息息相关，必须慎重保护

4.6 口令安全

何为脆弱的口令?

- 少于10个字符
- 单一的字符类型，例如只用小写字母，或只用数字
- 用户名与口令相同
- 所有系统都使用相同的口令
- 口令一直不变

最常被人使用的弱口令

- 自己、家人、朋友、亲戚、宠物的名字
- 生日、结婚纪念日、电话号码等个人信息
- 工作中用到的专业术语，职业特征
- 字典中包含的单词，或者只在单词后加简单的后缀

4.6 口令安全

口令设置建议：

1. 口令至少应该由10个字符组成
2. 口令应该是大小写字母、数字、特殊字符的混合体
3. 不要使用名字、生日等个人信息和字典单词

值得注意的是：虽然口令是越复杂越好，但“选用20个随机字符作为口令”的建议也不可取；人们总习惯选择容易记忆的口令，如果口令难记，可能会被写下来，这样反倒更不安全

例

找到一个生僻但易记的短语或句子（可以摘自歌曲、书本或电影），然后创建它的缩写形式，其中包括大写字母和标点符号等
例：My son Tom was born at 8:05 ->MsTwb@8:05

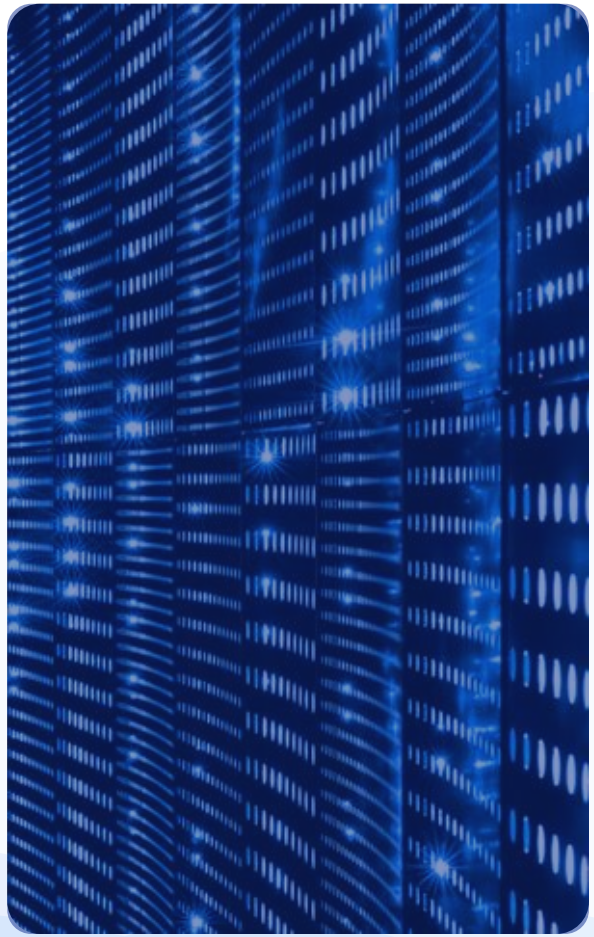
例

试着使用数字和特殊字符的组合，避免“qwerty”这样的直线，而使用Z字型或者多条短线
缺点：这种方法很容易被人看出来，键盘输入时不要让人看见。

4.6 口令安全

口令管理：

1. 员工有责任记住自己的口令
2. 初始口令设置不得为空
3. 口令设置不得少于10个字符
4. 口令应该包含特殊字符、数字和大小写字母
5. 口令应该经常更改，设定口令最长有效期为不超出3个月
6. 口令输入错误次数限制



目 录

CONTENTS

5．内容回顾

信息安全三要素：

保密性

完整性

可用性

信息安全中最薄弱的环节：

人

我们应该怎么做：

提高信息安全意识

掌握和实行良好的安全习惯

及时报告任何异常事件

常见情景：

离开工位

重要信息保密

电子邮件安全

病毒防范

移动介质安全

口令安全

信息安全从自身做起！

从一点一滴做起！

谨记您的安全责任：确保敏感信息免遭窃取、丢失、非授权访问、非授权泄漏、非授权拷贝，这些信息既包括纸质文件，又包括计算机和存储设备中的信息。

新员工信息安全培训

欧西爱司物流（上海）有限公司

IT部