# 信息资产安全管理

1. 保密性要求较高的敏感纸质数据，不需要再使用时,我们应该如何?  **A**
2. 通过碎纸机将其碎掉
3. 将其直接扔到垃圾桶
4. 带出办公区送给他人
5. 作为再生纸使用
6. 确认丢失笔记本电脑中保存的重要资料，若是涉及设备登录密码这类敏感信息，应在第一时间  **D**

A. 关闭相关设备

B. 登录到这些设备

C. 找到丢失的重要资料的备份数据

D. 更改所有设备密码

1. 以下哪项在信息资产管理中不属于数据资产  **C**
   1. 机密信息
   2. 邮件服务器中保存的邮件
   3. 管理制度文档
   4. 内部公共信息

# 物理安全

1. 关于物理安全,以下哪种行为是不允许的?  **B**
2. 遇到门禁时,主动刷卡
3. 直接尾随进入物理区域
4. 遇到未佩戴标识卡的人时主动进行盘查
5. 佩戴公司身份标识卡
6. 办公室突然来了不认识的人，应该怎么做？  **D**
   1. 不询问，让他自己找要找的人
   2. 不询问，但注意着
   3. 看情况，不忙的时候询问
   4. 主动询问
7. 离开座位时,我们应该( ),将桌面上的敏感资料锁入柜中  **C**

A. 拨除电源

B. 要他人照看电脑

C. 锁定计算机

D. 将显示屏关闭

# 人员安全

1. 公司员工在入职时有哪些安全要求？  **D**

A. 领用办公电脑

B. 领用办公用品

C. 填写相关个人信息

D.签订劳动合同与保密协议

1. 在信息安全管理体系中指的第三方包括：( )和第三方人员（合作伙伴）。  **A**

A. 承包方人员

B. 集团

C. 非公司短期雇员

D. 非公司长期雇员

1. 以下哪个做法是不对的？  **C**
   1. “自己的同事进入机房也要进行登记”
   2. “客户的项目完成了，应该把给客户开通的零时账号注销了”
   3. “汇哲马老师是老朋友了，WIFI密码告诉他好了，就不用申请了”
   4. “无论什么岗位，入职的安全意识培训都是要做的”

# 应用开发安全

1. 威胁建模以哪4个步骤形成循环过程？  **A**
   1. 建模，识别威胁，措施，验证措施
   2. 建模，识别风险，控制风险，验证措施
   3. 识别威胁，识别风险，措施，验证措施
   4. 建模，识别威胁，措施，持续改进
2. 在设计开发安全需求时，应考虑哪三项安全属性？  **B**
   1. 机密性、完整性、不可抵赖性
   2. 机密性、完整性、可用性
   3. 完整性、可用性、可追溯性
   4. 可追溯性、可用性、不可抵赖性
3. 下列哪个环境不属于安全开发环境？  **D**
   1. 开发人员所使用的系统
   2. 源代码存放的系统
   3. 开发人员所在的办公室
   4. 开发小组所在的大楼

# 账号权限安全

1. 如果您接触到单位的外包/第三方人员，您是否会因为工作需要把密码告知为您服务的第三方人员？ **B**
   1. 会告诉
   2. 不会，自己输入
   3. 会告诉，第三方使用后自己会更换
   4. 会告诉，自己会定期修改
2. 员工使用帐户过程中,哪个是不允许的?  **A**
   1. 允许GUEST帐号存在
   2. 使用域帐号
   3. 删除不使用的帐户
   4. 一人使用一个帐号
3. 账号申请的正确方式应该是？  **C**
   1. 申请人本人持工牌向账号管理部门提出口头申请
   2. 申请人本人通过公司邮箱向账号管理部门提出申请
   3. 由申请人所属部门的授权申请人对其账户权限进行整理审核，再向账号管理部门提出申请
   4. 由申请人的直属领导对其账户权限进行整理审核，再交由授权申请人向账号管理部门提出申请

# 笔记本电脑的使用

1. 以下哪种方式是不安全的笔记本电脑使用方式？  **C**

A. 无人看管时，将其锁入侧柜中

B. 设置开机口令和屏保口令

C. 让笔记本电脑处于无人看管状态

D. 将笔记本电脑放置在安全的位置，确保没有失窃和损毁的危险

1. 笔记本电脑在放置状态时，应采用（）的方式来防止笔记本电脑丢失，具有单独办公室的人员除外，但办公室的门窗在无人时必须落锁。 **C**
2. 放入未加锁侧柜
3. 锁屏
4. 物理加锁
5. 随意放置
6. 小王向公司借用笔记本电脑用于出差，以下哪个做法是正确的？  **C**
   1. 考虑旅途会无聊，下载了PPS播放器缓冲电影
   2. 硬盘空间不够了，我删掉点原来的内容
   3. 出差前做个数据备份及加密
   4. 在机场候机室，笔记本放在身边的座椅上自己睡着了

# 上网行为规范

1. 以下哪项不是干扰网络正常运行的活动？()  **B**

A. 发送和接收大量数据阻塞网络

B. 给客户发送工作电子邮件

C. 发动拒绝服务攻击

D. 登录未经授权的网络、主机或网络设备

1. 在日常工作和生活中，经常需要从互联网上下载文件，此时必须要关注下载内容的安全性，谨慎使用下载完成的文件，以避免造成不必要的损害。以下关于互联网下载、使用等行为的说法，错误的是  **D**
2. 不随意下载使用来路不明的文件或程序
3. 应进入软件的官方下载主页，或那些规模大、知名的网站进行下载
4. 后缀名为 \*.exe、\*.rar、\*.zip、\*.doc等文件，下载后一定要先杀毒
5. 在浏览网页过程中弹出的插件，都可以直接安装
6. 出差时在机场候机室，应连接以下哪个WIFI网络  **D**
   1. CMCC
   2. 任意一个没有密码的WIFI
   3. 自带的没有密码的移动WIFI
   4. 都不连接

# 社会工程学

1. 以下哪项不属于社会工程学？  **D**
   1. 骗取他人的信任，从而获取有用的信息
   2. 搜集他人的信息，尝试破解他人的账号密码
   3. 冒充某公司的员工或来访人员，混入该公司内部
   4. 通过技术手段拦截他人的电子邮件
2. 社会工程学常被黑客用于  **A**
   1. 口令获取
   2. ARP 攻击
   3. TCP拦截
   4. DDOS攻击
3. 该注意哪项内容，防范社会工程学的攻击  **D**
   1. 不轻易相信陌生人
   2. 收到“领导”的邮件或电话命令，应通过手机或面对面的形式确认命令
   3. 加强信息安全意识教育培训工作
   4. 以上都是

# 口令安全

1. 10. 如下哪项是记住密码的最好方式？  **A**
2. 使用记忆联想游戏或熟悉的短语
3. 告诉可信的人
4. 从来不要更改密码
5. 将密码写下来存放在安全的地方
6. 以下关于口令安全的说法，错误的是 **D**
7. 一般情况下，设置口令时，应保证口令最小长度为6位
8. 最长90天进行一次口令更改
9. 口令应至少包含数字、大小写字母及特殊符号中的任意两种字符
10. 为避免遗忘，应将口令设置为生日、电话号码等容易记忆的内容
11. 下列关于口令持有人保证口令保密性的正确做法是  **D**
12. 将口令记录在笔记本中
13. 将口令贴在计算机机箱或终端屏幕上
14. 将计算机系统用户口令借给他人使用
15. 一旦发现或怀疑计算机系统用户口令泄露，立即更换

# 社交网络安全

1. 社交网站安全防护建议错误的选项是 **D**
2. 尽量不要填写过于详细的个人资料
3. 不要轻易加社交网站好友
4. 充分利用社交网络的安全机制
5. 信任他人转载的信息
6. 在使用社交网站是，遇到他人发来的网络链接，我们应该怎么做？ **D**
   1. “发给我肯定是好玩的，打开看看”
   2. “是同事发的，肯定不会有问题，打开看看”
   3. “这个人不认识，但是我们公司的，可能有事，打开看看”
   4. “是个陌生人，打开有风险，还是不打开了”
7. 社交网站中个人隐私泄露的形式一般有？  **D**
   1. 引导用户填写隐私信息
   2. 诱骗用户填写隐私信息
   3. 数据挖掘
   4. 以上都是

# 数据安全

1. 移动存储介质在使用后，应立即（ ）存储在移动介质中的数据  **D**
2. 保护
3. 备份
4. 检查
5. 清除
6. 使用者应对笔记电脑中的重要数据进行( ) **D**

A. 任意共享

B. 锁屏保护

C. 设置屏保

D. 加密保护

1. 在移动办公时，需要使用到重要数据，应怎么做？ **D**
   1. 开启防病毒软件
   2. 为数据加密
   3. 使用VPN传输
   4. 以上都是

# 无线安全

1. 第三方公司人员到公司洽谈业务，期间向您要公司无线网络的账号密码，您应该怎么做？ **C**
2. 给他一个公用的账号密码
3. 将自己的账号密码告诉他
4. 礼貌的告诉他，公司的无线网络使用需要相应审批申请
5. 让他使用公共电脑上网
6. 以下哪项不是无线网络的安全隐患？  **D**
   1. 网络带宽被盗用
   2. 机密外泄
   3. 危机电脑安全
   4. 覆盖范围小，可能出现连接中断

# 电子邮件安全

1. 为了防止邮箱邮件爆满而无法正常使用邮箱，您认为该怎么做？  **C**

A. 看完的邮件就立即删除

B. 定期删除邮箱的邮件

C. 定期备份邮件并删除

D. 发送附件时压缩附件

1. 可以从哪些方面增强收邮件的安全性 **A**
2. 不断优化垃圾邮件设置、查看邮件数字签名，确认发件人信息、定期更新病毒软件
3. 不断优化垃圾邮件设置、查看邮件数字签名，确认发件人信息、定期更新病毒软件、邮件传输加密
4. 查看邮件数字签名，确认发件人信息、定期更新防毒软件、邮件传输加密
5. 全部不是
6. 确认收件人电子邮件地址，尽量通过直接点击( )、选择通讯录中的联系人等方式选择联系人，在邮件发出之前应再次确认收件人地址，防止误发邮件。  **C**
7. 转发
8. 全部回复
9. 回复
10. 撰写

# 防病毒管理

1. 在防范病毒时，以下哪些活动是不允许的？  **A**
2. 手工停止防病毒软件或卸载防病毒软件
3. 检查OS补丁升级情况
4. 进行病毒升级
5. 进行手工的病毒扫描
6. 以下哪种行为会导致感染或传播病毒？  **B**
7. 关闭不使用的端口
8. 下载并安装未知来源的软件
9. 升级病毒库
10. 安装终端控制软件
11. 员工发现电脑中毒后，应立即（），并马上报告给技术人员  **A**

A. 进行病毒扫描

B. 硬盘格式化

C. 重装操作系统

D. 拨掉网线将其与内网进行隔离

1. 以下哪项工作不能提高防病毒工作的实施效果？  **C**
   1. 及时安装系统补丁
   2. 定期进行漏洞扫描
   3. 对数据加密保存
   4. 加强安全设备的监控和管理

# 信息安全意识

1. 信息安全最大的威胁是？  **C**
   1. 木马病毒、蠕虫病毒等恶意代码
   2. 信息安全部门不作为
   3. 人员普遍缺乏安全意识
   4. 信息安全产品和设备不够先进
2. 私自安装下载的软件有多种危害，以下哪种不是私自安装软件而导致的危险？  **B**
3. 感染病毒
4. 手机丢失
5. 可能涉及到版权，导致法律风
6. 可能被种下木马
7. 以下哪种行为最可能会导致敏感信息泄露？  **A**
8. 打印的敏感文件未及时取走
9. 及时清除使用过的移动介质中的数据
10. 硬盘维修或报废前进行安全清除
11. 企密信息作废时通过碎纸机碎掉
12. 以下哪项是只有你具有的生物特征信息？  **D**
13. 指纹、掌纹、手型
14. 指纹、掌纹、虹膜、视网膜
15. 指纹、手型、脸型、声音、签名
16. 指纹、掌纹、手型、虹膜、视网膜、脸型、声音、签名
17. 小王是某公司的员工，正当他在忙于一个紧急工作时，接到一个陌生的电话：“小王您好，我是系统管理员，咱们的系统发现严重漏洞，需要进行紧急升级，请提供您的账户信息”，他应该\_\_\_\_\_  **C**
18. 配合升级工作，立即提供正确的账户信息
19. 先忙手头工作，再提供账户信息
20. 身份不明确，电话号码认识，直接拒绝
21. 事不关己，直接决绝
22. 如果关系很好的同事问您要很重要的工作资料，您会给吗？  **C**
    1. 直接给
    2. 直接拒绝
    3. 会请示领导再决定是否给
    4. 会问清楚用途，自己决定是否给
23. 如果在打印机边上看到打印的敏感信息，应该怎么做  **D**
    1. 不是我打的，和我没关系
    2. 都没人来拿，我拿回去当草稿纸也好
    3. 直接扔垃圾桶
    4. 稍等片刻，如没人来拿就用碎纸机粉碎