信息安全意识培训试题

（共 200 题，每题 0.5 分，总分 100 分）

姓名：_____ 得分：_____

选择题

一、 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**

A. 通过碎纸机将其碎掉
B. 将其直接扔到垃圾桶
C. 带出办公区送给他人
D. 作为再生纸使用

2. 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

3. 所有的信息资产都可根据()来进行分级 **A**

A. 机密性、完整性和可用性
B. 机密性、真实性和不可否认性
C. 真实性、完整性和不可否认性
D. 破坏性、泄露性和可用性

4. 以下哪项在信息资产管理中不属于数据资产 **C**

A. 机密信息
B. 邮件服务器中保存的邮件
C. 管理制度文档
D. 内部公共信息

5. 以下哪项不是正确的资产责任人的分类？ **D**

A. 资产所有者
B. 资产管理者
C. 资产使用者
D. 资产购买者

6. 资产清单中应包括以下哪些内容？ **D**

A. 资产类型

B. 资产位置
C. 资产价值
D. 全部都是

7. 以下哪项不属于资产管理的四个步骤？ **D**
A. 资产识别
B. 资产评价
C. 资产管理
D. 资产保护

8. 以下哪个资产价值的计算公式是正确的 **A**
A. Round1{Log2[(A×2Conf+B×2Int+C×2Ava)/3]}
B. Round1{Limit0→∞[(A×2Conf+B×2Int+C×2Ava)/3]}
C. Round2{Log2[(A×2Conf+B×2Int+C×2Ava)/3]}
D. Round1{∑ [(A×2Conf，B×2Int，C×2Ava)/3]}

二、 物理安全

9. 以下哪项不在物理安全的防护范围内的？ **D**
A. 机房
B. 办公室
C. 地下停车场
D. 围墙外的花坛

10. 关于物理安全,以下哪种行为是不允许的? **B**
A. 遇到门禁时,主动刷卡
B. 直接尾随进入物理区域
C. 遇到未佩戴标识卡的人时主动进行盘查
D. 佩戴公司身份标识卡

11. 哪个描述是不正确的？ **A**
A. 机房的位置选择应避免处于建筑物的地下、底层或顶层
B. 外部人员进入机房时应经过申请，并得到相关负责任的审批同意，由专人陪同进入
C. 机房地板应铺设防静电地板，并在地板反面涂刷防水涂料
D. 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料.

12. 办公室突然来了不认识的人，应该怎么做？ **D**
A. 不询问，让他自己找要找的人
B. 不询问，但注意着
C. 看情况，不忙的时候询问
D. 主动询问

13. 离开座位时,我们应该( ),将桌面上的敏感资料锁入柜中 **C**
A. 拔除电源
B. 要他人照看电脑

C. 锁定计算机
D. 将显示屏关闭

14. 以下哪项不属于物理安全的保护范围 **D**
A. 防火
B. 防电磁
C. 防雷
D. 防洪水

三、 人员安全

15. 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

16. 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

17. 以下哪种做法不能有效提高员工执行信息安全策略的主动性 **C**
A. 动之以情、晓之以理，加强安全意识培训
B. 提供激励及奖励机制
C. 提供信息安全策略宣贯，以行政命令要求员工遵守信息安全策略
D. 实行处罚措施。

18. 签署保密协议是为了？ **D**
A. 给予员工一种警示
B. 明确员工的保密责任
C. 对员工起到一定的约束作用
D. 以上都是

19. 下列关于保密协议的描述，错误的是？ **B**
A. 保密协议是一种有法律效力的约定
B. 口头协议不能作为保密协议
C. 保密协议分为单方和双方两种
D. 保密协议必须明确保密期限

20. 以下哪个做法是不对的？ **C**
A. “自己的同事进入机房也要进行登记”
B. “客户的项目完成了，应该把给客户开通的零时账号注销了”
C. “汇哲马老师是老朋友了，WIFI 密码告诉他好了，就不用申请了”

D. “无论什么岗位，入职的安全意识培训都是要做的”

四、 应用开发安全

21. 威胁建模以哪 4 个步骤形成循环过程？ **A**

A. 建模，识别威胁，措施，验证措施
B. 建模，识别风险，控制风险，验证措施
C. 识别威胁，识别风险，措施，验证措施
D. 建模，识别威胁，措施，持续改进

22. 以下哪项不是威胁建模的优点？ **D**

A. 在设计的时候,将安全融于设计
B. 更好的理解系统的安全形势
C. 提高开发者在开发过程中对安全的关注
D. 改进整个开发流程的安全

23. 以下哪项不是开发中的安全目标？ **D**

A. 可靠性
B. 可信赖性
C. 健壮性
D. 安全性

24. 在设计开发安全需求时，应考虑哪三项安全属性？ **B**

A. 机密性、完整性、不可抵赖性
B. 机密性、完整性、可用性
C. 完整性、可用性、可追溯性
D. 可追溯性、可用性、不可抵赖性

25. 以下哪项开发项目应将信息安全需求考虑到开发需求中？ **A**

A. 企业内网即时交流系统
B. 文字处理软件单机版
C. 原考勤系统增加自动计时模块
D. 以上全部

26. 开发过程的安全责任人的责任不包括哪项？ **D**

A. 安全策略的执行及跟踪
B. 受理开发人员的问题咨询
C. 安全相关的培训
D. 安全相关的测试

27. 下列哪个环境不属于安全开发环境？ **D**

A. 开发人员所使用的系统
B. 源代码存放的系统
C. 开发人员所在的办公室
D. 开发小组所在的大楼

五、 账号权限安全

28. 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**

A. 会告诉
B. 不会，自己输入
C. 会告诉，第三方使用后自己会更换
D. 会告诉，自己会定期修改

29. 员工使用帐户过程中,哪个是不允许的? **A**

A. 允许 GUEST 帐号存在
B. 使用域帐号
C. 删除不使用的帐户
D. 一人使用一个帐号

30. 应将账号以什么形式进行分类？ **D**

A. 按岗位分
B. 按角色分
C. 按系统分
D. 都不对

31. 账号申请的正确方式应该是？ **C**

A. 申请人本人吃工牌向账号管理部门提出口头申请
B. 申请人本人通过公司邮箱向账号管理部门提出申请
C. 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
D. 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

32. 普通用户账号应多少年审查一次其权限设置是否合理？ **C**

A. 一年
B. 两年
C. 三年
D. 四年

33. 外部人员临时申请账号最多不可超过多久？ **D**

A. 三个月
B. 六个月
C. 十个月
D. 十二个月

六、 笔记本电脑的使用

34. 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

35. 下列关于电脑安全不正确的是？ B
A. 在笔记本电脑交接的时候，清除所有业务数据
B. 私自涂改、拆换笔记本电脑配置与资产编号签
C. 对于报废的笔记本硬盘，进行消磁或物理破坏处理
D. 笔记本电脑需要维修时，将电脑交由综合管理部帮助安全清除其数据

36. 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
A. 放入未加锁侧柜
B. 锁屏
C. 物理加锁
D. 随意放置

37. 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
A. 考虑旅途会无聊，下载了 PPS 播放器缓冲电影
B. 硬盘空间不够了，我删掉点原来的内容
C. 出差前做个数据备份及加密
D. 在机场候机室，笔记本放在身边的座椅上自己睡着了

七、 上网行为规范

38. 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

39. 没有得到明确授权前，可以通过公司网络访问如下哪种外部网络资源( ) C
A. 交友网站
B. 网络游戏
C. 访问公司电子邮件系统
D. P2P 软件

40. 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
A. 不随意下载使用来路不明的文件或程序
B. 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
C. 后缀名为 *.exe、*.rar、*.zip、*.doc 等文件，下载后一定要先杀毒
D. 在浏览网页过程中弹出的插件，都可以直接安装

41. 出差时在机场候机室，应连接以下哪个 WIFI 网络　　D

A. CMCC
B. 任意一个没有密码的 WIFI
C. 自带的没有密码的移动 WIFI
D. 都不连接

42. 在畅游网络时，哪钟做法是不对的？　　C

A. 在社交网站上评论好莱坞艳照门的内容
B. 浏览“房东”事件，并与网友积极讨论
C. 在论坛中向他人索要赌博网站地址
D. 以上都不对

43. 以下哪种行为是正确的？　　D

A. “今天好闲，趁着没人把昨天更新的美剧在线看了”
B. “老婆说晚上想看变形金刚 4，找个资源下下来晚上回去看”
C. “哎呀，公司给我装的这个软件真不好用，我自己去下个新版本的”
D. “中午吃饭的时候把昨天客户发的技术文档下下来，对了限个速，不能影响别人工作”

44. 哪些行为是被允许的　　D

A. 网络嗅探
B. 扫描
C. 传播病毒
D. 授权访问

八、 社会工程学

45. 对于社会工程学，以下哪项描述是不正确的？　　C

A. 社会工程学是利用人们的心理弱点
B. 社会工程学也是一种欺骗的手段
C. 社会工程学的主要目的是破坏
D. 社会工程学是对人的研究

46. 以下哪项不属于社会工程学？　　D

A. 骗取他人的信任，从而获取有用的信息
B. 搜集他人的信息，尝试破解他人的账号密码
C. 冒充某公司的员工或来访人员，混入该公司内部
D. 通过技术手段拦截他人的电子邮件

47. 社会工程学常被黑客用于　　A

A. 口令获取
B. ARP 攻击
C. TCP 拦截
D. DDOS 攻击

48. 该注意哪项内容，防范社会工程学的攻击 **D**

A. 不轻易相信陌生人
B. 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
C. 加强信息安全意识教育培训工作
D. 以上都是

九、 口令安全

49. 多久更换一次计算机的密码较为安全？ **B**

A. 一个月或一个月以内
B. 1——3 个月
C. 3——6 个月
D. 半年以上或从不更换

50. 以下哪种口令不属于弱口令？ **D**

A. 12345678E7
B. Abcdefg
C. AAAAAAA
D. Qw!bydp00dwz1

51. 10. 如下哪项是记住密码的最好方式？ **A**

A. 使用记忆联想游戏或熟悉的短语
B. 告诉可信的人
C. 从来不要更改密码
D. 将密码写下来存放在安全的地方

52. 以下关于口令安全的说法，错误的是 **D**

A. 一般情况下，设置口令时，应保证口令最小长度为 6 位
B. 最长 90 天进行一次口令更改
C. 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
D. 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

53. 为什么需要定期修改密码？ **B**

A. 确保不会忘得密码
B. 降低电脑受损的机率
C. 遵循公司的安全政策
D. 减少他人猜测到密码的机会

54. 下列关于口令持有人保证口令保密性的正确做法是 **D**

A. 将口令记录在笔记本中
B. 将口令贴在计算机机箱或终端屏幕上
C. 将计算机系统用户口令借给他人使用
D. 一旦发现或怀疑计算机系统用户口令泄露，立即更换

十、 社交网络安全

55. 社交网站安全防护建议错误的选项是 D
A. 尽量不要填写过于详细的个人资料
B. 不要轻易加社交网站好友
C. 充分利用社交网络的安全机制
D. 信任他人转载的信息

56. 在使用社交网站是，遇到他人发来的网络链接是，我们应该怎么做？ D
A. “发给我肯定是好玩的，打开看看”
B. “是同事发的，肯定不会有问题，打开看看”
C. “这个人不认识，但是我们公司的，可能有事，打开看看”
D. “是个陌生人，打开有风险，还是不打开了”

57. 社交网站中个人隐私泄露的形式一般有？ D
A. 引导用户填写隐私信息
B. 诱骗用户填写隐私信息
C. 数据挖掘
D. 以上都是

58. 正确的做法是 D
A. 在微博上发表最近正在实施的项目
B. 打开陌生人发来的网络链接
C. 在社交网站上的个人信息中填写公司名称、电话、E-mail 地址
D. 上班时间，不能浏览社交网站

十一、 数据安全

59. 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
A. 保护
B. 备份
C. 检查
D. 清除

60. 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

61. 在移动办公时，需要使用到重要数据，应怎么做？ D
A. 开启防病毒软件
B. 为数据加密

C. 使用 VPN 传输
D. 以上都是

62. 以下哪项数据丢失的风险是一般组织可以接受的？ D
A. 存储数据丢失
B. 通信数据被拦截
C. 内部人员泄漏数据
D. 以上都不

十二、 无线安全

63. 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
A. 给他一个公用的账号密码
B. 将自己的账号密码告诉他
C. 礼貌的告诉他，公司的无线网络使用需要相应审批申请
D. 让他使用公共电脑上网

64. 以下哪项不是无线网络的安全隐患？ D
A. 网络带宽被盗用
B. 机密外泄
C. 危机电脑安全
D. 覆盖范围小，可能出现连接中断

十三、 电子邮件安全

65. 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

66. 可以从哪些方面增强收邮件的安全性 A
A. 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
B. 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
C. 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
D. 全部不是

67. 员工应保证接收所有电子邮件及其附件时首先()。 A
A. 进行病毒扫描
B. 查看正文,再打开附件
C. 转发邮件
D. 直接打开附件

68. 以下哪种电子邮件行为是允许的? D

A. 拦截查看其他用户的电子邮件
B. 进行邮件接龙
C. 发送诽谤邮件
D. 通过电子邮件发送非企密工作邮件

69. 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

A. 转发
B. 全部回复
C. 回复
D. 撰写

十四、 防病毒管理

70. 在防范病毒时，以下哪些活动是不允许的？ A

A. 手工停止防病毒软件或卸载防病毒软件
B. 检查 OS 补丁升级情况
C. 进行病毒升级
D. 进行手工的病毒扫描

71. 以下哪种行为会导致感染或传播病毒？ B

A. 关闭不使用的端口
B. 下载并安装未知来源的软件
C. 升级病毒库
D. 安装终端控制软件

72. 网页病毒主要通过以下哪种途径传播？ C

A. 邮件
B. 文件交换
C. 网页浏览
D. 光盘

73. 发现同事电脑中毒该怎么办？ C

A. 不关我事，继续办公
B. 协助同事查找问题
C. 及时报告给信息安全人员
D. 用 U 盘把同事电脑里面资料拷到自己电脑里

74. 为了更好地防范病毒的发生，以下哪项不是我们应该做的？ A

A. 设置光驱的自动运行功能
B. 定期对操作系统补丁进行升级
C. 安装公司指定的防病毒系统，定期进行升级
D. 使用注册过的可信的 U 盘

75. 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. 拔掉网线将其与内网进行隔离

76. 对防病毒工作的检查不包括以下哪项？ D

A. 防病毒的安装情况
B. 防病毒制度的执行幸亏
C. 病毒事件的处理情况
D. 病毒数量增减情况

77. 以下哪项工作不能提高防病毒工作的实施效果？ C

A. 及时安装系统补丁
B. 定期进行漏洞扫描
C. 对数据加密保存
D. 加强安全设备的监控和管理

十五、 应急演练

78. 应急预案编制完成后，还应确保预案的批准、（）和维护。 B

A. 更新
B. 实施
C. 培训
D. 演练

79. 49、应急演练的基本任务是：检验、评价和（）应急能力。 D

A. 保护
B. 论证
C. 协调
D. 保持

80. 演练的参演人员所承担的具体任务主要包括（）。 C

A. 保护财产或公众健康
B. 获取并管理各类应急资源
C. 与其他应急人员协同处理重大事故或紧急事件
D. 扮演、替代正常情况或响应实际紧急事件时应与应急指挥中心、现场应急指挥所相互作用的机构或服务部门

十六、 信息安全意识

81. 信息安全最大的威胁是？ C

A. 木马病毒、蠕虫病毒等恶意代码

B. 信息安全部门不作为
C. 人员普遍缺乏安全意识
D. 信息安全产品和设备不够先进

82. 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
A. 感染病毒
B. 手机丢失
C. 可能涉及到版权，导致法律风
D. 可能被种下木马

83. 以下哪种行为最可能会导致敏感信息泄露？ A
A. 打印的敏感文件未及时取走
B. 及时清除使用过的移动介质中的数据
C. 硬盘维修或报废前进行安全清除
D. 企密信息作废时通过碎纸机碎掉

84. 浏览器存在的安全风险主要包括： D
A. 网络钓鱼、隐私跟踪
B. 网络钓鱼、隐私跟踪、数据劫持
C. 隐私跟踪、数据劫持、浏览器的安全漏洞
D. 网络钓鱼、隐私跟踪、数据劫持、浏览器的安全漏洞

85. 以下说法错误的是 ？ B
A. 需要定期更新 QQ 软件
B. 可以使用非官方提供的 QQ 软件
C. 不在合作网站轻易输入 QQ 号
D. 完善保密资料，使用保密工具

86. 以下哪项是只有你具有的生物特征信息？ D
A. 指纹、掌纹、手型
B. 指纹、掌纹、虹膜、视网膜
C. 指纹、手型、脸型、声音、签名
D. 指纹、掌纹、手型、虹膜、视网膜、脸型、声音、签名

87. 禁止从事与本职工作不相关的活动，以下哪项是与本职工作相关的活动？ B
A. 使用公司电子邮箱在工作时间从事私人活动
B. 在网上查找与工作相关的资料
C. 使用公司电子邮箱在工作时间从事私人活动
D. 使用私人邮箱发送私人邮件

88. 以下哪种行为存在安全隐患？ B
A. 出入公司时，观察是否存在陌生人随尾
B. 在电梯内与同事高声谈论工作
C. 使用移动介质后及时清除存储在移动介质的资料
D. 复印后的资料及时取走

89. 信息安全的基本属性是？ D

A. 保密性
B. 完整性
C. 可用性
D. A，B，C 都是

90. 下面关于使用公共电脑的叙述中错误的是 D

A. 不在未安装杀毒软件的公共电脑上登录个人账户
B. 不在网吧等公共电脑上使用网上银行
C. 离开电脑前要注销已登录的账户
D. 在公共电脑中存放个人资料和账号信息

91. 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

A. 配合升级工作，立即提供正确的账户信息
B. 先忙手头工作，再提供账户信息
C. 身份不明确，电话号码认识，直接决绝
D. 事不关己，直接决绝

92. 目前，部分公司禁止员工上班时间浏览微博，同时禁止发布和工作相关的微博，针对此规定，您的看法是？ A

A. 公司应该禁止员工任意发布涉及工作内容、公司文化等相关内容的微博
B. 微博为每个人同了自由的言论平台，微博属于个人行为，公司无权限制员工的言论自由
C. 工作时间可以限制，但是下班后是个人时间，公司部应该再限制员工的作为
D. 微博是每个人发表自己心情、抒发情怀，散步情绪的地方，难免设计工作内容，并且网络时个虚拟空间，每个人的身份也不一定是真实的，所以并不会直接影响企业的信息安全

93. 不符合安全意识的选项是： D

A. 使用物理加锁的方式防止笔记本丢失
B. 对笔记本电脑中的重要数据进行加密保护，以防丢失泄密
C. 安装公司指定的防病毒软件
D. 下载未知来源的文件

94. 当您准备登录电脑系统时，有人在您的旁边看着您，您将如何： B

A. 在键盘上故意假输入一些字符，以防止被偷看
B. 友好的提示对方避让一下，不要看您的机密
C. 不理会对方，相信对方是友善和正直的
D. 凶狠地示意对方走开，并报告这人可疑

95. 哪项没有安全的使用个人电脑？ （ ） D

A. 设置操作系统登录密码，并开启系统防火墙
B. 安装杀毒软件并及时更新病毒特征库
C. 尽量不转借个人电脑
D. 在未安装杀毒软件的电脑上登录个人帐户

96. 对于计算机备份，正确的是 C

A. 不备份
B. C 盘比较重要，我只备份 C 盘
C. 定期进行数据备份
D. 用的是自己的电脑，就备份自己的资料

97. 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

A. 直接给
B. 直接拒绝
C. 会请示领导再决定是否给
D. 会问清楚用途，自己决定是否给

98. 如果在打印机边上看到打印的敏感信息，应该怎么做 D

A. 不是我打的，和我没关系
B. 都没人来拿，我拿回去当草稿纸也好
C. 直接扔垃圾桶
D. 稍等片刻，如没人来拿就用碎纸机粉碎

99. 下班离开前应 D

A. 直接离开
B. 关闭电脑后离开
C. 锁定电脑，并检查文件是否保存好了
D. 关闭电脑，将办公桌整理干净，文件上锁保存

100. 以下哪种观念是正确的 C

A. 信息安全是信息安全部门的事，和我无关
B. 信息安全是技术活，我只要配合技术部门就好
C. 信息安全应该从自己做起，不仅要配合相关部门，还应该积极学习相关知识
D. 买了那么多信息安全产品，信息安全工作绝对做的很好了。

是非题（√或×）

1. 在人员离开电脑前，应将计算机锁定 √
2. 办公环境安全是物业保安部的事，和信息安全无关 ×
3. 密码越复杂越好 ×
4. 电话诈骗也是社会工程学的一种方法 √
5. 在外工作连上网络就可以直接访问公司内网了 ×
6. 北方天气干燥，机房不需要控制湿度 ×
7. 自己公司的员工出入机房，没有登记也没关系 ×
8. 公司应用系统都在内网，人员离职不需要回收其访问权限，反正他也访问不到内网 ×
9. 汇哲的老师是非常熟悉的合作伙伴了，来访就不需要登记了 ×
10. 人员调岗时，不仅要变更其岗位角色，还要变更其账户权限 √
11. 信息安全是信息安全部门的事，应用开发人员在开发设计阶段不需要考虑信息安全功能 ×
12. 开发人员所处的办公环境也属于安全开发环境保护范围之内 √

13. 开发人员在编写代码是必须遵守编码规范 √
14. 安全设计原则是安全设计中的一部分，根据已定的安全设计原则进行设计，能够为之后的具体开发过程打下良好的安全基础 √
15. 安全目标通常从保密性、完整性及可用性三个方面去考虑 ×
16. 威胁建模师以预防和验证功能为中心 ×
17. 威胁建模也不能解决一些现实上的缺陷，如：缓冲区溢出、内存泄露及过时的数据库等 √
18. 安全漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷 √
19. 产品测试过程中的安全测试应由专人负责 √
20. 系统维护阶段修复漏洞的代价就是需求阶段的 200 倍 √
21. 软件安全开发流程分为 5 个步骤：准备—需求—设计—编码---测试 ×
22. 设计安全需求时，主要针对信息资产的机密性、完整性及可用性进行规划设计 ×
23. 根据账号的不同分类应制定不同的定期审阅策略，高权限账号每半年审阅一次 ×
24. 笔记本的基础安全措施有三点，杀毒软件，系统升级及账户密码 √
25. HDD 密码只要换了内存就没用了 ×
26. 只要数据有备份，笔记本电脑丢了也没什么太大关系 ×
27. 杀毒软件只能清除已经感染的病毒，并不能起到屏蔽作用 ×
28. TRM 芯片与 BIOS 密码是相辅相成的 √
29. 在使用人员离开笔记本时，需锁定电脑屏幕 √
30. 公司笔记本电脑坏了，应及时保修，避免影响正常工作 ×
31. 在公共场所应使用 VPN 连接办公网络，在自己家里是不需要的 ×
32. 购物是女性的天性，女性在上班访问购物网站是应该允许的 ×
33. 工作中有个不常用的软件需要下载使用，应该用最大带宽下载速度下载，减少影响他人正常上网的时间 ×
34. 好莱坞女星的艳照门，大家都在下，我也下个看看 ×
35. “听说太平洋保险汽车报废最低只要一元”——某论坛发帖 ×
36. 社会工程学是把对物的研究方法全盘运用到对人本身的研究上，并将其变成人为控制的工具 ×
37. 社会工程学说白了就是使用各种手段欺骗
38. 反向社会工程学是指攻击者通过技术或者非技术的手段给网络或者计算机应用制造“问题”，使其公司员工深信，诱使工作人员或者网络管理人员透露或者泄漏攻击者需要获取的信息。 √
39. 安全审核工作是社会工程学攻击防范主要手段之一 √
40. 含有恶意代码的软件也是社会工程学的手段之一 √
41. 数据的威胁不包括被破坏，因为恢复被破坏的数据的方法有很多 ×
42. 在远程办公时使用 VPN 连接，可以保障数据传递过程中的完整性和可用性 √
43. 数据是无形的，不能定义其价值 ×
44. 数据只要使用复杂的加密就可以了，不用设置访问权限 ×
45. 自然灾害并不是数据的主要威胁之一 √
46. 只要把无线网络的 SSID 隐藏了，密码复不复杂就无所谓了，反正别人也看不到 ×
47. 无线网络就是为了方便大家的移动设备上网，所以范围一定要大 ×
48. 使用无线网络的很多设备都不是公司的资产，难以控制，所以无线网络一定不能访问公司内部网络 ×
49. 凡是未经用户许可就强行发送到用户的邮箱中的任何电子邮件都可称为垃圾邮件 √
50. 垃圾邮件的主要危害是占用网络带宽，并不会对信息数据造成危害 ×
51. 回复邮件应直接使用“回复”功能，防止误发邮件； √

52. 在外办事自己的电脑没带，可借用同时的邮箱收发邮件 ×
53. 在接受邮件附件时，应先将附件下载到本地，再用防病毒软件对附件进行扫描，确认无误后方可打开 ×
54. 为了方便处理一些个人事宜，可以将公司邮箱留给他人，方便在上班时间联系。 ×
55. 防病毒软件工作都是自动的，不需要多余的人员管理 ×
56. “防病毒软件是 IT 部门给装的，我又不懂这种技术的东西，平时没我什么事” ×
57. 系统安装补丁更新和防病毒工作没有直接关系 ×
58. BYOD 设备的越狱和提权可以使得设备安装原本收费的安全防护软件，对 BYOD 的安全十分有帮助 ×
59. BYOD 设备很容丢失，不应将私密信息存放其中 ×
60. 一个 APP 游戏需要访问通讯录，因为十分想玩只好妥协 ×
61. BYOD 设备一直在自己的身边，而且经常要用，不用麻烦的设置解锁密码 ×
62. 我的 IPHONE 又要更新系统了，每次更新都用的不顺手，再也不更新了 ×
63. BYOD 属于个人设备，企业不应该管制 ×
64. 信息安全是国家安全的组成部分 √
65. 信息安全受到刑罚的约束 √
66. 企业信息安全是企业正常运行的重要保障。 √
67. 完善、合理的信息安全工作，能够帮助企业提高核心竞争力 √
68. 企业信息安全最主要的威胁来自黑客 ×
69. 在目前的信息安全工作中，大多数的管理或技术人员都选择使用后期补救的安全漏洞解决方法 √
70. 定义资产责任人的目的是使信息资产的管理具体落实到人，并且通过具体职责的界定，使信息资产的价值得到有效保证 √
71. 资产清单应包括所有为从灾难中恢复 而需要的信息，包括资产类型、格式、位置、备份信息、许可信息和业务价值 √
72. 信息资产的管理者应对信息资产进行合理的安全等级标识 √
73. 对于同类型资产应采用同样的资产标识 ×
74. 敏感及重要信息资产的管理应符合国家及行业法律法规的要求 √
75. 应急演练应至少每年进行一次 √
76. 在发现自己能处理的安全事件时，启动应急响应太麻烦了，可以自己解决就自己解决，不用汇报，以免将小事扩大 ×
77. 在启动应急响应程序时，应有专人向相关部门或人员发送通知 √
78. 在应急响应程序结束后，应由职能和业务部门负责系统及功能测试 √
79. 信息安全事件应分级处理 √
80. 信息安全意识培训应该只针对 IT 人员，业务人员不需要 ×
81. 信息资产的分类主要依据为机密性、完整性及可用性 ×
82. 使用公司邮箱地址在外部网站中注册是不安全的行为 √
83. 为了加强企业在互联网中的宣传，可以将公司的客户信息、重要战略目标等放在社交网络上。 ×
84. 发现计算机感染了病毒后，首先应的的是立即拔掉网线，防止再次感染。 ×
85. 数据应定期备份，可以选择全备份，也可以选择增量备份 ×
86. 业务操作人员需要经常对系统进行一定的修改，可以给其系统管理员的权限，提高工作效率。 ×
87. 打印错的合同或协议应该及时扔进垃圾桶处理 ×
88. 使用了 VPN，就不会因为远程连接服务器而导致服务器感染病毒 ×
89. 应该设置一个较为复杂的密码防止被黑客破解，如果记不住可以写在自己 ×

的笔记本上

90. “为保证密码不会被黑客猜解，我决定每周更换一次密码” ×
91. 为了更好的保护 BYOD，应该破解 BYOD 系统的管理员权限，使得个人拥有控制权 ×
92. “领导邮箱发来的 exe 文件，说需要安全测试，先装来看看” ×
93. 无线网络时需要频繁使用的，定期更换密码不方便大家的使用，所以不用定期更换 ×
94. 机房的大楼是新造的，楼顶的避雷针完全能够保护机房遭受雷击的威胁。 ×
95. “领导让我把备份介质锁起来，公司正好有个不用的带锁木质书柜，就锁里面好了” ×
96. “机房如果发生严重的火灾，应立即拨打 119，切断电源，并执行应急响应，切换到备用系统中” √
97. 每个产品都有安全漏洞，就连微软的 windows 系统都有，我们的产品有些小漏洞不用放在心上，只要事后能够补救就行。 ×
98. 安全设计需要变更时，应遵守变更控制规则，并且要有安全方面的人员跟踪与审查，安全方面的人员需要评估变更是否影响现有的威胁和防御措施。 √
99. 社会工程学都是基于人的攻击，网络这种虚拟环境中不会发生 ×
100. 信息安全意识的提高可以避免人员违规操作的发生，有利于信息安全工作的展开。 √