湖南科技大学考试试题纸（ A 卷）

（ 2019 － 2020 学年度第 1 学期）

课程名称: 信息安全管理 开课单位: 计算机学院 命题教师: 李章兵

授课对象: 计算机 学院 16 年级 信安 1-3 班

考试时量: 100 分钟 考核方式: 考试 考试方式: 闭卷

审核人: 审核时间: 年 月 日

一、判断题 (本题共 20 分, 每小题 2 分)

1. 信息安全保障阶段中，安全策略是核心，对事先保护、事发检测和响应、事后恢复起到了统一指导作用。（ ）

2. 一旦发现计算机违法犯罪案件，信息系统所有者应当在 2 天内迅速向当地公安机关报案，并配合公安机关的取证和调查。 （ ）

3. 我国刑法中有关计算机犯罪的规定，定义了 3 种新的犯罪类型 （ ）

4. 虽然在安全评估过程中采取定量评估能获得准确的分析结果，但是由于参数确定较为困难，往往实际评估多采取定性评估，或者定性和定量评估相结合的方法。 ( )

5. 信息设备到期报废、淘汰处置或改为他用时，应当清除存储在设备中的信息。（ ）

6. “资产责任人”是指有权限变更资产安全属性的人。( )

7. 所有员工应该发现并报告安全方面的漏洞或弱点以及安全事件。（ ）

8. 系统备份与普通数据备份的不同在于，它备份系统程序、应用程序、参数配置以及数据，以便迅速恢复系统运行。（ ）

9. 保护关键业务过程免受信息系统失误或灾难的影响，应定义恢复的优先顺序和时间指标。（ ）

10. 《网络安全法》是 2017 年 1 月 1 日起正式施行。（ ）

二、选择题 (本题共 30 分, 每小题 2 分，必要时多选)。

1. 信息安全经历了三个发展阶段，以下( )不属于这三个发展阶段。
A. 通信保密阶段 B. 加密机阶段 C. 信息安全阶段 D. 安全保障阶段

2. 风险评估过程中的预防性控制措施是（ ）。
A. 强制访问控制 B. 告警 C. 审核活动 D. 入侵监测方法

3. 在建立信息安全管理体系时，首先应该做的事情是（ ）。
A. 风险评估 B. 建立信息安全方针和目标
C. 风险管理 D. 制定安全策略

4. 信息安全管理体系是 PDCA 动态持续改进的一个循环体。下面理解不正确的是(　　)。
A. 组织中的每个部分或个人，均可以 PDCA 循环，大环套小环，一层一层地解决问题。
B. 推动 PDCA 循环，关键在 P 这个计划阶段。
C. 每通过一次 PDCA 循环，都要进行总结，提出新目标，再进行第二次 PDCA 循环。
D. 按顺序进行，它靠组织的力量来推动，像车轮一样向前进，周而复始，不断循环。

5. 涉及国家秘密的计算机信息系统，必须 (　　) 。
A. 实行物理隔离　　B. 实行逻辑隔离　　C. 实行单向隔离　　D. 以上都不是

6. 移动存储介质的管理和使用应防止（　　）。
A. 信息失效　　B. 病毒危害　　C. 公私混用　　D. 遗失、被盗

7. 计算机机房装修材料应符合 GB 50016《建筑设计防火规范》，选择（　　）。
A. 难燃、非燃材料　　B. 防潮、防起尘材料
C. 吸音、抗静电材料　　D. 防辐射材料

8. 电源是计算机网络系统的命脉，计算机机房后备电源应选择(　　)。
A. UPS　　B. 发电机　　C. 蓄电池　　D. 干电池

9. 计算机机房应安装(　　)。
A. 门禁、影像监控系统　　B. 温度、湿度监控系统
C. 防火、 防水、防潮系统　　D. 以上都是

10. 窃听技术是在窃听活动中使用的窃听设备和窃听方法的总称。不用中继技术窃听距离最远的技术是(　　)。
A. 谐波无线窃听　　B. 微波窃听　　C. 激光窃听
D. 电话窃听　　E. 定向麦克风　　F. 外墙音频放大器

11. 窃照装置也越来越多样化、微型化，下面（　　）属于窃照装置。
A. 可伸缩光学窥镜　　B. 电视窥视录像机
C. 微光电视录像机　　D. 光纤窥视系统

12. 对于信息安全管理中的人力资源安全，以下理解不正确的是（　　）。
A. 上岗前要对担任敏感和重要岗位的人员要考察其以往的违法违规记录
B. 雇佣中要有及时有效的惩戒措施
C. 出了事故后要有针对性地进行信息安全意识教育和技能培训
D. 离职人员要撤销其访问权限

13. 信息安全的符合性检查不包括（　　）
A. 法律法规符合性　　B. 技术标准符合性
C. 安全策略符合性　　D. 内部审核活动

14. 计算机信息系统安全等级保护的等级是由 (　　) 确定。
A. 计算机信息系统面临的风险
B. 计算机信息系统资源的经济和社会价值及其面临的风险
C. 计算机信息系统价值

D. 以上都不是

15. 业务连续性管理 (BCM) 的原则是预防为先，恢复为后，其中预防的目的是(　　)。

A. 减少威胁的可能性　　B. 保护企业的弱点区域

C. 减少灾难发生的可能性　　D. 防御危险的发生并降低其影响

三、简答题 (本题共 20 分, 每小题 10 分)。

1. 请列举信息安全风险的七大要素，并详细说明这七大风险要素之间的相互关系。

2. 简述信息安全管理中人员安全管理的三大基本原则，并进行相应的解释。

四、综合分析题 (本题共 30 分, 每小题 15 分)。

1. 查某公司设备资产，负责人说台式机放在办公室，办公室做了来自环境的威胁的预防；笔记本经常带入带出，有时在家工作，领导同意了，在家也没什么不安全的。请从信息安全管理上分析。

2. 假设您是某企业的 CIO，请就本单位的人员使用、升迁或离职、新员工招聘谈谈如何进行信息安全管理。

附加题：（10 分）

请就手机 APP 的下载、安装和使用过程中要求用户同意软件读取通信录、位置跟踪、手机照片等信息，以及自动云备份，谈谈如何进行信息安全管理。

湖南科技大学考试试题参考答案及评分细则

（2019-2020 学年度第 一 学期）

课程（A 卷） 信息安全管理 **上课学院** 计算机学院 **班级** 2016 级信息安全 1-3 班

应试学生人数 97 **实际考试学生人数** _____ **考试时量** 100 **分钟**

命题教师 李章兵 **审核人** _____ **考试时间：** 年 月 日

一、判断题 (本题共 20 分, 每小题 2 分)

1-5 ××× √ √ 6-10 √ √ √ √ ×

二、单项选择题 (本题共 30 分, 每小题 2 分)。

1-5 BDBBA 6-10 ABCD，ABCD，A，ABC(D)， A 11-15 ABCD，B，D，B，C

三、简答题 (本题共 20 分, 每小题 10 分)

1. 答: 信息安全风险的七大要素包括资产、威胁、脆弱点、风险、影响、安全措施和安全需求。它们之间的关系如下:
   (1) 威胁利用脆弱点将导致风险的产生;
   (2) 资产具有价值, 并对组织业务有一定的影响, 资产价值及影响越大则其面临的风险越大;
   (3) 安全措施能抵御威胁、减少脆弱点, 因而减少安全风险;
   (4) 风险的存在及对风险的认识导出安全需求, 安全需求通过安全措施来满足或实现。
2. 答: 人员管理的三大基本原则是
   (1) 多人负责原则，即每一项与安全有关的活动，都必须有两人或更多人在场；
   (2) 任期有限原则，任何人最好不要长期担任与安全有关的职务，以保持该职务具有竞争性和流动性；
   (3) 职责分离原则，出于对安全的考虑，科技开发、生产运行和业务操作都应当职责分离。

四、综合分析题 (本题共 30 分, 每小题 15 分)

1. 参考答案

主要观点：组织场所外的设备安全，应对组织场所的设备采取安全措施，要考虑工作在组织场所以外的不同风险。

1. 笔记本带出办公室，有丢失、被非法访问风险；采取随身锁的安全措施；
2. 在家里使用，有感染病毒、泄露单位重要文件信息的风险；采取隔离家庭网络或防火墙、杀毒防护措施；
3. 染毒的笔记本带回办公室，有交叉感染办公室台式电脑的风险，有交叉拷贝数据文件被泄露的风险；采取严格的杀毒与隔离措施。

2. 参考答案

见课件 PPT 第 4 章（2），课本 106-112

分：内部人员分级授权，升迁、离职人员的授权变更、新员工安全培训等阐述

对于内部工作人员，采取分级授权访问控制措施，对于敏感数据和文件进行分级管理；

员工升迁后，将收回设备、系统 ID 并根据级别重新授权；

员工离职后，收回设备或由技术主管销毁设备上的信息，收回系统 ID 及其访问权限；

新员工入职：对员工进行信息安全培训，对应级别进行访问授权。

附加题（10 分）

自由发挥，酌情加分。