湖南科技大学考试试题纸（ A 卷）

（ 2021 － 2022 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 18 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. 信息安全策略的制定和维护中，最重要的是要保证其明确性和相对稳定性。（ ）

3. 安全风险评估过程中由于参数确定较为困难，实际往往多采取定性评估，或者定性和定量评估相结合的方法。 ( )

4. 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。（ ）

5. 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。（ ）

6. 信息安全领域内最关键和最薄弱的环节是技术和管理制度。（ ）

7. 灾难恢复计划或者业务连续性计划关注的是信息资产的可用性属性。（ ）

8. 系统备份是备份系统程序、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. 信息系统安全定级应由业务信息安全和系统服务安全两方面确定。（ ）

二、选择题 (本题共 30 分, 每小题 2 分)。

1. 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

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. 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. 推动 PDCA 循环，关键在 P 这个计划阶段。

B. 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。

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。

4. 在策略生命周期中，以下哪个是正确的：(　　)
A. 需求分析、制定、发布、推行、审核、废除
B. 制定、发布、推行、审核、修订、废除
C. 需求分析、制定、发布、推行、审核、修订
D. 需求分析、制定、发布、推行、审核、修订、废除

5. 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

6. 物理安全包括（　）
A. 设备安全、介质安全、系统安全、环境安全
B. 设备安全、系统安全、环境安全、人员安全
C. 设备安全、介质安全、环境安全、人员安全
D. 设备安全、网络安全、环境安全、系统安全

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. 吸音、难燃、非燃材料　　B. 防潮、防起尘材料
C. 抗静电材料、防辐射材料　　D. 以上都是

8. 区域安全管理中下面错误的描述是（　　）
A. 安全区域保护可采用围墙和门控，警卫、智能锁、电子监视和警报系统都是适当措施。
B. 隔离送货区域、装载区域、信息处理设施，控制授权访问。
C. 敏感信息处理设施的位置标示引人注目，安装监控。
D. 来访人员进入需要审批并记录。

9. 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. 定向麦克风　　B. 微波窃听　　C. 激光窃听
D. 电话窃听　　E. 谐波无线窃听　　F. 外墙音频放大器

10. 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. 离职人员要撤销其访问权限；
C. 雇佣中要有及时有效的惩戒措施；
D. 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。

11. 应急响应是组织为应对各种意外事件的发生所做的准备和采取的措施，方法顺序（ ）
A. 准备、检测、抑制、根除、恢复、跟踪
B. 准备、跟踪、检测、抑制、根除、恢复
C. 准备、检测、跟踪、抑制、恢复、根除
D. 准备、抑制、根除、恢复、检测、跟踪

12. 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. 减少灾难发生的可能性

C. 保护企业的弱点区域　　D. 防御危险的发生并降低其影响

13. 自主访问控制 DAC 和强制访问控制 MAC 的描述错误的是（　　）

A. DAC 允许合法用户以用户或组的身份访问策略规定的客体；

B. DAC 允许用户自主授权自己拥有的客体的访问权限给其他用户；

C. MAC 中的主体和客体都有带偏序关系的安全等级标记；

D. MAC 是一种多级访问控制策略，客体的访问权限由操作系统决定。

14. 信息安全等级保护工作的主要内容包括五个方面（　　）。

A. 策略、管理制度、技术、设备、测评

B. 定级、备案、测评、建设整改、检查

C. 定级、策略、设备、测评、检查

D. 策略、定级、备案、测评、建设整改

15. 信息系统安全等保定级时考察的受侵害客体是（　　）。

A. 公民、法人和其他组织的合法权益　　B. 社会秩序、公共利益

C. 国家安全　　D. 以上都是

三、问答题 (本题共 40 分, 每小题 10 分)。

1. 什么是信息安全管理体系 ISMS？建立 ISMS 分哪几步骤？（8’）
2. 简述信息安全风险的七大要素，并画图说明要素之间的相互关系。（10’）
3. 信息系统生命周期包括哪 5 个阶段？信息系统安全等级分哪几级？（10’）
4. 信息系统安全等保测评的目的是什么？如何确定其安全等级？试画出安全等级矩阵表。（12’）

四、综合分析题 (本题共 10 分)。

假设您是某组织的 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，以及共享充电、公共 WIFI 的使用谈谈如何进行信息安全管理。