湖南科技大学考试试题纸（A 卷）

（2018-2019 学年度第一学期）

课程名称: 信息安全管理 **开课单位:** 计算机科学与工程学院 **命题教师:** 李雄

授课对象: 计算机科学与工程 **学院** 2015 **年级** 信息安全 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:** 2018 **年** 10 **月** 29 **日**

一、填空题 (本题共 10 分，每空 1 分)。

1. 信息安全威胁主要源于三个方面，即_____、_____和人的因素。
2. TCP/IP 体系结构中包含了四个功能层，从下到上分别是_____、_____、传输层和应用层。
3. 常见的不间断电源 (UPS) 包括持续供电型 UPS、_____、_____和逆向转换型 UPS。
4. 信息安全审计的作用与功能包括取证、_____、_____和发现系统运行异常等。
5. 数据备份是数据恢复和目标重建的重要基础，根据备份策略来说可以将数据备份方式分为_____、增量备份、_____和综合性完全备份。

二、单项选择题 (本题共 30 分，每小题 3 分)。

1. 下面哪项是风险评估过程中的预防性控制措施_____。

   A. 强制访问控制　　B. 告警

   C. 审核活动　　D. 入侵监测方法

2. 计算机病毒通常是_____。

   A. 一条命令　　B. 一个文件

   C. 一个标记　　D. 一段程序代码

3. 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

4. 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

5. 信息安全管理体系是 PDCA 动态持续改进的一个循环体。对于 PDCA 循环的特点，以下理解不正确的是_____。

A. 组织中的每个部分，甚至个人，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

6. 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

7. 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

8. 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

9. 通用准则 CC 标准分为三个部分，以下不属于这三部分的是_____。

A. 简介和一般模型　　B. 安全保证要求

C. 安全功能要求　　D. 保密性要求

10. 下面_____是信息安全类的法律法规。

A. 网络安全法　　B. 邮政法

C. 统计法　　D. 气象法

三、判断题 (本题共 10 分，每小题 2 分)

1. IP 协议数据流采用的是密文传输,所以信息很容易被在线窃听、篡改和伪造。 (　　)
2. DOS 是一种既简单又有效的进攻方式，其目的就是拒绝用户的服务访问，破坏系统的正常运行，最终使用户的部分 Internet 连接和网络系统失效，甚至系统完全瘫痪。 (　　)
3. 网络边界保护中主要采用防火墙系统，在内网和外网之间存在不经过防火墙控制的其他通信连接，不会影响到防火墙的有效保护作用。 (　　)
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. DNS 对于自己无法解析的域名将会直接拒绝服务。 (　　)

四、简答题 (本题共 50 分，每小题 10 分)。

要求：所有题目需回答详尽。

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 TCP 三次握手的过程及可能遭受的攻击。
3. 信息系统安全问题中最核心的问题是管理问题，而其中“人”的管理尤为复杂。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。
4. 防火墙具有哪些主要功能? 防火墙存在的局限性主要有哪些?
5. 口令认证 (Password authentication) 方式因其简单易用被广泛应用于各种信息系统中，但口令管理不当会带来很大的安全隐患。根据所学的信息安全知识，请你设计一套口令管理的基本原则。