

2021年软考-中级 系统集成项目管理工程师 基础精讲班

-20安全管理



讲师:朱建军 (江山老师)





第 17 章：信息系统安全管理（2 分）

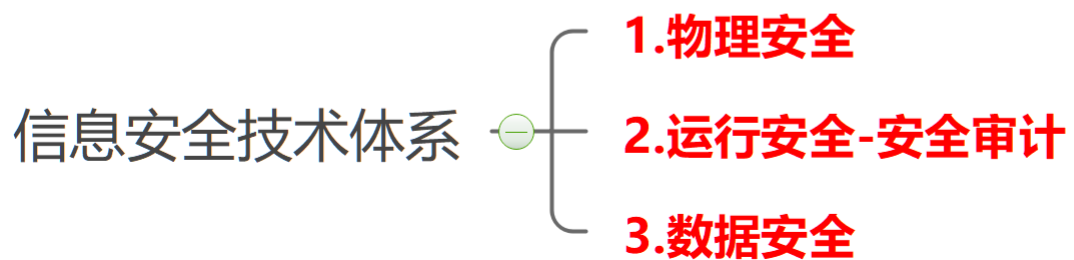
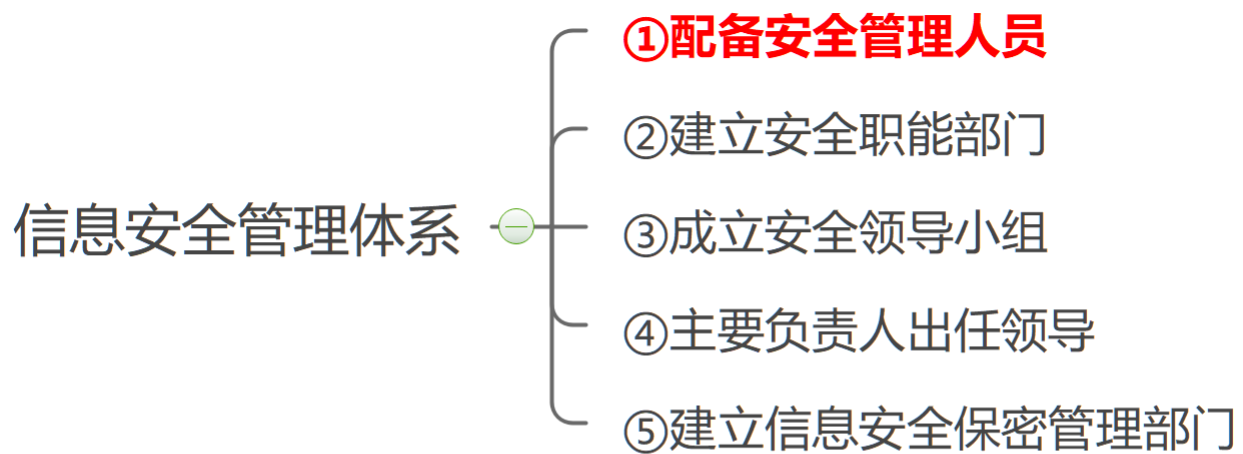
| 分值 年份 考点情况 | 09 上 | 09 下 | 10 上 | 10 下 | 11 上 | 11 下 | 12 上 | 12 下 | 13 上 | 13 下 | 14 上 | 14 下 | 15 上 | 15 下 | 16 上 | 16 下 | 17 上 | 17 下 | 18 上 | 18 下 | 19 上 | 19 下 | 20 下 |
|------------------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| 1、信息安全属性/技术 | 1 | | | | | 1 | | 1 | | 1 | | | | 1 | 1 | | 1 | | 1 | | | 1 | 1 |
| 2、数据完整性机制 | | 1 | | | | | | | | | | | | | | | | | | | | | |
| 3、系统安全/保密层次 | | 1 | 1 | 1 | | | 1 | | 1 | | | | 1 | | | | | 1 | 1 | | 1 | | |
| 4、人员物理应用安全 | | 1 | | 1 | | 1 | | | | | 1 | | 1 | | 1 | | | | 1 | 1 | | 1 | 1 |
| 5、信息安全技术/管理体系 | | | | | | 1 | 1 | | | | 1 | | 1 | | | | | | | | | | |
| 6、访问控制内容步骤 | | | 1 | | | | | | | 1 | | | | 1 | | | | | | | | | |
| 7、信息安全等级 | | | | | 1 | | | 1 | | | | | | 1 | | | 1 | | | 1 | | | |
| 8、安全措施/风险评估 | | | | | 2 | | 1 | | | 1 | 1 | | | 1 | | | | | | | 1 | | |
| 9、MD5 | | | | | | | | | | 1 | | | | | | | | | | | | | |
| 10、加密 | | | | | | | | | | | | | 1 | 1 | | | | | | | | | |
| 11、信息安全管理部門 | | | | | | | | | | | | | | | | | | 1 | | | | | |
| 总的分值 | 1 | 3 | 2 | 2 | 3 | 3 | 3 | 2 | 1 | 4 | 3 | | 4 | 5 | 2 | | 2 | 2 | 3 | 2 | 2 | 2 | 2 |

学习建议：信息安全管理内容比较杂，需要把教程认真去看下，可能是难点，尽量得分

| | | |
|------|-----------------|------|
| 信息安全 | 安全属性的定义、机房防静电方式 | 19 下 |
|------|-----------------|------|

信息安全属性及目标

- 1. 保密性  { 信息不被泄漏给**未授权**的个人、实体和过程或不被其使用的特性
技术：①**最小授权原则** ②**防暴露** ③**信息加密** ④**物理保密**
- 2. 完整性  { 信息未经授权不能进行改变的特性。即应用系统的信息在存储或传输过程中保持不被偶然或蓄意地**删除、修改、伪造、乱序、重放和插入等破坏和丢失的特性**
技术：①**协议** ②**纠错编码方法** ③**密码校验和方法** ④**数字签名** ⑤**公证**
- 3. 可用性  — 应用系统信息**可被授权实体访问并按需求使用**的特性。即信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性
- 4. 不可抵赖性  — 也称作**不可否认性**，在应用系统的信息交互过程中，确信参与者的真实同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺



机房场地选择

机房空调、降温

- ①基本温度要求 — 应有必要的空调设备，使机房温度达到所需的温度要求
- ②较完备空调系统 — 应有较完备的中央空调系统
- ③完备空调系统

机房防静电

- 1.接地与屏蔽 — 采用必要的措施，使计算机系统有一套合理的防静电接地与屏蔽系统
- 2.服装防静电 — 人员服装采用**不易产生静电的衣料**，工作鞋采用**低阻值材料**制作
- 3.温、湿度防静电 — 控制机房温、湿度，使其保持在不易产生静电的范围内
- 4.地板防静电 — 机房地板从表面到**接地系统的阻值**，应控制在不易产生静电的范围内
- 5.材料防静电 — 机房中使用的各种家具，如工作台、柜等，应选择**产生静电小的材料**
- 6.维修MOS电路保护 — 在硬件维修时，应采用**金属板台面的专用维修台**，以保护MOS电路

机房接地防雷

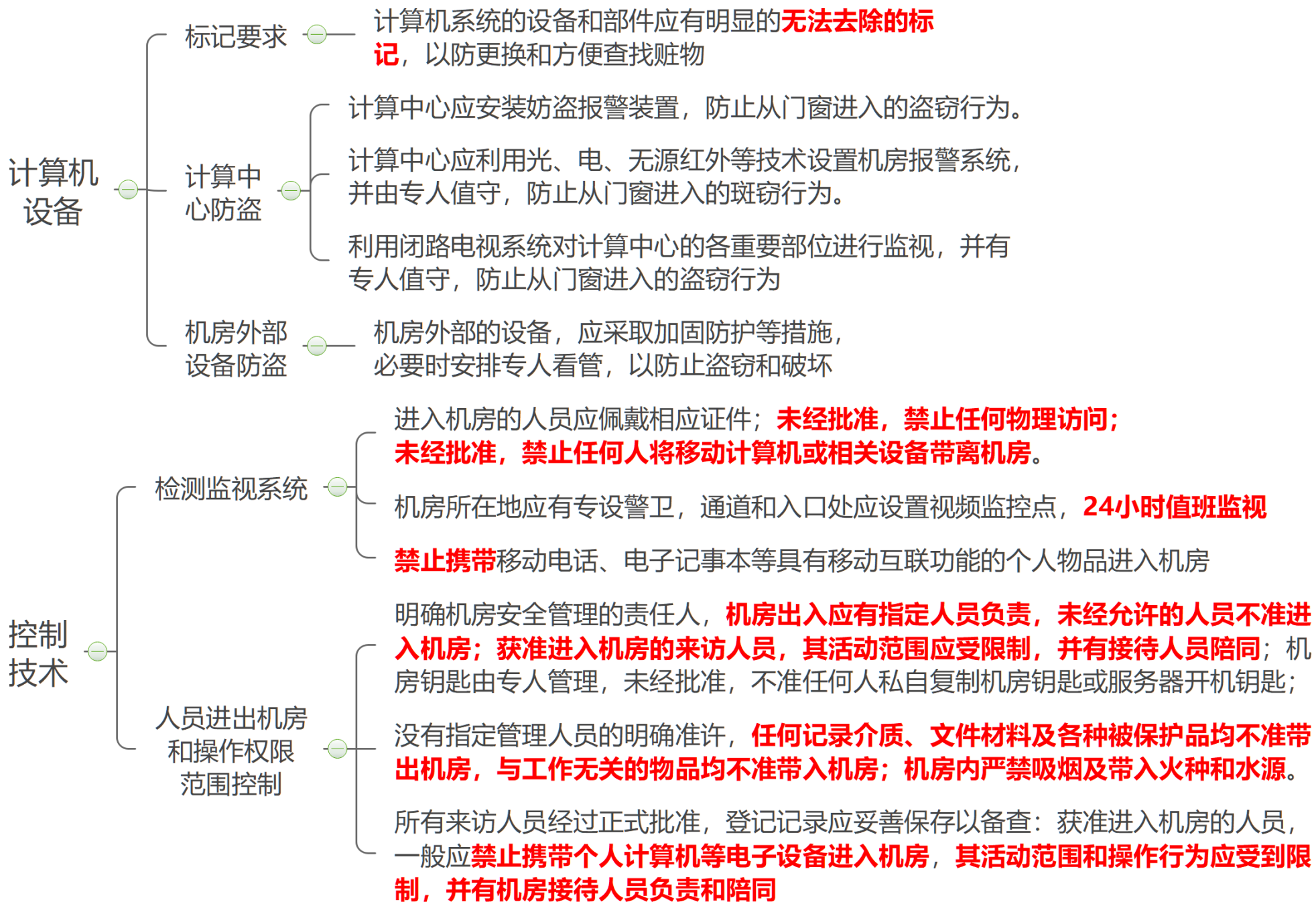
- ①接地要求 — 采用地桩、水平栅网、金属板、建筑物基础钢筋构建接地系统等
- ②去耦、滤波要求 — 设置信号地与直流电源地，并注意不造成额外耦合，保证去耦、滤波等的良好效果
- ③避雷要求 — 设置避雷地，以深埋地下，与大地良好相通的金属板作为接地点
- ④防护地与屏蔽地要求 — 设置安全防护地与屏蔽地，采用阻抗尽可能小的良导体的粗线，以减少各种地之间的电位差。应采用焊接方法，并经常检查接地是否良好，检测接地电阻，确保人身、设备和运行的安全。

电源

- ①分开供电
- ②紧急供电：配置抗电压不足的基本设备、改进设备或更强设备，如基本UPS，改进的UPS、多级UPS和应急电源（发电机组）等。
- ③备用供电
- ④稳压供电：采用线路稳压器，防止电压波动对计算机系统的影响
- ⑥不间断供电：采用不间断供电电源，防止电压波动、电器干扰和断电等对计算机系统的不良影响。

电磁兼容

对需要防止电磁泄露的计算机设备应配备电磁干扰设备，在被保护的计算机设备工作时电磁干扰设备不准关机；必要时可以采用屏蔽机房。**屏蔽机房应随时关闭屏蔽门；不得在屏蔽墙上打钉钻孔，不得在波导管以外或经过过滤器对屏蔽机房内外连接任何线缆；**应经常测试屏蔽机房的泄露情况并进行必要的维护



环境与 人身安全

防火

- 机房和重要的记录介质存放间建筑材料的耐火等级，应符合规定的**二级耐火等级**；机房相关的其余基本工作房间和辅助房建筑材料的耐火等级应不低于**二级防火等级**
- 计算机机房应设火灾自动报警系统，主机房、基本工作间应设**卤代烷灭火系统**
- 凡设置卤代烷固定灭火系统及火灾探测器的计算机机房，其吊顶的上、下及活动地板下，均应设置**探测器和喷嘴**
- 吊顶上和活动地板下设置火灾自动探测器，通常有两种方式：
 - 1.**均匀布置**，但密度要提高，每个探测器的保护面积为 $10\sim 15\text{m}^2$
 - 2.在易燃物附近或有**可能引起火灾的部位以及回风口**等处设置探测器

机房隔壁不能为卫生间或水房，漏水会对机房造成损害，同时机房肯定不能用水来灭火了

防漏水 和水灾

- ①与主机房无关的给排水管道**不得穿过主机房**
- ②主机房内如设有地漏，地漏下应加设水封装置，并有防止水封破坏的措施。
- ③机房内的设备需要用水时，其**给排水干管应暗敷，引入支管宜暗装**。管道穿过主机房墙壁和楼板处，应设置套管，管道与套管之间应采取可靠的**密封措施**。
- ④机房**不宜**设置在用水设备的**下层**
- ⑤机房房顶和吊顶应有**防渗水措施**
- ⑥安装排水地漏处的楼地面应低于机房内的其他楼地面

防静电

- 主机房内绝缘体的静电电位不应大于**1kv**

岗位安全 考核与培训

- 1.对安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员和重要业务应用操作人员等信息系统关键岗位人员进行统一管理；允许一人多岗，但**业务应用操作人员不能由其他关键岗位人员兼任**；关键岗位人员应定期接受安全培训，加强安全意识和风险防范意识。
- 2.兼职和轮岗要求：**业务开发人员和系统维护人员不能兼任或担负安全管理员、系统管理员、数据库管理员、网络管理员和重要业务应用操作人员等岗位或工作**；必要时关键岗位人员应采取**定期轮岗制度**。
- 3.权限分散要求：在上述基础上，应坚持关键岗位“**权限分散、不得交叉覆盖**”的原则，**系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作**。
- 4.多人共管要求：在上述基础上，**关键岗位人员处理重要事务或操作时，应保持二人同时在场，关键事务应多人共管**
- 5.全面控制要求：在上述基础上，应采取对内部人员全面控制的安全保证措施，对所有岗位工作人员实施全面安全管理。

离岗人员 安全管理

- 1.基本要求：立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限；**收回所有相关证件、徽章、密钥和访问控制标记等；收回机构提供的设备**
- 2.调离后的保密要求：在上述基础上，管理层和信息系统关键岗位人员调离岗位，必须经单位人事部门**严格办理调离手续，承诺其调离后的保密要求**。
- 3.离岗的审计要求：在上述基础上，设计组织机构管理层和信息系统关键岗位的人员调离单位，必须进行**离岗安全审查，在规定的脱密期限后，方可调离**。
- 4.关键部位人员的离岗要求：在上述基础上，关键部位的信息系统安全管理人员离岗，应按照机要人员管理办法办理。

安全和保密层次

- 系统级安全
 - 策略:敏感系统的隔离、**访问IP地址段的限制、登录时间段的限制、会话时间的限制、连接数的限制**、特定时间段内登录次数的限制以及远程访问控制等
 - 是应用系统的**第一道防护大门**
- 资源访问安全
 - 是最常见的应用系统安全问题，**几乎所有**的应用系统都会涉及这个安全问题
 - 在客户端上，为用户提供和其权限相关的用户界面，**仅出现和其权限相符的菜单和操作按钮**，在服务端则对**URL程序资源和业务服务类方法的调用**进行访问控制。
- 功能性安全——如用户在操作业务记录时，**是否需要审核，上传附件不能超过指定大小**等
- 数据域安全
 - 1.**行级**数据域安全，即用户可以访问哪些业务记录，一般以用户所在单位为条件进行过滤；
 - 2.**字段级**数据域安全，即用户可以访问业务记录的哪些字段

安全检查

企业要加强对应用系统安全运行管理工作的领导，每年至少组织有关部门对系统运行工作进行一次检查。部门**每季度**进行一次自查。要加强对所辖范围内应用系统运行工作的监督检查。检查可采取**普查、抽查、专项检查**的方式**定期或不定期**地进行

安全管理制度

- 安全组织 — 由**单位**主要领导人领导，不能隶属于计算机运行或应用部门
- 安全等级 —
 - 保密等级 —
 - 绝密
 - 机密
 - 秘密
 - 可靠性等级 —
 - A级 — 最高
 - B级
 - C级 — 最低
- 操作规程 — 应用系统操作人员应为专职，关键操作步骤要有两名操作人员在场，必要时需要对操作的结果进行检查和复核。对系统开发人员和系统操作人员要进行**职责分离**。

用户管理制度

- 建立用户身份识别与验证机制，防止非授权用户进入应用系统
- 用户权限的分配必须遵循“**最小特权**”原则
- 用户密码应**严格保密，并及时更新**
- 重要用户密码应密封交安全管理员保管，人员调离时应及时**修改相关密码和口令**

信息系统的安全保护等级

- 第一级 — 个人合法权益造成损害
- 第二级 — 个人合法权益严重损害，或社会利益遭到损害
- 第三级 — 公共利益造成严重损害或国家安全造成损害
- 第四级 — 公共利益造成特别严重损害或国家安全造成严重损害
- 第五级 — 国家安全造成特别严重损害

户籍全解放

计算机系统安全保护能力的五个等级

- 用户自主保护级
- 系统审计保护级
- 安全标记保护级
- 结构化保护级
- 访问验证保护级

>>> 练一练

【例1-17上】数字签名技术属于信息系统安全管理中保证信息（）的技术。

A.保密性 B.可用性 C.完整性 D.可靠性

【例2-17下】应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。针对应用系统安全管理，首先要考虑（）。

A.系统级安全 B.资源访问安全 C.功能性安全 D.数据域安全

【例3-18上】只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改，这体现了信息安全的（）。

A.机密性 B.可用性 C.完整性 D.可控性

>>> 练一练

【例4-18上】关于信息系统岗位人员的安全管理的描述，不正确的是（）。

- A.对安全管理员、系统管理员、重要业务操作人员等关键岗位进行统一管理
- B.紧急情况下，关键岗位人员可独自处理重要事务或操作
- C.人员离岗后，应立即中止其所有访问权限
- D.业务开发人员和系统维护人员不能兼任安全管理员

【例5-18上】应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、数据域安全等。以下描述不正确的是（）。

- A.按粒度从大到小排序为系统级安全、资源访问安全、数据域安全
- B.系统级安全是应用系统的第一道防线
- C.功能性安全会对程序流程产生影响
- D.数据域安全可以细分为文行级数据域安全和字段级数据域安全

>>> 练一练

【例6-18下】在信息系统安全技术体系中,安全审计属于 ()

A.物理安全 B.网络安全 C.数据安全 D.运行安全

【例7-18下】根据《信息安全等级保护管理办法》规定,信息系统受到破坏后,会对社会秩序和公共利益造成严重损害,或者对国家安全造成损害,则该信息系统的安全保护等级为 ()

A.一级 B.二级 C.三级 D.四级

【例8-19上】应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全,其中粒度最小的层次是 ()。

A.系统级安全 B.资源访问安全 C.功能性安全 D.数据域安全

>>> 练一练

【例9-19上】关于信息系统岗位人员安全管理的描述，不正确的是（）。

- A.业务应用操作人员不能由系统管理员
- B.业务开发人员不能兼任系统管理员
- C.系统管理员可以兼任数据库管理员
- D.关键问题人员处理重要事务或操作时，应保持二人同时在场

【例10-19下】（）技术不能保障应用系统的完整性。

- A.奇偶校验法
- B.数字签名
- C.物理加密
- D.密码校验

【例11-19下】关于信息系统岗位人员管理的要求，不正确的是（）。

- A.安全管理员和系统管理员不能由一人兼任
- B.业务开发人员不能兼任安全管理员、系统管理员
- C.系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作
- D.关键岗位在处理重要事物或操作时，应保证二人同时在场

>>> 练一练

【例12-20下】保障信息系统完整性的方法不包括（）。

- A.物理加密 B.数字签名 C.奇偶校验法 D.安全协议

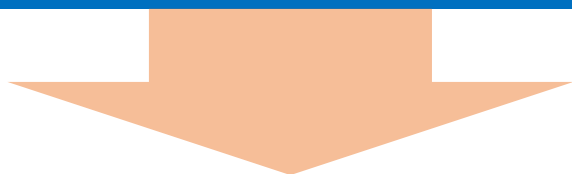
【例13-20下】关于信息系统岗位人员管理的要求,不正确的是（）。

- A.业务开发人员和系统维护人员不能兼任安全管理、系统管理员
B.对安全管理员、系统管理员等重要岗位进行统一管理,不可一人多岗
C.系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作
D.关键岗位在处理重要事务或操作时,应保证二人同时在场

| | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| C | A | C | B | D | D | C | D | C | C |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| A | A | B | | | | | | | |

非常感谢您的聆听

加入正版课程获得VIP全套增值服务



问题咨询联系江山老师 QQ/微信：51815498 /915446173



江山老师答疑微信



官方公众号



备份公众号

扫一扫
加关注
抢先学
早拿证



微信扫码做题