一、单选题

**1. 按国家会计制度要求，操作系统、数据库、网络设备、安全设备记录登录、重大操作、事件错误等日志信息，日志信息保存期限不得少于：**

**C**

A.3个月

B.6个月

C.1年

D.2年

**2.行内办公用计算机访问互联网应采用哪种方式：**

**A**

A.沙盒+代理

B.ADSL拨号上网

C.WIFI热点

D.3G/4G拨号上网

**3.** **以下哪项不是信息技术一般性控制审计的内容：**

**D**

A. 信息安全管理

B. 系统开发与采购管理

C. 业务持续性计划

D. 系统配置控制

**4.系统用户的行为可以被下列哪种方式正确的记录和追溯责任：**

**C**

A. 识别和批准

B. 批准和认证

C. 识别和认证

D. 批准

**5.以下哪个角色的任务是确保IT部门的工作与业务目标保持一致：**

**C**

A.首席执行官

B.董事会

C.IT战略委员会

D.审计委员会

**6.业务系统的访问授权职责归属于：**

**A**

A.数据所有者

B.安全管理员

C.IT安全经理

D.需求提出者的上级部门

**7.以下哪种是降低网络钓鱼风险的最有效方法：**

**D**

A.集中式监控系统

B.反病毒软件

C.在局域网中设置禁止网络钓鱼的策略

D.对所有用户进行网络安全培训

**8.IT审计中，应采用哪种方法来判断是否对生产程序进行了非授权修改：**

**B**

A.系统日志分析

B.符合性测试

C.取证调查分析

D.分析性调查

**9.与信息相关的四大安全原则是：**

**B**

A.保密、访问控制、完整性、不可抵赖性

B.保密、鉴别、完整性、不可抵赖性

C. 鉴别、授权、不可抵赖性、可用性

D. 鉴别、授权、访问控制、可用性

**10.关于邮件收发，以下哪种说法是错误的：**

**B**

A.应使用notes邮箱收发办公邮件，避免通过互联网邮箱处理办公信息。

B.使用个人notes邮箱对外发送敏感信息时，应加密处理。

C.不得转发非法邮件，对来历不明的邮件保持警惕，不随意点击邮件中的链接，对附件进行病毒检测后再打开。

D. 按“知所必需”原则，谨慎使用邮件群发功能。

二、多选题

**1.出现以下情况时，启动计划外专项信息科技检查工作：**

**ABCD**

A.信息科技运行中发现重大隐患

B.内部或同业出现重大信息科技风险事件

C.信息科技审计中发现重大问题

D.监管机构下发信息科技检查工作要求，或发布严重信息科技风险提示

**2.关于生产数据获取，以下哪些说法是正确的：**

**ACD**

A.生产数据提取遵循最小化满足使用需求的原则，必须经数据业务主管部门审批

B.信息技术部建立通过信息系统下载批量数据的申请、审批流程，明确数据实际使用人

C.系统后台提取数据必须通过安全运维管理平台或数据提取专用终端进行，操作过程可追溯

D.用于开发测试的生产数据必须脱敏

**3.以下哪些维护活动应纳入变更管理:**

**ABC**

A.信息系统的应用版本在生产环境的投产、升级、调整

B.对机房设备设施、网络、存储、营业终端、基础软件等的安装部署、升级、扩容、迁移、拆除、维护

C.从业务操作界面无法获取，而采用技术手段对业务生产数据的修改

D.用户领用办公PC机，并为其分配IP地址、安装办公软件

**4. 对员工的互联网访问行为进行安全监控和审计, 监控和审计的内容必须包括:**

**ACD**

A.用户账户

B.用户密码

C.源地址和目的地址

D.访问时间

**5.以下哪些情况发生时，必须更新相关信息系统应急预案：**

**ABCD**

A.系统升级

B.网络改造

C.设备更新

D.配置参数变化

**6.业务专用IT设备采购需满足一定安全要求，以下哪些说法是正确的：**

**ABCD**

A.用户密码等认证类信息必须以加密方式存储

B.只允许以应用程序界面提供服务，严禁预留访问底层操作系统及后台数据库的隐蔽通道。

C.严禁配置无物理防护的USB端口。

D.Windows设备需支持安装我行指定的防病毒软件。

**7. 信息安全管理基本原则是：**

**ABCD**

A.全面管理

B.预防为主

C.分级保护

D.合规审慎

**8. 关于生产数据传递，以下哪些说法是正确的：**

**ABC**

A. 使用物理介质传递生产数据时，应由专人负责押运，确保物理介质安全到位。

B. 数据提取过程所产生的中间数据应妥善处理，不得泄露给无关人员。

C. 严禁在无建行人员监管下通过第三方（如EMS等）进行介质传递。

D.在互联网上传输生产数据时应进行加密处理,以确保信息安全

**9.我行的信息技术审计准则中，已明确了以下哪些内容：**

**BD**

A.IT审计业务的短期和长期计划

B.IT审计业务的目标和范围

C.对IT审计人员详细的培训计划

D.IT审计的程序

**10.以下哪些措施可以有效降低针对IT系统的舞弊：**

**ABCD**

A.定期岗位轮换

B.强制休假

C.控制对设备的访问

D.将负责输入和输出的系统角色分离

三、填空题

1.系统用户账号申请与分配应遵照**\_\_\_\_\_\_\_\_**原则，仅赋予用户能够完成工作所需的最小权限。

**最小化**

2. **\_\_\_\_\_\_\_\_**技术可防范涉密信息在传输、处理、存储过程中出现泄露或被篡改的风险。

**加密**

3.信息技术应急预案的建设和演练应遵循**\_\_\_\_\_\_\_\_**、**\_\_\_\_\_\_\_\_**、**\_\_\_\_\_\_\_\_**和**\_\_\_\_\_\_\_\_**原则。

**规范性**、**完整性**、**有效性**和**持续性**

4.信息技术应急预案的演练方式包括：**\_\_\_\_\_\_\_\_**、**\_\_\_\_\_\_\_\_**和**\_\_\_\_\_\_\_\_**。

**桌面演练**、**模拟演练**和**实战演练**

5.根据我行信息系统参数管理办法，信息系统参数分为**\_\_\_\_\_\_\_\_**和**\_\_\_\_\_\_\_\_**。

**技术参数**和**业务参数**

6.外部用户提出非现场审计系统应用临时需求时，应按照相关规定进行审批，并由**\_\_\_\_\_\_\_\_**进行操作并将结果数据对其提供。

**审计机构**

7.为防止因遗失等原因而造成的审计数据泄密，存放重要数据的移动存储设备必须加密保护。凡是涉及高安全等级信息，必须保存到**\_\_\_\_\_\_\_\_**中。

**加密盘**

8. 对于国家有权机关、监管和审计需要、业务处理必需下载、**\_\_\_\_\_\_\_\_**后用于开发测试等需分发到办公计算机的数据，总分行后台数据分发者在数据安全组件中创建到办公计算机的生产数据卸数工单。

**脱敏**