测试点 1-1

(1)载体依附性、价值性
(2)传递性、共享性
(3)时效性
(4)时效性
(5)传递性、时效性
(6)真伪性
(7)可处理性、普遍性

测试点 1-2

(1)完整性>可用性>保密性：学校的门户网站主要是面向师生和部分社会人员（比如想考研本校的外校人员），因此该网站上信息的准确性和完整性应该位于优先级的首位；考虑到在某一特定时间段，访问该门户网站的次数可能会激增，因此网站应该有较好的可用性来应对不同情况下可能发生的访问；门户网站上一般是对老师、课程的简要介绍，保密级别较低，因此保密性位于优先级的最后。
(2)可用性>完整性>保密性：输送点控制系统保障整个城市的用电，责任十分重大。因此为了防止系统产生不必要的崩溃，其可用性必须位于优先级首位；完整性是对输送电力关键信息的保障，决定了电力输送是否正确且成功，因此完整性位于优先级第二位；该系统保密级别较低，因此保密性位于优先级的最后。
(3)保密性>完整性>可用性：研究所的研究成果保密级别较高，因此保密性位于优先级首位；科研成果存储在该系统中，必须保证资料的准确性和完整性，因此完整性位于优先级第二位；该系统作为存储系统，用于访问和使用的机会不多，因此可用性位于优先级最后。

测试点 1-3

(1)保密性、完整性、
(2)安全威胁：场景一中的文件包含的敏感信息被监听后可能被泄露、造成更严重的安全威胁；场景二中的授权消息被修改后计算机 E 对其执行也会造成严重的后果。属于信息泄露、完整性破坏。
(3)攻击行为属于被动攻击中的网络监听和主动攻击中的改写、重放。

测试点 1-4

(1)通信安全，1949 年香农《保密通信的信息理论》→主机（计算机）安全，1983 年美国国防部《可信计算机评估准则》→网络安全，《ISO7498-2-1989 标准》→安全保障，1998 年《信息保障技术框架》→网络空间安全，习近平“没有网络安全，就没有国家安全”
(2)认识一：信息安全是相对的，没有绝对的安全。即使是最严密的系统，也会存在漏洞。
认识二：信息安全是一个动态过程，而不是一个产品（或技术）以及多个产品（或技术）的简单堆叠，具有生命周期。比如九十年代的信息安全系统已经不适用于当今先进技术条件背景下的信息安全防护需求。
认识三：信息安全防护是个全面保护的过程，遵循“木桶原理”，即一个木桶的容积决定于组成它的最短的一块木板，一个系统的安全强度等于它最薄弱环节的安全强度。比如 iPhone 的指纹识别机制采用了十分顶层的安全机制，但曾有技术人员直接绕开了锁屏界面，进入到桌面。可见即使指纹系统安全强度再高，由于其他系统机制的安全级别低，也会导致高级别的安全系统失效。
认识四：信息安全包括外部和内部的安全，人是安全机制中最薄弱环境。泄密事件往往是人

为的。
认识五：信息安全是国家安全不可分割的一部分。习近平总书记提出“没有网络安全，就没有国家安全”，当今社会的国家战争更多的发生在没有硝烟的战场上。因此信息安全是国家安全的首要保障对象。

测试点 1-5

(1)数据安全指对数据收集、存储、检索、传输等过程提供的保护，不被非法冒充、窃取、篡改、抵赖。（处理对象），内容安全指依据信息内涵判断是否违反特定安全策略，采取相应的安全措施。（语义内容）
(2)安全服务是指系统提供的安全防护措施（鉴别服务、访问控制、数据机密性、数据完整性、抗抵赖）安全机制是用来实施安全服务的机制（加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制、公证机制）。比如想要保证数据完整性（安全服务）就必须使用安全机制中的数字签名技术。
(3)打开支付终端（鉴别服务）、扫描支付二维码（数据机密性、数据完整性）、输入支付金额并确认（数据机密性）、输入支付口令并确认（鉴别服务、数据机密性）、收到支付确认结果（鉴别服务、抗抵赖）

测试点 1-6

(1)网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。
(2)应用理论层（各种网络空间安全应用技术）、技术理论层（系统安全理论技术、网络安全理论技术）、基础理论层（网络空间理论、密码学）。

测试点 1-7

(1) 棱镜计划（PRISM）是一项由美国国家安全局（NSA）自 2007 年小布什时期起开始实施的绝密电子监听计划，该计划的正式名号为“US-984XN”。英国《卫报》和美国《华盛顿邮报》2013 年 6 月 6 日报道，美国国家安全局（NSA）和联邦调查局（FBI）于 2007 年启动了一个代号为“棱镜”的秘密监控项目，直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等在内的 9 家国际网络巨头皆参与其中。“棱镜门”事件之前，我国在网络安全领域虽有所建树，但总体来说并没有一个长远的合理规划。“棱镜门”事件迫使我们必须从更高、更深、更远的方面进行反思。面对网络空间严峻而又复杂的现实风险和战略挑战，必须积极应对，有所作为，才能确保网络空间的国家安全和发展利益。
(2)具备及时发现问题、深入分析问题和独立解决问题的能力：信息安全是一个复杂的、隐蔽性很强的问题，一般是难以被人发现的，作为合格的信息安全人才应该具有敏锐的眼光和清晰的思路，能够从纷繁复杂的表面现象背后找到实质问题，也就是发现问题的能力。然后针对问题进行分析，找出问题的根源并及时解决。从发现网络安全问题到堵塞网络漏洞、消除安全隐患，这段时间越短越好，这样对网络安全所带来的影响就越小，造成的损失也越小。对于网络安全问题要透过现象看本质，不能等到问题已经爆发、造成严重损失后再去解决问题，而是要采取主动措施防范问题发生。