e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
j) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

9.1.10.7 恶意代码防范管理

本项要求包括：

a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
b) 应定期验证防范恶意代码攻击的技术措施的有效性。

9.1.10.8 配置管理

本项要求包括：

a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
b) 应将基本配置信息改变纳入系统变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

9.1.10.9 密码管理

本项要求包括：

a) 应遵循密码相关的国家标准和行业标准；
b) 应使用国家密码管理主管部门认证核准的密码技术和产品；
c) **应采用硬件密码模块实现密码运算和密钥管理**。

9.1.10.10 变更管理

本项要求包括：

a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
c) 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

9.1.10.11 备份与恢复管理

本项要求包括：

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和

恢复程序等。

9.1.10.12 安全事件处置

本项要求包括：

a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序；

e) **应建立联合防护和应急机制，负责处置跨单位安全事件。**

9.1.10.13 应急预案管理

本项要求包括：

a) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

c) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

d) 应定期对原有的应急预案重新评估，修订完善；

e) **应建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练。**

9.1.10.14 外包运维管理

本项要求包括：

a) 应确保外包运维服务商的选择符合国家的有关规定；

b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

c) 应保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

9.2 云计算安全扩展要求

9.2.1 安全物理环境

9.2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

9.2.2 安全通信网络

9.2.2.1 网络架构

本项要求包括：

a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b) 应实现不同云服务客户虚拟网络之间的隔离；

c) 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；

d) 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；

e) 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务；

f) **应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问；**

g) **应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式；**

h) **应为第四级业务应用系统划分独立的资源池。**

9.2.3 安全区域边界

9.2.3.1 访问控制

本项要求包括：

a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

9.2.3.2 入侵防范

本项要求包括：

a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；

d) 应在检测到网络攻击行为、异常流量情况时进行告警。

9.2.3.3 安全审计

本项要求包括：

a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

9.2.4 安全计算环境

9.2.4.1 身份鉴别

当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

9.2.4.2 访问控制

本项要求包括：

a) 应保证当虚拟机迁移时，访问控制策略随其迁移；

b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。

9.2.4.3 入侵防范

本项要求包括：

a) 应能检测虚拟机之间的资源隔离失效，并进行告警；

b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；

c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

9.2.4.4 镜像和快照保护

本项要求包括：

a) 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；
b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
c) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。

9.2.4.5 数据完整性和保密性

本项要求包括：

a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；
b) 应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；
c) 应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；
d) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。

9.2.4.6 数据备份恢复

本项要求包括：

a) 云服务客户应在本地保存其业务数据的备份；
b) 应提供查询云服务客户数据及备份存储位置的能力；
c) 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；
d) 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

9.2.4.7 剩余信息保护

本项要求包括：

a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；
b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

9.2.5 安全管理中心

9.2.5.1 集中管控

本项要求包括：

a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；
b) 应保证云计算平台管理流量与云服务客户业务流量分离；
c) 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；
d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

9.2.6 安全建设管理

9.2.6.1 云服务商选择

本项要求包括：

a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；
b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；
c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；
e) 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。

9.2.6.2 供应链管理

本项要求包括：
a) 应确保供应商的选择符合国家有关规定；
b) 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；
c) 应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

9.2.7 安全运维管理

9.2.7.1 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

9.3 移动互联安全扩展要求

9.3.1 安全物理环境

9.3.1.1 无线接入点的物理位置

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

9.3.2 安全区域边界

9.3.2.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

9.3.2.2 访问控制

无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

9.3.2.3 入侵防范

本项要求包括：
a) 应能够检测到非授权无线接入设备和非授权移动终端的接入行为；
b) 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；
c) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
d) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；
e) 应禁止多个 AP 使用同一个认证密钥；

f) 应能够阻断非授权无线接入设备或非授权移动终端。

9.3.3 安全计算环境

9.3.3.1 移动终端管控

本项要求包括：

a) 应保证移动终端安装、注册并运行终端管理客户端软件；

b) 移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等；

c) 应保证移动终端只用于处理指定业务。

9.3.3.2 移动应用管控

本项要求包括：

a) 应具有选择应用软件安装、运行的功能；

b) 应只允许指定证书签名的应用软件安装和运行；

c) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；

d) 应具有接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。

9.3.4 安全建设管理

9.3.4.1 移动应用软件采购

本项要求包括：

a) 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名；

b) 应保证移动终端安装、运行的应用软件由指定的开发者开发。

9.3.4.2 移动应用软件开发

本项要求包括：

a) 应对移动业务应用软件开发者进行资格审查；

b) 应保证开发移动业务应用软件的签名证书合法性。

9.3.5 安全运维管理

9.3.5.1 配置管理

应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

9.4 物联网安全扩展要求

9.4.1 安全物理环境

9.4.1.1 感知节点设备物理防护

本项要求包括：

a) 感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；

b) 感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；

c) 感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；
d) 关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）。

9.4.2 安全区域边界

9.4.2.1 接入控制

应保证只有授权的感知节点可以接入。

9.4.2.2 入侵防范

本项要求包括：
a) 应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；
b) 应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

9.4.3 安全计算环境

9.4.3.1 感知节点设备安全

本项要求包括：
a) 应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更；
b) 应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力；
c) 应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。

9.4.3.2 网关节点设备安全

本项要求包括：
a) 应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力；
b) 应具备过滤非法节点和伪造节点所发送的数据的能力；
c) 授权用户应能够在设备使用过程中对关键密钥进行在线更新；
d) 授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

9.4.3.3 抗数据重放

本项要求包括：
a) 应能够鉴别数据的新鲜性，避免历史数据的重放攻击；
b) 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

9.4.3.4 数据融合处理

本项要求包括：
a) 应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用；
b) **应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令。**

9.4.4 安全运维管理

9.4.4.1 感知节点管理

本项要求包括：

a) 应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；
b) 应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
c) 应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

9.5 工业控制系统安全扩展要求

9.5.1 安全物理环境

9.5.1.1 室外控制设备物理防护

本项要求包括：

a) 室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；
b) 室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

9.5.2 安全通信网络

9.5.2.1 网络架构

本项要求包括：

a) 工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用符合国家或行业规定的专用产品实现单向安全隔离；
b) 工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；
c) 涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离。

9.5.2.2 通信传输

在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。

9.5.3 安全区域边界

9.5.3.1 访问控制

本项要求包括：

a) 应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；
b) 应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

9.5.3.2 拨号使用控制

本项要求包括：

a) 工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身份鉴别和访问控制等措施；
b) 拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问

控制等措施；

c) **涉及实时控制和数据传输的工业控制系统禁止使用拨号访问服务。**

9.5.3.3 无线使用控制

本项要求包括：

a) 应对所有参与无线通信的用户(人员、软件进程或者设备)提供唯一性标识和鉴别；

b) 应对所有参与无线通信的用户(人员、软件进程或者设备)进行授权以及执行使用进行限制；

c) 应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；

d) 对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。

9.5.4 安全计算环境

9.5.4.1 控制设备安全

本项要求包括：

a) 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

b) 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

c) 应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理；

d) 应使用专用设备和专用软件对控制设备进行更新；

e) 应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。

9.5.5 安全建设管理

9.5.5.1 产品采购和使用

工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

9.5.5.2 外包软件开发

应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。

10 第五级安全要求

略。

附 录 A
（规范性附录）
关于安全通用要求和安全扩展要求的选择和使用

由于等级保护对象承载的业务不同，对其的安全关注点会有所不同，有的更关注信息的安全性，即更关注对搭线窃听、假冒用户等可能导致信息泄密、非法篡改等；有的更关注业务的连续性，即更关注保证系统连续正常的运行，免受对系统未授权的修改、破坏而导致系统不可用引起业务中断。

不同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求是有差异的，即使相同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求也有差异。

等级保护对象定级后，可能形成的定级结果组合见表 A.1。

表 A.1 等级保护对象定级结果组合

安全保护等级	定级结果的组合
第一级	S1A1
第二级	S1A2，S2A2，S2A1
第三级	S1A3，S2A3，S3A3，S3A2，S3A1
第四级	S1A4，S2A4，S3A4，S4A4，S4A3，S4A2，S4A1
第五级	S1A5，S2A5，S3A5，S4A5，S5A4，S5A3，S5A2，S5A1

安全保护措施的选择应依据上述定级结果，本标准中的技术安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为 S）；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 A）；其他安全保护类要求（简记为 G）。本标准中所有安全管理要求和安全扩展要求均标注为 G，安全要求及属性标识见表 A.2。

表 A.2 安全要求及属性标识

技术/管理	分类	安全控制点	属性标识
安全技术要求	安全物理环境	物理位置选择	G
		物理访问控制	G
		防盗窃和防破坏	G
		防雷击	G
		防火	G
		防水和防潮	G
		防静电	G
		温湿度控制	G
		电力供应	A
		电磁防护	S