ICS 91.010.30
P 00

团　　体　　标　　准

T/GDCSA 003—2021

信息技术应用创新项目数据安全保护规范

Data security protection specifications for information technology application innovation projects

2021－**－**发布　　2021－**－**实施

广东省网络空间安全协会
信息技术创新联盟　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2020 给出的规则起草。

本标准由***提出。

本标准由广东省网络空间安全协会和信息技术创新联盟归口。

本标准起草单位：　。

本标准主要起草人：　。

本标准是首次发布。

信息技术应用创新项目数据安全保护规范

1 范围

本标准规定了信息技术应用创新项目数据安全保护的要素和方法。

本标准适用于组织对信息技术应用创新项目数据安全的保护工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1 网络安全 cyber security（数据安全）

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

4 主要内容

4.1 通用安全

4.1.1 数据分类分级(美)

a) 应明确数据分类分级原则、标准和方法，并建立数据分类分级模型。

b) 应建立统一数据分类分级及数据资产管理工具，实现对数据的分类分级自动识别，形成数据分类分级结果报告，持续跟踪数据分类分级标识效果。

c) 应对不同类别和级别的数据开展关键安全点梳理，并针对不同的安全点建立相应的安全技术措施，包括访问控制、数据脱敏、数据加密等安全管理和控制措施。

4.2 数据安全

4.2.1 产生阶段（管理+技术）

4.2.1.1 数据生产/录入岗位权限

应对数据产生、录入等相关岗位的帐号配置最小权限；删除数据时，应对操作内容进行二次审核授权。

4.2.1.2 安全审计

a) 应对用户进行安全审计，记录并审核用户的协议、行为及安全事件；审计记录应包含事件的日期和时间、事件类型、主体标识、客体标识和结果等内容；

b) 审计记录应禁止被修改；

c) 审计记录应定期进行备份；

d) 审计进程应确保未被挂起或中断；

e) 应具备异常分析手段，发现异常用户和实体行为。

4.2.1.3 数据源鉴别

a) 应明确数据采集的目的、用户、方式、范围、采集源等，对外部采集的数据须确认其合法性和完整性，防止数据被仿冒或伪造；

b) 应对采集过程中的数据进行数据溯源并记录，确保数据源采集的可追溯性。

c) 对产生数据的数据源进行身份鉴别和记录，防止数据仿冒和数据伪造，应满足以下要求：

—组织建设:应建立相关组织，指定人员负责对数据源进行鉴别和记录；

—制度流程:应制定数据源管理的相关制度,规范数据源采集流程；

—人员能力:岗位人员应理解数据源鉴别标准和熟悉内外部数据采集的业务（流程）,并能够结合实际情况执行。

—技术工具: 应采取技术手段对内外部收集的数据和数据源进行识别和记录;应采取技术手段对追溯数据进行安全保护，关键追溯数据须进行备份。

4.2.1.4 数据质量保障

a) 应采取适当的措施确保数据的准确性，可用性，完整性和时效性；

b) 应建立有效的数据纠错机制；

c) 应建立机制,定期检查数据的质量。

4.2.2 存储阶段（管理+技术）

4.2.2.1 数据库高可用性

数据存储应须考虑数据库的高可用性，应满足以下要求：

a) 数据库应具备一定的抗攻击能力，确保避免主数据宕机影响正常使用；

b) 数据库应具备一定数据冗余能力，如日志异步、同步、存储同步等；

c) 冗余数据应保证其一致性；

d) 应明确启用冗余资源的方法，如故障的感知与应对方法；

e) 应建立数据库读写分离机制。

4.2.2.2 数据库可靠性

a) 数据库应具备用户登录验证机制，对登录用户进行校验；

b) 数据库应具备配置最小权限功能，可精确分配用户权限；

c) 具有安全审计能力，并实现数据库的访问危险操作阻断；

d) 应采取措施，防止数据库内容被非法修改；

e) 应采取措施，防止非授权用户对数据库的恶意存取和破坏；

f) 应采取措施，防止数据库中重要或敏感的数据被泄露；应及时发现系统漏洞并修补，无法修补的应采取其他安全防护措施防止外部攻击；

4.2.2.3 数据库审计

a) 应实时对数据库操作进行细粒度审计，对危险操作进行告警；

b) 应识别数据库越权使用、权限滥用，管理数据库帐号权限；

c) 应跟踪敏感数据访问行为，及时发现敏感数据泄漏；

d) 应检测数据库配置弱点、发现安全漏洞并修补；

e) 应完整记录数据使用过程的操作日志,以备对潜在违约使用者责任的识别和追责；

f) 应具备信息化技术手段或机制，对数据滥用行为进行有效的识别、监控和预警；

4.2.2.4 数据库访问权限（白名单限制）

a) 应基于用户身份标识与鉴别、数据访问控制、数据扩容及复制等策略进行数据库访问；

b) 应采用三权分立模式；

c) 应具备黑白名单策略机制。

4.2.2.5 物理管控（机房）

a) 应参照 GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》（8.1.1 章节）或 GB50174-2008《电子信息系统机房设计规范》（B 级）进行设计。

4.2.2.6 存储介质选择

a) 应设立统一负责存储介质管理的岗位和人员，明确各类介质使用的规范；

b) 应当基于组织机构的数据分类分级要求以及介质使用的要求，制定存储介质访问和使用安全策略和管理规范，并制定介质使用的审批和记录流程；

c) 应当建立获取存储介质的规范流程，通过可信渠道获取存储介质；

d) 应当建立存储介质的标记规程，明确介质存储的数据对象，并对介质访问和使用行为进行记录和审计；

e) 应建立对存储介质使用的常规和随机检查流程，确保存储介质的使用遵守机构公布的关于介质的使用规范；

4.2.2.7 存储方式选择（分层存储）

介质存储方式

a) 介质库存放应注意防尘、防潮，远离高温和强磁场，以及保存期限等；

b) 应根据关键业务数据、热数据、温数据和冷数据等数据类型，通过层管理系统的建立实现自动分层存储，当数据冷却时自动往下移动。

数据存储方式

应采取的数据存储方式包括但不限于在线存储、脱机存储 、近线存储 、异站保护等。

4.2.2.8 敏感数据定位

a) 应通过通过主动探测的方式进行数据安全资产管理，定位敏感数据，对敏感数据进行打标签，形成数据资产地图；

b) 应支持多种敏感数据以及相似性敏感数据的识别与发现；

c) 应根据定义好的敏感数据，利用工具对数据进行敏感数据扫描发现，对发现的数据进行数据定位、数据分类、数据分级。

d) 应对用户权限及节点的流量监控，基于敏感数据的调用行为进行基线建模，一旦发现越过基线的访问和调用及时告警；

4.2.2.9 数据备份方式

a) 应建立在线、离线的多级数据归档方式，支持海量数据的有效归档、恢复和使用；

b) 应具备数据备份的多种压缩策略和实现技术，确保压缩数据备份的完整性和可用性；

c) 应明确数据备份和恢复管理工作的岗位和人员；

d) 应建立数据备份策略和管理制度；

e） 应建立数据备份与恢复的操作规程，明确定义备份和恢复的范围、频率、工具、过程、日志、时长等；

4.2.2.10 远程运维安全（敏感数据脱敏）

a） 应明确各数据存储系统的安全管理员以及岗位职责；

b） 应对运维过程中访问的敏感数据进行实时脱敏，并明确脱敏的流程和方法；

c） 应定期对脱敏后的数据进行去标识化的评估。

4.2.2.11 数据加密存储

a） 应在数据写入和读取时将数据进行加密和解密；

b） 应采用密码技术保障重要数据在存储过程中的保密性，对鉴别数据、重要业务数据和重要个人信息等数据按需执行数据存储加密措施，防止敏感数据外泄。

c） 应采取国密加密算法；

d） 应对加密密钥进行定期备份，防止密钥丢失导致密文数据无法恢复。

e） 应明确密文数据申请访问流程，列明需要访问的数据目标、数据类别（精细到表或字段级）、访问时间、合理性及必要性等。

4.2.2.12 数据防勒索

a） 应对数据的存储介质建立相关防勒索机制，如数据存储终端、服务器等；

b） 应对重要数据所在运行环境包括数据库及大数据组件节点环境进行安全加固。

4.2.2.13 数据容灾备份

a） 应根据数据重要程度，针对重要的数据应具备跨地域的容灾能力；

b） 应明确数据容灾备份和恢复管理工作的岗位和人员；

c） 应建立数据容灾备份策略和管理制度；

d） 应建立数据备份与恢复的操作规程，明确定义数据备份和恢复的范围、频率、工具、过程、日志、时长等；

e） 应定期对备份数据进行有效性恢复测试。

4.2.3 使用阶段

4.2.3.1 无线网络管理

a) 应支持多项认证方式包括但不限于短信认证、APP 认证等；

b) 应对无线网关等设备记录的用户数据进行详细分析，提供丰富的日志报表；

c) 应能够识别与管控无线网络中与工作无关的应用；

d) 应具备流量管理功能，合理分配带宽资源，提高带宽利用率；

e) 应详细记录内网人员上网轨迹作为追查依据；

f) 应采取必要技术措施发现存在网络中的钓鱼 SSID、第三方非法 SSID，且能够通过有效措施进行屏蔽。

4.2.3.2 端口使用管控

a) 应对 PC 端口进行实时管控，严防企业核心数据外泄，端口管控范围包含蓝牙、光驱、串口/并口、USB 接口、WIFI 接口、调制解调器、红外设备等；

b) 针对有线用户使用场景，应具备端口准入能力。

4.2.3.3 终端防病毒

a) 终端设备应安装防病毒客户端，实时提供病毒防护能力；

b) 应具备防病毒客户端统一管理能力，并定时更新病毒库。

4.2.3.4 主机运行管理（应用白名单控制）

a) 应确保终端接入网络，需要采取相应的措施来消除威胁，降低整体安全风险，确保内部办公环境下的数据安全；

b) 应建立终端安全管控规范及技术能力，至少覆盖网络准入、补丁管理、安全基线、入侵防御、防病毒、数据防泄漏、软件管理、行为审计等方面。

4.2.3.5 终端用户身份鉴别

a) 应建立终端接入用户身份认证机制，支持系统内置账号和外部数据源方式；

b) 应具备动态鉴权能力，通过周期性地校验终端用户的合法性和安全状态，隔离非法用户；

c) 应对系统中的每一用户或与之相连的终端设备进行有效的标识与鉴别，只有通过鉴别的用户才能被赋予相应的权限，进入系统并在规定的权限内操作；

d) 应保证身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

e) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

4.2.3.6 终端实体和用户行为分析

a) 应具备终端实体和用户行为分析能力，包括终端操作系统层面和用户流量层面，及时阻断高危应用服务和高风险操作行为；

b) 应具备安全审计能力，安全审计主要涉及的方面包括:用户登录情况、管理用户的操作行为，关键的业务操作行为、系统功能执行以及系统资源使用情况等；

c) 应采取一定的技术手段监控和分析用户、实体的行为，实现从网络系统中采集日志、流量以及行为数据并创建实体的动态行为基线，通过利用行为基线进行对比分析等。

4.2.3.7 终端数据防泄露

a) 应对终端上的数据提供分类分级、安全防护、安全监测等防护功能；

b) 应通过文件水印、数据加密、防截屏等技术，实现多种数据泄露途径的封堵和有效审计回溯；

c) 应保证数据在终端使用过程中，采取技术手段从风险、合规等角度出发，以审计和阻断网络传输的敏感数据。

4.2.3.8 打印刻录审计

a) 应针对本地或网络打印行为进行审计及控制；

b) 支持对终端光盘刻录行为进行审计及控制，能够审计到终端在何时做过刻录、刻录的文件名称等信息；可以禁止终端进行光盘刻录，避免终端的违规刻录行为；

c) 对需刻录文档设置只读、打印、修改、再次授权、阅读次数及生命周期等权限，授权用户只能按照规定好的权限进行使用，无法通过属性修改、内容复制、副本另存等方式越权使用；

d) 通过内容复制/粘贴、拖拽、副本另存为、截屏/录屏、打印等方式对文档内容进行移植及转储，需要对用户上述操作行为进行安全审计。

4.2.3.9 使用身份鉴别

a) 应对使用阶段的身份进行标识和鉴别，确保身份标识具有唯一性，采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术进行身份鉴别。身份鉴别信息应具有复杂度要求并定期更换；

b) 应定期对登录使用的身份账号进行识别、梳理及分类，防止非法账号、闲置账号、过期账号等存在；

c) 应具有登录失败处理机制，配置结束对话、限制非法登录次数和连接超时自动退出等技术措施；

d) 应对使用阶段的管理工具或终端设备进行可信验证，防止工具被假冒或篡改；

e) 应在远程使用数据时，对传输通道两端进行主体身份鉴别和认证。

4.2.3.10 数据访问控制

a) 应基于“权限最小原则”做好数据访问权限的分配和控制，授予使用阶段数据管理用户所需的最小权限，并严格控制特权账号和高权限账号，实现管理用户的权限分离；

b) 应根据数据资产分类和分级，设置对应访问控制策略，访问控制策略规定用户对客体数据资产的访问规则；

c) 应将对重要数据资产的特权或高危操作、导入导出等操作进行授权审批管理，避免误操作及违规操作；

d) 数据访问控制的颗粒度应达到主体为用户级或工具级，客体颗粒度为：数据库表级及字段级、数据库对象级（敏感对象、系统对象、表空间）、数据库代码级（过程、函数、触发器、视图）；

e) 应对重要主体和客体设置安全敏感等级标记，并控制不同主体对不同敏感安全标记数据资源的访问；

f) 应建立数据访问控制策略和审计机制；

g) 应建立针对数据访问和操作的日志监控技术工具，实现对数据异常访问和操作进行告警；

h) 应重点监控高敏感数据以及特权账户对数据的访问和操作；

i) 应采取一定的技术手段对于接入数据库的行为提供多维度的监控，包括身份管理、应用防假冒、防撞库、直连控制和免密登陆等；

j) 应对数据资源访问基于应用程序名、IP 地址、操作系统账户、数据库实例名、时间等进行授权，实现权限进行集中管理，形成统一权限库；

k) 应重命名或删除默认账户，“修改默认账户的默认口令；

l) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

4.2.3.11 数据脱敏处理

a) 应梳理使用阶段的数据使用场景，对不同场景下的数据使用执行静态脱敏或动态脱敏等不同的技术脱敏措施；

b) 应根据数据使用方的不同身份和不同数据访问目的，对查询访问的敏感数据进行脱敏处理；

c) 应根据不同类型的敏感字段采用不同的脱敏规则，基于场景需求自定义脱敏规则；

d) 应通过敏感数据识别字典和脱敏算法来处理数据表中的敏感信息；

e) 应通过脱敏规则进行数据变形，实现敏感信息的可靠保护的数据脱敏；

f） 数据在进行数据脱敏后应当保证数据的一致性和业务的关联性，应用于数据抽取、数据分析；

g） 数据脱敏后应保留原始数据格式和特定属性；

h） 应对数据脱敏处理过程相应的操作进行记录。

4.2.3.12 数据入侵防范

a） 应对可疑的数据操作行为进行监测，对大量敏感数据外传以及账号异常高频操作等行为具备实时预警能力；

b） 应能发现可能存在的已知数据库漏洞，并在经过充分测试评估后，及时修复漏洞或采取防御措施；

c） 应能监测对重要数据库节点入侵的行为，并在发现严重入侵事件时提供阻断及告警；

d） 应当采取一定的技术手段通过实时全流量采集、各种资产日志分析，对业务系统的安全进行实时监测，对出现的安全风险进行及时的告警和阻断；

e） 应按统一的要求部署防护工具，如防病毒、硬盘加密、终端入侵检测等软件，并定期进行软件的更新；

f） 应部署相关设备对网络可用性及数据泄漏风险进行防范，如入侵检测，入侵防御，威胁分析检测与防护等设备。

4.2.3.13 数据使用审计

a） 应完整记录数据使用过程的操作日志，以备对潜在违约使用者责任的识别和追责；

b） 数据使用审计记录应包含时间、用户名、IP 地址、客户端程序名、数据库以及数据操作指令等信息，可对查询，新增，修改，删除等行为进行审计记录；

c） 数据使用审计的记录应采用单独的第三方审计设备，定期备份，避免受到未逾期的删除、修改或覆盖，且审计日志保存至少 12 个月。

4.2.3.14 安全信息和事件管理及责任认定

a） 应设立负责数据安全事件管理和应急响应的责任部门和人员；

b） 应明确数据安全事件管理和应急响应的策略；

c） 应实时关注信息系统运行状况，及时排除运行故障，做好维护记录；

d） 应按内部规定程序报批；

e） 应对所有连入外网的计算机实行物理隔离，以防内部数据外泄和遭受恶意攻击；

f） 任何单位和个人不得从事危害计算机信息系统安全的行为。

4.2.4 传输阶段（管理+技术）

4.2.4.1 接入管理

a) 应对重要数据传输通道进行加密传输(如采用 TLS/SSL 方式)，限制非法设备接入，保留日志记录，禁止采用移动介质传输数据；

b) 应采用符合国家密码要求的传输加密方式；

c) 应跟进传输通道加密保护的技术发展（如零信任）,评估新技术对安全方案的影响,适当引人新技术以应对最新的安全风险；

4.2.4.2 流量清洗

a) 应采用一定的技术手段对数据统一清洗，在数据清洗环节，根据校验规则，对数据的字段空值约束、字段值类型约束、数据的结构约束（是否字段缺失或者不对），均进行校验处理；

b) 应对传输的数据流量进行实时监控，发现不限于 DDoS 攻击在内的异常流量，在不影响业务数据的情况下，清洗异常流量。

4.2.4.3 未知威胁阻断

a) 应通过一定技术手段检测数据在传输过程中的未知威胁,如利用沙箱技术分析传输恶意文件的敏感行为，检测结果将同步至安全防护设备，对未知威胁进行阻断；

b) 应具备未知威胁流量检测分析能力并及时响应，阻断未知威胁。

4.2.4.4 网络防病毒

a) 应在数据传输通道中关键节点建立网络防病毒引擎，对数据流量进行深度包检测，对网络病毒进行阻断过滤；

b) 应及时更新病毒库。

4.2.4.5 完整性保护

a) 应设立管理传输通道和数据内容加密的岗位和人员，负责整体的加密原则和技术的提供，由各的技术团队负责具体场景下的实现数据传输加密；

b) 应提供对传输通道两端进行主体身份鉴别和认证的技措施；

c) 应对传输数据的完整性进行检测，并具备恢复控制的技术措施；

d) 应建设密钥管理系统提供数据的加密解密、签名验签等技术措施；

e) 应有对传输数据的完整性进行检测，并具备数据容错或恢复的技术手段；

f) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性；

g) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性。

4.2.5 交换阶段（管理+技术）

4.2.5.1 数据脱敏

应在数据被共享前，按照分类分级的策略，对数据进行适当的脱敏处理。

4.2.5.2 数据溯源

应具有网络流量的原始数据包存储和回溯查询能力。

4.2.5.3 数据接口

a) 应建立组织对外数据接口的安全管理机制，防范组织数据在接口调用过程中的安全风险；

b) 应明确数据接口的安全控制策略，包括身份鉴别、访问控制、授权策略、安全协议等；

c) 应明确数据接口安全要求，包括接口参数、名称，对不安全输入参数进行限制或过滤；

d) 应对数据库接口的调用、配置的修改、用户及权限、网络连接、系统资源的变化等进行安全审计和防护。

4.2.5.4 数据导入导出

a) 建立数据导入导出的安全管理制度,基于组织机构的数据分类分级要求定义数据导入导出相关的安全策略；

b) 在数据导入导出过程中应有严格的审核制度，并对导入导出数据做安全审计及标识；

c) 应对数据导入导出过程中的安全性进行管理，包括身份认证、权限控制、传输加密等方式；

d) 针对数据导入导出的安全管理制度进行定期更新，并定期开展审计工作。

4.2.5.5 数据共享

a) 应明确数据共享内容范围、形式和管控措施，及相关人员的职责和权限；

b) 应明确数据共享审计规程和审计日志管理要求,明确审计记录要求，以应对数据共享安全事件的处置、应急响应和事后调查；

c) 数据共享交换应采取身份验证，身份验证方式至少包括用户名/口令、数字证书等；

d) 数据共享交换时应采用传输链路加密或内容加密、数字签名等机制；

e) 数据共享交换时应遵循最小化原则。

4.2.5.6 数据发布

a) 应制定数据发布的审核制度，并对发布数据进行安全审计和标识；

b) 数据发布的过程中应对发布数据的格式、适应范围、发布者与使用者权利和义务执行的必要控制；

c） 建立数据资源公开事件应急处理流程。

4.2.5.7 数据交换监控

a） 应对数据交换行为制定数据交换风险行为识别和评估规则，并定期对数据交换行为进行审计；

b） 数据交换时应提前设定数据内容敏感性检查和安全性检查机制；

c） 应在数据交换时实时监控共享交换过程中的所有行为和内容，监控是否存在恶意数据获取、数据盗用等风险，具备对异常或高风险数据交换操作的自动化识别和实时预警能力，在双方数据不一致情况时可确定问题和责任所在。

4.2.6 销毁阶段（管理+技术）

4.2.6.1 数据销毁制度

a） 应依照数据分类分级的策略建立数据销毁策略和管理制度，明确数据销毁的场景、销毁对象、销毁方式和销毁要求；

b） 数据销毁策略和管理制度应正式发布；

c） 应定期更新数据销毁策略和管理制度。

4.2.6.2 敏感数据销毁

应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

4.2.6.3 极为敏感数据销毁

不再使用或无法使用的存储介质在进行报废处理前，应进行信息消除处理，信息消除处理时所采取的信息消除技术、设备和措施应符合国家及地方的有关规定；

4.3 国产密码在信息技术应用创新项目数据安全的应用

a） 国产密码技术在信息技术应用创新数据安全各阶段中的典型应用：数字签名、远程运维安全（敏感数据脱敏）等；

b） 国产密码算法在信息技术应用创新数据安全中的应用框架：密码管理基础设施-密码资源层-密码支撑层-密码服务层-密码应用层。

4.3.1 国产密码应用需求

信息技术创新应用项目采用的密码算法必须是安全可信、自主可控的国产密码，密码产品须符合国家密码主管部门的规范要求，技术必须是国产自主可控的密码技术。

信息技术创新应用系统需要使用密码应用服务，在系统设计时必须考虑采用国产自主可控的密码算法及产品。国产密码可以构建安全可靠的身份认证、权限管理、访问控制机制，用于接入安全问题；基于密码应用，采取数据加密传输、数据加密存储、数据库加密、完整性保护等措施，保护数据的机密性、完整性；应用密码技术，使用数据标签、签名验签等方式，实现数据与应用的可追溯性、不可抵赖性。

4.3.2 网络和通信安全密码应用

信息技术创新应用系统应按照《信息系统密码应用基本要求》信息系统网络和通信安全的基本要求，对物理资源层网络和通信安全进行设计。

应用于网络和通信安全的密码应用的措施如下：

1)应在网络边界部署网络密码机、边界认证类网关，在业务系统前端部署安全认证网关，在通信前基于密码技术对通信双方进行身份认证，通过信息加密传输防止通信数据被非法截获、假冒和重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；

2)应在网络边界部署网络密码机、跨域访问控制系统，保证网络边界和系统资源访问控制信息的完整性；

3)应通过网络密码机，采用完整性保护技术保证通信过程中敏感信息字段或整个报文的完整性；

4)应通过网络密码机，采用加密技术保证通信过程中敏感信息字段或整个报文的机密性；

5)应使用SSL 协议建立一条安全的信息传输通道，对网络中的密码设备进行集中管理；

6)应建立VPC 网络，实现虚拟网络的隔离；

7)应根据承载的业务系统安全保护等级划分不同安全级别的资源池区域，并实现资源池之间的网络隔离；

8)应制定安全机制，避免虚拟机通过网络非授权访问宿主机；

9)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；

10)应对远程执行特权命令进行限制。

4.3.3 应用和数据安全密码应用

信息技术创新应用系统应按照《信息系统密码应用基本要求》第三级信息系统应用和数据安全的基本要求，对应用和数据安全进行设计。

应用与数据安全密码应用的措施如下：

1)应使用信任服务体系的身份认证服务对登录应用的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；

2)应使用密码机、数据保护系统、大数据安全保险箱对业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息进行完整性保护；

3)应使用网络密码机对鉴别数据、重要业务数据和重要用户信息等进行加密传输保护，保证重要数据在传输过程中的机密性；

4)应使用密码机、大数据安全保险箱、数据存储加密网关、数据库加密网关、数据库加密系统、数据保护系统对鉴别数据、重要业务数据和重要用户信息等进行加密存储，保证重要数据在存储过程中的机密性；

5)应使用网络密码机对网络传输中的鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等数据进行完整性保护，保证重要数据在传输过程中的完整性；

6)应使用密码机、大数据安全保险箱、数据存储加密网关、数据库加密网关、数据库加密系统、云数据保护系统对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等重要数据文件进行完整性保护，保证重要数据在存储过程中的完整性；

7)应使用密码机、大数据安全保险箱、云数据保护系统对日志记录进行完整性保护；

8)应使用可信应用注册与验证系统对重要应用程序的加载、注册、卸载进行安全控制。

4.3.4 操作系统安全密码应用

信息技术创新应用系统操作系统安全密码应用应满足以下要求：

1)应经过授权的用户才能进行管理或审计操作；

2)应提供给用户的审计数据的真实性和完整性。其安全主要关注点为身份认证、访问控制、管理数据安全存储等；

3)应对管理指令进行完整性保护和真实性鉴别；

4)用户管理控制台是操作系统提供给用户使用的系统，用户可以使用该系统管理服务。在用户管理控制台中，应关注用户身份认证、加密通讯、用户隐私数据保护等。

4.3.5 分布式存储安全密码应用

信息技术创新应用系统的数据存储一般是采用分布式存储,涉及到的安全问题有网络传输安全、存储节点安全以及数据加密存储。

1)网络传输安全应通过构建安全传输通道，通过 SSL VPN 网关构建安全SSL 通道；

2)存储节点安全应通过加密、身份鉴别、访问控制等手段实现；

3)数据加密存储是指数据在写进磁盘前，应对数据进行加密。