ICS
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术
大数据服务安全能力要求

Information security technology —

Security capability requirements for big data services

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

（本稿完成日期：2016 年 12 月 15 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准主要起草单位：清华大学、中国电子技术标准化研究院、阿里巴巴（北京）软件服务有限公司、中国移动通信集团公司、国家信息安全工程技术研究中心、四川大学、阿里云计算有限公司、中国软件评测中心、腾讯云计算（北京）有限责任公司、华为技术有限公司、浙江蚂蚁小微金融服务集团有限公司、中国信息安全测评中心、中国电子科技网络信息安全有限公司、中电长城网际系统应用有限公司、陕西省信息化工程研究院、联想集团、广州赛宝认证中心服务有限公司、天津南大通用数据技术股份有限公司、西安未来国际信息股份有限公司、北京匡恩网络科技有限责任公司、北京赛博兴安科技有限公司、深圳市深信服电子科技有限公司、中国科学院信息工程研究所、中国科学院软件研究所、北京京东尚科信息技术有限公司。

本标准主要起草人：XXXX。

引　言

大数据将对全球生产、流通、分配和消费活动、社会生活方式和国家治理能力产生重要影响。然而，大数据系统却面临着诸多的安全威胁。本标准围绕大数据服务业务需求，确定了大数据服务安全目标，规范了大数据服务提供者的基础服务安全要求、覆盖数据生命周期的数据活动安全要求和大数据平台与应用的系统服务安全要求。

本标准一方面为大数据服务提供者的大数据系统的建设、运营和运维安全能力提供指导，另一方面为第三方机构对大数据服务提供者的大数据服务安全能力评估提供依据。

本标准从大数据应用提供者角色将大数据服务安全能力要求分为一般要求和增强要求。大数据服务提供者应依据附录A定义的大数据服务业务模式、大数据平台架构和大数据应用组件部署方式，选择本标准列举的大数据服务安全能力要求项进行安全建设和评估。

信息安全技术 大数据服务安全能力要求

1 范围

本标准定义了大数据服务安全目标，规范了大数据服务提供者的安全能力，包括大数据服务提供者的基础服务安全能力、覆盖数据生命周期管理的大数据活动安全能力、大数据平台与应用的系统服务安全能力。

本标准适用于为政府部门和社会公众提供大数据服务的相关方，包括数据提供者、大数据应用提供者、大数据平台提供者、大数据服务协调者等，也可为第三方对大数据服务安全能力的评估提供参考。

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，仅所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（包括所有的修改版）适用于本文件。

GB/T 25069—2010 信息安全技术 术语

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T AAAAA—AAAA 信息技术 大数据参考框架

GB/T BBBBB—BBBB 信息安全技术 大数据安全管理指南

GB/T CCCCC—CCCC 信息安全技术 个人信息安全规范

GB/T 22080—2016 信息技术 安全技术 信息安全管理体系要求

GB/T 22081—2016 信息技术 安全技术 信息安全管理实践指南

GB/T 31496—2015 信息技术 安全技术 信息安全管理体系实施指南

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069—2010、GB/T 31167—2014、GB/T 31168—2014、GB/T XXXXX—XXXX确立的以及下列术语适用于本标准。

3.1.1

数据生命周期 data lifecycle

用于描述大数据的“数据—信息—知识—价值”数据价值链和数据生命周期管理相关数据活动。

注：数据生命周期一般包括数据收集、传输、存储、处理（如计算、分析、可视化等）、共享、销毁等阶段。

3.1.2

数据服务 data service

信息系统所提供的一种数据采集、存储、组织、管理、查询和分析的数据处理软件服务。

注：数据服务封装了数据生命周期管理过程和数据源相关的各种数据实体操作,让数据使用者透明地处理多个数据资源，维护所管理数据的完整性和一致性，并通过数据分析与可视化活动提供数据增值服务，为机构的数据业务和商业模式改进提供可持续的数据基础。

3.1.3

大数据服务 big data service

覆盖数据生命周期、支撑机构大数据管理和数据价值发现的多种数据活动的一种数据服务。

注：大数据服务一般指面向海量、异构、快速变化的结构化、半结构化和非结构化数据，通过底层可伸缩的大数据平台和上层覆盖大数据应用数据生命周期相关数据活动的数据服务。

3.1.4

大数据服务提供者 big data service provider

提供大数据服务的机构或个人。

注：大数据服务提供者包括数据提供者、大数据平台提供者、大数据应用提供者和大数据服务协调者四种逻辑角色。

3.1.5

数据提供者 data provider

负责将机构内外部的各种数据或信息资源通过大数据平台或应用的数据收集服务引入机构的大数据平台的机构或个人。

注：数据提供者是大数据服务提供者的一种逻辑角色。依据大数据服务的数据来源，数据提供者可分为外部公共数据资源提供者、外部机构数据提供者和机构内部数据提供者。

3.1.6

大数据平台提供者 big data platform provider

负责建立和运营大数据平台相关的计算框架、存储框架和网络拓扑结构，在此平台上执行大数据应用，同时保证数据机密性、完整性和真实性的的机构或个人。

注：大数据平台提供者是大数据服务提供者的一种逻辑角色。大数据平台提供者可分为大数据基础设施提供者、大数据存储管理提供者和大数据应用支撑提供者。

3.1.7

大数据应用提供者 big data application provider

负责开发和部署大数据应用，提供数据生命周期相关的数据服务，以满足大数据服务协调者定义的业务需求以及安全和隐私保护需求的机构或个人。

注：大数据应用提供者是大数据服务提供者的一种逻辑角色。大数据应用提供者可分为大数据应用支撑服务提供者、大数据应用服务提供者和大数据应用集成服务提供者。

3.1.8

大数据服务协调者 big data service orchestrator

负责配置和管理大数据平台和大数据应用各类安全功能组件和安全策略,编排大数据服务所需的数据活动和系统服务活动，并将它们整合到可运行的大数据平台中，确保机构的大数据服务能按照相关的法律、法规要求安全高效地正常运行的的机构或个人。

注：大数据服务协调者是大数据服务提供者的一种逻辑角色。按照大数据平台和大数据应用安全角色不同，大数据服务协调者可分为安全管理员、安全审计员、数据管理员、密钥管理员等。

3.1.9

大数据使用者 big data consumer

使用大数据平台或应用的末端用户、其他IT系统或智能感知设备。

注：大数据使用者使用大数据服务提供者提供的数据分析服务，数据租售服务、数据共享服务、数据交易服务、技术支持服务、数据业务咨询服务等数据服务和系统服务。大数据使用者可分为政府部门、企事业单位自身和其他利益相关者、社会公众等。

3.1.10

大数据系统 big data system

大数据系统也称为大数据生态系统，包括大数据用户、大数据应用和大数据平台。

注:大数据用户分为大数据使用者和大数据服务提供者。大数据应用为数据提供者和大数据使用者提供数据采集、数据预处理、数据整合、数据存储、数据处理、数据分析、数据可视化、数据销毁等覆盖数据生命周期的数据服务。大数据平台提供对不同来源数据聚合、不同数据类型融合、各种类型数据实体操作封装、分布式数据存储和并行处理等数据集成和分析技术，并使用多种协议简化各数据源之间的数据接口，编程接口和数据提供者接口之间的映射，以及可伸缩服务过程中异常处理，使大数据使用者透明地访问或更新大数据系统中多源数据，以通用的、可互操作的、灵活的使用模式管理这些海量、异构、快速变化的结构化、半结构化和非结构化数据资源。

3.2 缩略语

下列缩略语适用于本文件。

表1 缩略语

ABE	Attribute-Based Encryption	属性基加密
ACL	AccessControlList	访问控制列表
APT	Advanced Persistent Threat	高级持续性威胁
DoS	Denial of Service	拒绝服务
IT	InformationTechnology	信息技术
PKI	Public Key Infrastructure	公钥基础设施
SLA	Service-Level Agreement	服务水平协议
SSL/TLS	Secure Sockets Layer/ Transport Layer Security	安全套接层/传输层安全
SQL	StructureQueryLanguage	结构化查询语言
TPM	Trusted Platform Module	可信平台模块
VM	Virtual Machine	虚拟机
XACML	eXtensible Access Control Markup Language	可扩展访问控制标记语言
XML	eXtensible Markup Language	可扩展标记语言

4 大数据服务安全

4.1 大数据服务安全目标

从安全属性看，大数据服务安全目标包括数据和主体机密性、数据和主体真实性和大数据服务可用性三个方面。从大数据安全功能看，大数据系统安全目标包括大数据应用安全管理、身份鉴别和访问控制、大数据活动安全管理、大数据基础设施安全管理和大数据系统应急响应管理。

4.1.1 安全属性

——**机密性：**数据提供者、大数据平台提供者和大数据应用提供者应提供数据和数据主体机密性安全控制措施。例如：使用安全套接层/传输层安全（SSL/TLS）等安全协议保证数据传输的机密性；使用基于凭证的数据访问策略、基于属性的细粒度访问控制策略、基于虚拟机（VM）技术的边界控制等保证数据存储访问机密性；使用公钥基础设施（PKI）、基于身份/属性加密体制（ABE）等密码学方法保证数据托管存储访问机密性；使用支持密文数据搜索和加密数据同态处理等的功能加密技术提供密文数据透明处理；使用集中存储的密钥服务保证数据分布式存储和分布式处理的安全访问；使用数据匿名化处理技术、数据扰动技术、差分隐私技术等保障发布数据主体敏感信息的安全性等。

——**真实性：**大数据平台提供者和大数据应用提供者应确保大数据服务中数据和主体真实性。例如：使用终端输入验证方式来保证采集过程中收集的数据来自可信的数据源；使用领域相关的语义约束条件来验证数据语义或用户操作满足典型业务规则，确保数据操作过程中数据完整性；使用数字签名等密码技术从数学角度来验证数据和主体真伪；在传输过程中使用安全传输层协议等保证数据传输完整性；使用数据验证计算技术确保分布式数据关键片段计算确实符合预期的计算结果，启用细粒度或高级安全审计机制以确保大数据服务可追踪能力；使用可信计算平台模块（TPM）保证数据和主体处理值得信赖；使用大数据服务中各种加密机制、安全协议等保证数据完整性和数据主体敏感信息隐私保护等。

——**可用性：**大数据平台提供者和大数据应用提供者应监控大数据服务服务软件和硬件系统资产的健康运行，以确保数据生命周期各阶段的数据活动一直满足数据和主体机密和真实性安全目标。例如通过系统审计跟踪定位大数据服务过程中的性能瓶颈等，保证数据服务高效性；建立主动抵御拒绝服务攻击（DoS）的密码协议（使用加密、签名和其它加密完整性检查协议）以保证大数据服务可用性；基于大数据服务运行数据的自动化监控和分析，保证大数据服务自我保护能力（免疫系统），提高大数据服务的自适应能力；提供包含关键安全、性能指标以及趋势指针的仪表盘，以进行不间断的数据安全服务监控；使用机器学习等数据分析算法来持续评估数据服务安全基准活动的变化和监测异常事件；提供大数据平台及大数据应用组件配置合规及风险管理插件，提供包括自动监控、合规策略评估以及威胁建模等合规性和违反安全事件检测的系统健康运行管理组件和服务；提供基于日志、网络事件、智能代理的大数据分析等服务接口组件和辅助管理工具。

4.1.2 安全功能

——**大数据应用安全管理：**数据提供者和大数据使用者都是通过大数据应用终端、大数据服务组件和大数据服务接口与大数据系统进行交互。因此，大数据系统应安全地管理接入的大数据应用程序、大数据应用终端和外部潜在的大数据资源，提供诸如大数据应用程序安全注册、大数据应用安全元数据管理、大数据应用开发和部署策略等。大数据应用程序安全注册需登记和管理如物联网网络、移动终端等大数据应用终端设备、数字化产权保护下的各种数据资产、以及外部服务、应用程序和用户角色。大数据应用安全元数据管理应结构化存储和维护大数据服务安全相关的设备、用户、资产、服务组件等所有数据和主体安全要素，包括数据快速更新、数据结构变化、以及临时数据存储、数据有效性、大数据服务运行日志、溯源数据等系统运行安全统计数据，以支持应用数据生命周期、合规性控制等复杂应用的安全管理。大数据应用开发和部署实施策略涵盖符合机构信息系统环境建设的大数据应用部署和设施策略、大数据运行过程中的细粒度审计政策、以及不同大数据服务角色相关的行为规范等。大数据应用应该提供用户数据导入与导出，用户数据备份、用户行为数据保护等个性化数据安全管理功能。

——**身份鉴别和访问控制：**大数据应用提供者和大数据平台提供者应对大数据用户身份进行验证，并提供合适的访问控制授权引擎对用户访问的数据资源进行控制，提供诸如基础设施层用户身

份验证、应用程序层身份验证、终端用户层身份管理、服务提供商身份管理、粗粒度、细粒度、属性基等多种访问控制、多租户数据安全管理等。基础设施层用户身份验证应支持分布式计算技术、虚拟计算技术等计算方式的身份验证，例如基于硬件安全模块支持下的可信计算体系，从基础设施层提高大数据服务整体安全性。应用程序层用户身份验证应提供基于公钥基础设施（PKI）等技术的身份认证服务平台，实现对应用层用户的证书、账户、授权、认证和审计的集中管理、整合大数据服务资源、实现应用数据共享和全面集中管控目标。终端用户层身份管理应依据数据提供者和大数据使用者角色自动判断大数据应用中用户的身份信息，保证大数据服务系统中的用户标识和大数据应用用户参考标识与应用层授权信息之间的映射关系。服务提供商身份管理针对大数据系统中数据提供者、大数据服务协调者、大数据平台提供者、大数据应用提供者和大数据使用者，以多个服务身份使用大数据服务，使用安全性断言标记语言来定义数据资源提供者提供身份（和角色），添加安全和隐私保证等要求，扩展传统的用户身份鉴别和授权机制。大数据可聚合多个数据提供者的数据资源，细粒度访问控制使得大数据服务提供者不只是分享数据集和数据服务，同时也分享数据授权策略，因此，大数据系统需要提供基于属性访问控制引擎（如 XACML），提供策略编辑点、策略决策点、策略执行点和政策访问点等面向数据对象的授权管理和访问控制功能。

——**大数据活动安全管理：**围绕大数据的“数据—信息—知识—价值”数据价值链的数据生命周期活动，提供数据在传输、存储和使用过程中的加密功能和密钥管理功能，提供不同应用之间数据隔离与封装服务，确保用户数据机密性和可管理性；提供数据存储安全控制措施，包括不同数据副本或数据在不同空间的完整性检测措施，预防数据丢失，保证数据可访问性；部署必要的网络服务网关，确保数据的安全迁移、转换和共享；提供聚合数据管理措施，确保多数据源安全整合；提供服务组件计算可信性验证机制，确保应用服务组件的安全性；具备加密数据的透明计算能力；制定部署、迁移和保留策略、个人信息保护策略、去标识化和匿名化机制，确保数据生命周期中个人隐私与敏感数据的安全管理，包括个人信息再标识风险管理等；提供大数据应用终端验证、数字版权管理、信任管理、数据披露、数据交易伦理、数据治理等数据生命周期相关的是数据服务安全。

——**大数据基础设施安全管理：**提供网络、计算、存储和环境资源，包括点对点传输、存储转发、大数据交换与通信框架操作和维护相关的安全措施和隐私保护功能，提供诸如威胁和脆弱性管理、安装与配置管理、系统监测和报预警、运行日志和安全审计、网络边界控制和基础设施冗余和恢复等功能。威胁和脆弱性管理应识别大数据平台及大数据应用的脆弱性及相关威胁，对分布式拒绝服务攻击、密钥管理、加密协议及相关威胁主体，以及对脆弱性衍生的问题进行管理。安装与配置管理包括安全参数设置、安全组件部署、安全补丁管理、系统升级等，目的是保护大数据服务基础设施和数据完整性。系统监测和预警需要通过部署大数据运行安全相关的组件和服务实现，它基于大数据基础设施运行数据实现大规模安全情报、复杂事件融合、安全分析、恶意软件监测和修复等安全功能。日志记录和安全审计是通过管理基础设施产生的海量、多样和高速变化的日志大数据，在线分析和统计抽样这些日志信息，为基础设施的安全运营和优化提供安全统计数据。网络边界控制主要为数据源和数据服务不可知的基础设施安全域间建立一条安全连接通道，共享服务网络体系结构，保证在开放环境下基础设施的网络通信安全。基础设施冗余和恢复通过系统复制有计划的维护大数据系统内部软件层次的冗余，以支持故障转移、系统恢复能力或减少大数据基础设施性能延迟，因为从大数据安全失败中恢复系统可能比小数据更加需要高级的基础设施安装、部署与配置等准备工作。

——**大数据系统应急响应管理：**提供大数据服务基础设施和数据管理平台风险和责任相关的问题追责、安全合规、安全取证、安全事件管理、风险控制措施等。问题追责主要基于大数据平台和大数据应用之间的信息、流程和角色行为，通过追踪大数据系统的门户和检测点、向前和向

后的溯源数据检查等方式实现。大数据系统安全和隐私的合规跨多个领域分类，涉及隐私、行业规范和本国的法律。安全取证可通过大数据安全分析服务组件取证，也可通过在大数据安全失败场景下取证。安全事件管理落实事件处理所需的各类支持资源，为用户处理、报告安全事件提供咨询和帮助。风险控制措施协调应急响应活动与事件处理活动，并与大数据服务相关外部机构（如供应链中的外部服务提供商等）提供事件应急处理机制。

4.2 大数据服务安全能力

GB/T AAAAA—AAAA《信息技术 大数据参考框架》从信息技术和数据生命周期两个维度给出了一个通用的、由逻辑功能构件组成的大数据技术架构。大数据服务安全能力应基于该参考框架涵盖数据安全和系统安全两个维度，即从数据安全角度满足划数据生命周期阶段相关的数据收集、数据传输、数据存储、数据处理、数据交换和共享、数据销毁等数据活动安全要求，从系统安全角度满足大数据平台与应用的安全规划和开发部署、大数据应用管理、大数据平台安全运维和大数据服务安全审计相关安全要求。另外，大数据服务安全能力还应该包括策略与规程、组织与人员、数据资产、数据供应链、合规性等基础安全要求。

因此，本标准以风险管理为出发点，围绕数据生命周期的数据活动和IT层次架构的信息技术价值链，建立大数据服务安全能力框架（见图1），通过在基础安全能力建设、数据生命周期服务、平台与应用服务三个方面实施安全措施，确保大数据服务的机密性、真实性和可用性。该能力框架具有如下特点：

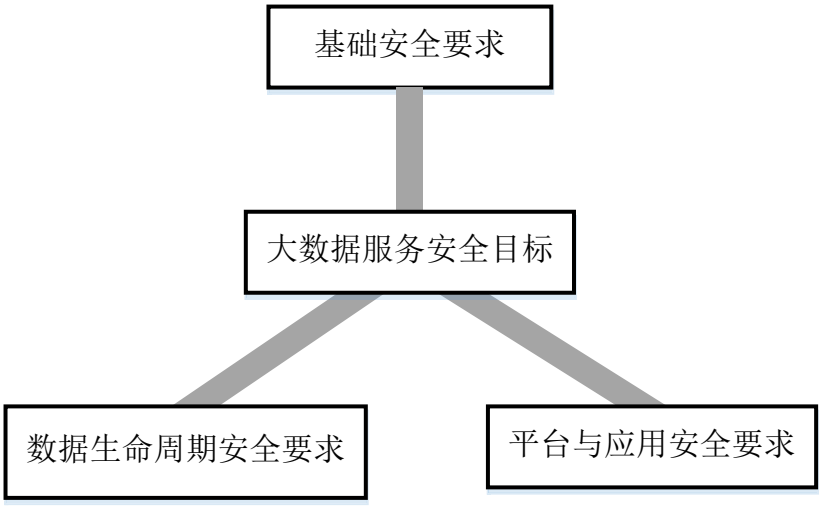


图1 大数据服务安全能力框架

a) 以安全策略与组织能力建设为基础：根据大数据服务安全目标，要求大数据服务提供者创建合适的大数据服务安全策略，建立组织安全架构和管理制度，包括系统和数据资产清单、业务流程和人员管理、安全合规性等大数据服务安全能力基础要求。

b) 强调在全生命周期内对数据进行安全保障：围绕大数据服务安全目标，要求大数据服务提供者针对大数据服务中数据生命周期相关的数据活动，形成数据服务安全规范、控制措施、管理流程等数据活动安全能力要求，目的是降低数据服务中的各种数据活动的安全风险，保障大数据业务活动的数据服务安全。

c) 强调在全生命周期内对平台与应用进行安全保障：围绕大数据服务安全目标，要求大数据服务提供者针对平台与应用从规划、开发部署到系统运维的生命周期各阶段工作，采取必要的技术和管理安全措施，目的是建立安全的大数据服务系统环境，降低大数据服务运行安全风险，保障大数据业务使命。

4.3 本标准结构

本标准共包括3个安全要求章节（第5章至第7章）。每个章节名称及其所含主要安全要求的数目是：

第5章 基础安全要求（一般要求60个，增强要求30个，共计90个）

第6章 数据生命周期安全要求一般要求142个，增强要求72个，共计214个）

第7章 平台与应用安全要求（一般要求196个，增强要求92个，共计288个）

本标准还包括附录A：大数据服务类型和大数据服务角色。

注：①本标准中章节的顺序不表明其重要性。另外，本标准的其他排列也没有优先顺序，除非特别注明。

注：② 本标准的一般要求和增强要求是从大数据服务提供者角度分类的，其他类型的大数据服务提供者应依据附录A定义的大数据服务业务模式和服务角色、大数据平台架构和大数据应用组件部署方式，选择本标准列举的大数据服务安全能力要求项进行安全建设和评估。

注：③大数据服务涉及的数据资源可能链依赖于其他机构提供的数据服务或产品，则其所承担的信息安全责任直接或间接地转移至其他机构，大数据服务提供者应以合同、协议或其他方式对大数据供应链上各方的相应安全责任进行规定并予以落实，要求他们也应具备与大数据服务提供者相当的安全防护能力。

5 基础安全要求

5.1 策略与规程

1.一般要求

大数据服务提供者应：

a) 依照风险评估结果制定符合机构大数据业务战略和目标的信息安全策略，展现机构的安全目标和原则，并能体现组织管理大数据服务安全的方法。

b) 确保所制定的信息安全策略覆盖数据生命周期的数据服务和系统服务，内容应包括目的、范围、岗位、责任、管理层承诺、内部协调及合规性等。

c) 制定策略相关的安全规程，并将策略和规程分发至大数据服务人员或角色，以推动大数据服务有关安全措施的实施。

d) 制定并实施与策略和规程相适应的大数据平台和大数据应用安全实施细则。

e) 定期审核和更新大数据服务安全策略及相关规程。

2.增强要求

大数据服务提供者应：

a) 定期评估大数据服务安全策略及规程文件的实施效果，并将效果反馈到文件的修订过程中。

b) 在机构架构发生重大调整或大数据业务发生重大变化时，及时评估大数据服务安全策略及规程文件的实施效果，并将效果反馈到文件修订过程中。

5.2 资产安全

5.2.1 数据资产

1.一般要求

大数据服务提供者应：

a) 建立数据资产安全管理策略，明确数据资产的安全管理目标、原则和范围。
b) 建立数据资产全生命周期安全管理制度和规程。
c) 按照数据资产价值和重要性建立数据资产分类分级方法和操作指南。
d) 建立数据资产机密性安全规范、管理制度和规程，如口令策略、密钥管理等。
e) 建立数据资产完整性安全规范、管理制度和规程，如语义约束、一致性规则等。
f) 建立数据资产可用性安全规范、管理制度和规程，如备份要求、备份恢复管理等。
g) 按照数据资产价值和重要性建立数据分类分级策略和规程、方法和操作指南的变更审批机制。
h) 建立数据资产组织与管理模式和数据资产登记制度。
i) 建立数据资产清单，明确数据安全责任主体及相关方。
j) 定期审核和更新数据资产安全管理策略及相关规程。

2.增强要求

大数据服务提供者应：

a) 建立机构内外部的各类数据资源的安全治理原则和数据整合规范。
b) 依据数据资产敏感度建立相应的标签、多级访问控制、数据加解密、数据脱敏等安全策略。

5.2.2 系统资产

1.一般要求

大数据服务提供者应：

a) 建立系统资产安全管理策略，明确系统资产的安全管理目标、原则和范围。
b) 建立系统资产建设和运营管理制度和规程，如规划、设计、采购、开发、运行、维护及报废。
c) 建立系统资产登记机制，形成系统资产清单，明确系统资产安全责任主体及相关方，并定期维护系统资产相关信息。
d) 建立和实施系统资产分类和标记规程，资产标记易于填写和依附在相应的系统资产上。

2.增强要求

大数据服务提供者应：

a) 建立大数据系统资产管理平台，对系统资产进行统一注册、审计、监控等。

5.3 组织和人员

5.3.1 组织结构

1.一般要求

大数据服务提供者应：

a) 建立大数据服务安全管理组织结构，按照安全角色和责任给职能部门配备合适的安全管理人员，并明确大数据安全管理的责任人。
b) 建立大数据安全领导小组，并指定机构最高管理者或授权代表担任小组组长。
c) 指定大数据系统规划、安全建设、安全运营和系统维护工作的责任部门。
d) 制定大数据安全追责制度。

2.增强要求

大数据服务提供者应：

a) 建立内部监督管理职能部门，对大数据重要业务过程和管理人员操作行为进行安全监督管理。
b) 建立集中的大数据服务安全管理及维护机构，配备必要的领导和技术管理人员，且机构最高管理人员应作为大数据安全领导小组最终责任人。

c) 设置专职的大数据服务安全关键岗位，建立规范化从事大数据平台、大数据应用以及个人信息等安全保护专责队伍。
d) 设立大数据服务安全评估及监督角色，并落实大数据服务安全检查、评估和考核具体部门或负责人。

5.3.2 人员管理

1.一般要求

大数据服务提供者应：

a) 制定大数据服务岗位人员招聘、录用、调岗、离岗、考核、选拔等管理制度。
b) 明确重要岗位人员安全责任和要求，并定期进行安全审查和技能考核。
c) 在录用重要岗位人员前对其进行背景调查，以符合相关的法律、法规、合同和道德要求，并与所有涉及大数据服务岗位人员应签订保密协议。
d) 明确重要岗位的兼职和轮岗、权限分离、多人共管等安全管理要求。
e) 对所有人员制定和实施培训计划，培训内容包括安全意识、专项技能以及补充知识方面内容，对培训结果进行评价和记录。
f) 对造成大数据安全服务破坏的人员按照规定给予处罚，并书面记录。
g) 建立第三方人员安全管理制度，对接触敏感资产的人员要求签署保密协议。

2.增强要求

大数据服务提供者应：

a) 明确关键岗位人员背景调查范围，并确定他们培训技能考核内容与频次。
b) 对关键岗位人员的安全资质进行管理，并定期对资质有效性和人员行为进行审查。

5.3.3 角色管理

1.一般要求

大数据服务提供者应：

a) 建立大数据服务相关的安全角色，明确安全角色的分配策略和授权规范，为大数据服务相关的安全角色指定安全管理人员。
b) 建立用户角色及角色权限的定期审查机制，及时更新相关角色权限及授权。
c) 明确大数据服务相关重要岗位及角色安全要求，建立重要岗位角色清单。

2.增强要求

大数据服务提供者应：

a) 依照大数据系统架构建立分层的角色体系、职责分离（如三权分立）等大数据服务安全目标建立角色管理机制。
b) 依照多租户安全管理要求建立用户应用上下文敏感的角色启动与停止管理机制。

5.3.4 人员培训

1.一般要求

大数据服务提供者应：

a) 针对不同安全角色制定相应的安全培训计划，并对培训计划定期审核和更新。
b) 针对关键岗位的转岗、岗位升级等制定相应的安全培训计划，并对培训计划定期审核和更新。
c) 按计划定期开展大数据服务安全培训，并对培训结果进行评价、记录和归档。
d) 根据大数据安全管理、大数据安全技术、大数据系统运行维护等内容对员工进行安全培训。

2.增强要求

大数据服务提供者应：

a) 依据角色人员配置安全要求，制定并开展安全实操技能的培训和考核。

5.4 制度和机制

1.一般要求

大数据服务提供者应：

a) 根据大数据安全管理策略和规程，制定具体的大数据安全管理制度和执行机制。

b) 制定大数据发布和共享细则、合同条款及审核机制，审核数据发布、转移、交换或共享的必要性、安全性及合规性。

c) 定期或在大数据安全策略或计划发生变更时，评审和更新大数据服务安全规章制度及其安全保障机制。

2.增强要求

大数据服务提供者应：

a) 制定覆盖数据生命周期的业务流程安全管理机制。

b) 对大数据安全制度和机制进行体系化的评估，如采用成熟度模型评估，并依据评估结果编制安全能力提升计划。

5.5 数据供应链

1.一般要求

大数据服务提供者应：

a) 建立数据供应链安全管理策略和方针，明确数据供应链安全管理的目标、原则和范围。

b) 制定数据供应链安全管理制度和规程，包括数据供应链参与方安全管理规范等。

c) 明确数据供应链安全管理的责任部门和人员。

d) 通过合作协议方式明确数据供应链中数据的使用目的、供应方式、参与方安全责任。

e) 对数据采集和发布设备与应用进行登记，对数据采集和发布行为进行记录和审计。

f) 对数据供应链参与方的数据消费行为进行合规性审计。

2.增强要求

大数据服务提供者应：

a) 依据数据业务链生态，明确数据链不同参与方的数据服务能力要求。

b) 设定专职的数据供应链责任部门和人员。

c) 定期对数据供应链参与方的数据安全管理能力进行审核，并对数据供应链参与方的安全风险进行评估。

d) 定期对数据供应链全生命周期安全风险进行评估。

5.6 元数据管理

1.一般要求

大数据服务提供者应：

a) 依据企业架构和数据业务建立相应的数据字典及其管理规范，如数据域、字段类型、表结构、逻辑存储和物理存储方式。

b) 依据大数据安全架构建立相应的安全元数据及管理规范，如口令策略、权限列表、授权规范。

c) 建立元数据访问控制策略、明确元数据角色及其授权控制机制。

2.增强要求

大数据服务提供者应：

a) 建立机构元数据管理系统。实现大数据服务元数据统一管理。
b) 依据资产分类分级策略建立元数据安全属性自动分级机制。
c) 建立标签策略，包括数据和主体与标签的绑定机制。

5.7 合规性管理

5.7.1 数据跨境传输

1.一般要求

大数据服务提供者应：

a) 定义个人信息和重要数据的国家或地区属性，并按照对应国家的相关法律法规要求进行数据生命周期操作。
b) 结合数据分类分级制定数据在类型、级别和敏感程度等方面要求，对需要跨境传输的数据制定数据传输安全策略。
c) 为确需跨境传输的个人信息和重要数据制定相应的数据脱敏策略和技术处理规范。
d) 结合业务需求制定跨境传输业务处理流程，建立跨境传输审批制度，建立跨境传输监督责任制，设置跨境传输操作员、审计员等角色。

2.增强要求

大数据服务提供者应：

a) 开发或采购符合法律、法规和本机构安全策略要求的数据脱敏、跨境传输的技术产品和工具。
b) 定期或发生重大信息安全事件时，对跨境传输有关制度、流程和技术工具进行审查和检验，审查检验结果需记录并提交机构最高级大数据服务安全管理组织审批。

5.7.2 个人信息保护

1.一般要求

大数据服务提供者应：

a) 在收集、存储、处理、交换和销毁阶段中涉及用户个人信息时满足国家的法律法规要求。
b) 在涉及到个人信息相关的操作时满足个人信息保护相关国家安全标准的要求，如《个人信息安全规范》。
c) 建立个人信息处理的授权审批规程和大数据分析结果的输出审核机制。
d) 建立个人信息数据的内部管控规章制度和过程，严控相关岗位人员的访问权限。
e) 采用合适的技术机制对个人信息进行保护，提供合适的保护能力，如采用脱敏规则、去标识算法、密码技术等。
f) 具备对个人信息处理操作行为的安全审计能力。

2.增强要求

大数据服务提供者应：

a) 定期对个人信息安全保护策略和措施进行评估，并及时更新。
b) 建立针对多源数据关联分析后个人信息保护的安全控制措施。
c) 具有评个人信息脱敏或去标识有效性评估能力。

5.7.3 重要数据保护

1.一般要求

大数据服务提供者应：

a) 在收集、存储、处理、分析和销毁阶段中涉及重要数据时确保满足国家的法律法规要求。

b） 建立重要数据的内部管控规章制度和过程，严控相关岗位人员的访问权限。

c） 建立重要数据处理审计机制，具备对重要数据处理操作行为的安全审计能力。

2.增强要求

大数据服务提供者应：

a） 定期对重要数据安全保护策略和措施进行评估，并及时更新。

b） 建立针对多源数据关联分析后涉及国家安全、社会公共利益等数据的控制措施。

5.7.4 密码支持

1.一般要求

大数据服务提供者应：

a） 建立符合国家密码管理条例要求有关规定的密码管理规范、管理框架和管理制度。

b） 按照国家密码管理条例要求有关规定使用和管理密码设施。

c） 按照国家密码管理条例要求有关规定生成密钥、分发密钥、存取密钥、更新密钥和销毁密钥。

2.增强要求

大数据服务提供者应：

a） 对密码管理和密钥运算操作相关的日志数据进行记录、保存和分析。

b） 具备密钥集中管理能力，保证密钥存储和更新的可伸缩性。

6 数据生命周期安全要求

6.1 数据收集

6.1.1 收集原则

1.一般要求

大数据服务提供者应：

a） 制定数据收集原则，确保数据收集是合法性、正当性和必要性。

b） 制定数据收集信息技术相关的安全规则，确保数据收集质量和安全原则的实施。

c） 确保数据搜集是与其大数据服务相关，且只采集满足业务所需的最小数据集。

2.增强要求

大数据服务提供者应：

a） 对数据收集中可能的避免合规性需求声明进行安全风险分析，建立相应的采集数据个人隐私、重要数据的安全保护。

6.1.2 数据分类

1.一般要求

大数据服务提供者应：

a） 按照数据资产分类分级策略对收集数据进行分类分级标识。

b） 对不同类别和级别的收集数据实施相应的安全管理策略和保障措施。

c） 记录并保存数据收集过程中分级分类的操作过程，对数据分级分类变更的操作记录进行审计。

2.增强要求

无。

6.1.3 数据采集

1.一般要求

大数据服务提供者应：

a) 定义采集数据目的和用途，明确数据采集源和采集数据范围。
b) 制定数据采集操作规程，规范数据采集渠道、采集流程和采集方式。
c) 对数据采集环境（如渠道）、采集设施和采集技术采取必要的安全管控措施。
d) 采取必要的技术手段，对采集到的数据进行完整性和一致性校验。
e) 明确数据采集过程中个人信息和重要数据的知悉范围和安全管控措施。
f) 记录并保存数据采集过程中个人信息和重要数据的操作过程。

2.增强要求

大数据服务提供者应：

a) 跟踪和记录数据采集过程，支持采集数据的溯源。
b) 采取必要的数据保护技术确保采集数据的真实性。
c) 采取必要的技术手段和（或）管理措施保证数据采集过程中个人信息和重要数据不被泄露。

6.1.4 数据清洗与转换

1.一般要求

大数据服务提供者应：

a) 制定数据清洗和转换过程中个人信息和重要数据安全管理规范。
b) 采取必要的技术手段和（或）管理措施，确保在数据清洗和转换过程中对个人信息和重要数据进行保护。
c) 记录并保存数据清洗和转换过程中个人信息和重要数据的操作过程。
d) 对数据清洗和转换工具或服务组件实施有效管理，做好标识并建账存档。

2.增强要求

大数据服务提供者应：

a) 具备清洗和转换过程中个人信息和重要数据产生安全问题的应急预案。
b) 采取必要的技术手段和（或）管理措施保证数据清洗和转换过程中个人信息和重要数据产生问题时的数据还原和恢复。

6.1.5 数据加载

1.一般要求

大数据服务提供者应：

a) 建立不同数据源和不同安全域之间数据加载安全策略、加载方式和授权规范。
b) 采取必要的技术手段和（或）管理措施，确保数据加载过程中的数据正确性和一致性。
c) 采取必要的技术手段和（或）管理措施，确保在数据加载过程中对个人信息和重要数据进行保护。
d) 记录并保存数据加载过程中个人信息和重要数据的操作过程。
e) 对数据加载工具和（或）服务组件实施有效管理，做好标识并建账存档。

2.增强要求

大数据服务提供者应：

a) 提供数据加载的故障恢复能力。

6.1.6 质量监控

1.一般要求

大数据服务提供者应：

a) 建立数据收集过程中质量监控规则，明确数据质量监控范围。

b) 制定数据质量要素、异常事件处理流程和规范，指定处理对应质量监控项的责任部门或人员。

c) 定义空缺值、内容冲突、不合规约束等评价数据源质量和数据收集质量管控措施的策略和标准。

2.增强要求

大数据服务提供者应：

a) 制定数据质量定级标准，明确不同级别的处理流程。

b) 定期对数据质量预判、防范和盘点，明确问题定位和修复的时间范围和责任部门或人员。

6.2 数据传输

1.一般要求

大数据服务提供者应：

a) 依据安全域内、安全域间、跨境传输等不同的数据传输场景建立相应的数据传输安全策略和规程。

b) 采用满足数据传输安全策略相应的安全控制措施，如数据安全通道、可信通道等。

c) 建立大数据传输接口安全管理工作规范，包括域内、域间和跨境数据传输接口。

d) 具备在构建传输通道前对两端主体身份进行鉴别的能力。

e) 具备对传输数据的完整性进行检测的能力，并提供相应的恢复控制措施。

f) 建立数据传输的安全技术管控措施，包括对密钥使用、通道安全配置、密码算法选择、传输协议升级等技术保护措施进行审批及监控。

2.增强要求

大数据服务提供者应：

a) 建立数据传输线路冗余机制，保证数据传输可靠性和网络线路可用性。

b) 提供覆盖国家相关规定的数据传输加密方式、密码协议与密码算法。

c) 具备实时高效的数据传输解决方案，确保数据传输效率满足相应的服务水平协议。

6.3 数据存储

6.3.1 数据存储架构安全

1.一般要求

大数据服务提供者应：

a) 建立可伸缩的分布式数据存储架构，满足数据量持续增长、数据快速读写需求。

b) 制定数据存储架构相关的安全规则和管理规范，包括数据访问控制规则、数据存储转移安全规则、数据存储完整性和多副本一致性管理规则、重要数据加密规则等。

c) 采用必要的技术或管控措施落实数据存储架构安全管理规则的实施，保证数据存储完整性和多副本一致性真实有效，具备对个人信息和重要数据加密存储能力。

d) 具备数据存储跨机柜、跨机房容错部署能力。

2.增强要求

大数据服务提供者应：

a) 具备数据存储跨地域的容灾部署能力。

b) 提供分层的数据存储加密架构，满足应用层、操作系统层、存储层等层次数据存储加密要求。

6.3.2 数据逻辑存储安全

1.一般要求

大数据服务提供者应：

a) 建立数据逻辑存储管理安全策略，以满足不同数据类型、不同数据容量和不同数据用户的逻辑存储安全管理要求。

b) 具备数据分片和分布式存储安全管理能力，满足分布式存储下数据存储完整性和机密性保护要求。

c) 建立数据逻辑存储访问控制机制，实现符合要求的数据逻辑存储隔离授权与操作能力。

2.增强要求

大数据服务提供者应：

a) 建立分层的逻辑存储授权管理规则和授权操作规范，实现对数据逻辑存储结构的分层和分级保护。

b) 具备数据存储自动压缩等数据有效存储管理能力。

6.3.3 数据存储访问控制

1.一般要求

大数据服务提供者应：

a) 为存储系统安全管理员提供用户标识与鉴别策略、数据访问控制策略，及其相关的操作规程。

b) 利用数据存储访问控制模块实施用户标识与鉴别策略、数据访问控制策略，并实现相关安全控制措施。

c) 具备数据分布式存储安全审计能力，提供受保护的审计信息存储能力。

d) 提供面向大数据应用提供者的安全控制机制，包括访问控制时效的管理和验证，以及接入数据存储的合法性和安全性认证。

2.增强要求

大数据服务提供者应：

a) 提供信息流控制机制，限制获得访问权的主体将数据传递给非授权的主体和客体，以及将权限授予其它主体和变更其安全属性。

b) 提供数据存储安全主动防御机制或措施，如基于用户行为或设备行为安全分析机制。

6.3.4 数据副本安全管理

1.一般要求

大数据服务提供者应：

a) 依据大数据服务的复制技术或数据备份与恢复技术建立数据存储冗余策略和管理制度，确保大数据服务可靠性与可用性。

b) 建立数据冗余强一致性、弱一致性等控制策略与规范，确保不同一致性水平需求的数据副本多样性和多变性存储管理要求。

c) 建立数据复制、备份与恢复操作过程规范，确保所有复制、备份和恢复日志记录都得到妥善保存。

d) 建立数据复制、数据备份与恢复定期检查和更新工作程序，包括数据副本更新频率、保存期限等，确保数据副本的有效性。

2.增强要求

大数据服务提供者应：

a) 制定对不同一致性水平要求的冗余数据提供不同等级的安全保护机制。

b) 具备数据副本存储的多种压缩策略和实现机制，并确保压缩数据副本的完整性和可用性。

6.3.5 数据时效性管理

1.一般要求

大数据服务提供者应：

a) 制定数据存储时效性管理策略和规程，如个人信息、重要数据存储应按照法律规定和监管部门的技术规范予以记录和妥善保存。

b) 明确存储数据分享、使用和清除有效期及其权利，具备数据时效性授权能力，并告知数据提供者。

c) 提供过期存储数据的安全保护规范和机制，对超出有效期的存储数据应具备再次获取数据提供者的授权能力。

d) 提供过期存储数据及其备份数据彻底删除方法和工具，能够验证数据已被完全消除或使其无法恢复。

2.增强要求

大数据服务提供者应：

a) 提供数据时效性自动检测能力，包括但不限于告警、自动清除以及拒绝访问。

b) 为不同时效性的数据提供分层的数据存储方法，提供按照时效性自动水平迁移的能力，确保高效地获得有效数据。

6.4 数据处理

6.4.1 分布处理安全

1.一般要求

大数据服务提供者应：

a) 建立数据分布式处理节点间可信连接策略和规范，如采用 Kerberos、可信模块等节点认证机制以确保数据分布式处理节点接入的可信性。

b) 建立数据分布式处理每个计算节点和用户安全属性的周期性确认机制，确保分布式处理预定义安全策略的一致性。

c) 建议分布式处理过程中数据文件鉴别和认证的策略和规范，确保分布式处理数据文件的可访问性。

d) 建立分布式处理过程中不同数据副本节点的更新检测机制，确保这些结点数据拷贝的真实性。

e) 建立分布式结算过程中数据泄露控制规范和机制，防止数据处理过程中的调试信息、日志记录、不受控制输出等泄露受保护的个人信息或重要数据。

2.增强要求

大数据服务提供者应：

a) 建立分布式处理外部服务组件审核机制，防止外部服务组件泄漏受保护的个人信息或重要数据。

b) 建立数据分布式处理节点的自动维护策略和管控措施，提供虚假结点监测、故障用户结点确认和自动修复的技术机制，避免云环境或虚拟环境下潜在的安全攻击。

6.4.2 数据分析安全

1.一般要求

大数据服务提供者应：

a) 建立数据分析相关数据源获取规范和管理机制，明确分析数据获取方式、访问接口、授权机制及其分析目标。

b) 建立大数据分析相关的多源数据聚合与关联分析操作规范和安全实施指南，确保分析数据获取质量和可信度。
c) 建立数据分析结果输出的安全审查机制和授权控制机制，并采取必要的技术手段和（或）或管控措施保证数据分析结果共享不泄露个人信息和重要数据。
d) 对数据分析结果共享的风险进行合规性评估，避免分析结果输出中包含可恢复的敏感数据，如用户重标识相关信息。
e) 建立数据派生、聚合、关联分析等安全分析过程中对数据资源操作规范，对相应的操作进行记录，以备对分析结果质量和可信性进行数据溯源。
f) 建立和落实对输出的数据分析结果进行审批的流程。

2.增强要求

大数据服务提供者应：

a) 提供基本的网络安全分析和数据安全分析算法，如沙箱技术的恶意代码检测、网络取证分析、异常流量监测、安全情报分析、用户行为分析等。
b) 具备基于机器学习的数据分析和挖据算法开发能力，包括集成外部大数据安全分析服务组件开发能力。
c) 采用技术手段处理输出分析结果，保证分析结果数据合规性，如采用符合行业规范的脱敏技术对输出结果中的敏感数据进行脱敏处理。

6.4.3 数据正当使用

1.一般要求

大数据服务提供者应：

a) 依据国家个人信息和重要数据保护的法律法规要求建立数据使用正当性原则，明确数据使用和分析处理的使用目的和范围。
b) 建立数据处理正当性的内部责任制度，保证在数据使用声明的目的和范围内对受保护的数据进行使用和分析处理。
c) 对标明使用目的数据使用提供细粒度访问控制机制，限定大数据使用者可访问的数据范围和使用目的。
d) 具备完整的数据使用操作记录和管理能力，以备潜在违约数据使用者责任的识别和追责。

2.增强要求

大数据服务提供者应：

a) 具备信息化技术手段或技术工具，对数据使用过程中的违约责任、缔约过失责任、侵权责任等进行分析和处理。

6.4.4 数据加密处理

1.一般要求

大数据服务提供者应：

a) 建立适合大数据业务的数据加密处理策略和规范，如采用搜索协同过滤加密体制，平衡数据处理的机密性和可用性需求。
b) 具备大数据环境下加密数据的透明处理能力，如使用关系加密技术、限制特定类型内积等加密机制。

2.增强要求

大数据服务提供者应：

a) 使用组签名、环形签名等技术实现认证和匿名的折中，平衡安全和隐私。

b) 使用基于属性的加密和访问控制。

6.4.5 数据处理溯源

1.一般要求

大数据服务提供者应：

a) 制定数据处理溯源策略和溯源机制、溯源数据存储和使用的管理制度。
b) 制定溯源数据表达方式和格式规范，以规范化组织、存储和管理溯源数据。
c) 采用必要的技术手段和（或）或管控措施实现分布式环境下溯源数据采集和存储，确保溯源数据能重现数据处理过程，如追溯操作发起者及发起时间。
d) 对关键溯源数据进行备份，并采取技术手段对溯源数据进行安全保护。

2.增强要求

大数据服务提供者应：

a) 建立基于溯源数据的数据业务与法律法规合规性审计机制，并依据审计结果增强或改进数据服务相关的访问控制与合规性保障工作。
b) 采取校验码、加密、数字签名等技术手段，保证溯源数据真实性和机密性。

6.4.6 数据归档处理

1.一般要求

大数据服务提供者应：

a) 依据大数据服务数据生命周期建立数据归档的相关规程。
b) 采用分布式数据存储架构实现数据归档。
c) 对用户访问归档数据的权限进行控制，确保归档数据安全。
d) 建立归档数据的压缩或加密策略，确保归档数据存储空间的有效利用和安全访问。
e) 定期地采取必要的技术手段和（或）或管控措施查验归档数据完整性和可用性。

2.增强要求

大数据服务提供者应：

a) 建立归档数据安全审计与恢复制度，指定专人负责。
b) 实现归档数据的容灾备份。

6.4.7 终端数据安全

1.一般要求

大数据服务提供者应：

a) 使用安全的软硬件设备构建终端数据处理环境，并使用工具来管理端点设备，确保终端设备接入安全。
b) 建立终端输入参数规范和约束规范，通过正则表达式等技术对输入进行检测，确保不会出现恶意输入。
c) 建立针对数据供应链或中间数据收集系统的恶意输入检测规范和管控措施。
d) 安装防火墙和防病毒软件，并定期扫描病毒木马，确保应用程序运行在安全的终端环境下。

2.增强要求

大数据服务提供者应：

a) 建立针对终端输入的攻击保护系统，防止伪造、盗用身份等攻击行为。
b) 建立终端设备数据采集、监控与审计系统，能追踪、分析和记录终端用户行为，采用人工智能技术识别异常操作。

c) 使用可信证书、可信设备、资源测试等检测并阻止伪装实体的多重身份或攻击者假定合法身份。

6.4.8 安全处理监控

1.一般要求

大数据服务提供者应：

a) 建立大数据处理集群的安全监控架构，能实时监控各节点的 CPU、内存、磁盘 IO 等计算和存储资源的状态。
b) 使用技术手段和（或）管控措施确保大数据处理集群安全高效地运行。
c) 能跟踪和控制大数据处理事务，对它进行终止、重启等操作。
d) 对大数据处理集群运行状态进行记录，并生成分析报告。

2.增强要求

大数据服务提供者应：

a) 建立应急处理机制，以应对大数据处理集群资源耗尽时的宕机风险。
b) 通过大数据处理集群的运行日志分析，能自动给出集群扩展方案。

6.5 数据共享

6.5.1 数据脱敏

1.一般要求

大数据服务提供者应：

a) 建立数据脱敏管理规范和制度，制定数据脱敏规则定义、脱敏策略配置、脱敏方法使用限制等。
b) 明确数据脱敏所涉及部门及职责分工，给出相关的数据脱敏应用场景，规定数据脱敏处理流程，并对数据脱敏过程记录进行文档化。
c) 提供数据共享过程中个人信息与重要数据所需的静态脱敏工具或服务组件。
d) 提供一种或多种风险可控的脱敏措施对敏感数据进行脱敏处理，例如：泛化、抑制、干扰等。
e) 提供脱敏数据识别和验证工具或服务组件，以验证脱敏后的数据能够满足相关法律法规的要求。
f) 能在屏蔽敏感信息时保留其原始数据格式和属性，以确保大数据应用程序可在使用脱敏数据的开发与测试过程中正常运行。

2.增强要求

大数据服务提供者应：

a) 设定专职的数据脱敏管理部门或人员，确保数据共享过程中数据脱敏合规性。
b) 明确列出需要脱敏的数据，明确列出需要脱敏的业务处理流程。
c) 提供脱敏数据发现方法和技术，包括敏感数据发现算法。
d) 明确敏感数据治理原则和规范，确保数据脱敏后的效用性。
e) 提供数据动态脱敏工具和服务组件。

6.5.2 数据导入安全

1.一般要求

大数据服务提供者应：

a) 建立数据导入安全相关的授权策略、数据不一致处理策略、数据导入控制策略。
b) 采取适当的技术措施对请求导入数据的终端、用户或导入服务组件进行身份鉴别，能验证终端、用户或服务组件的真实性。

c) 制定数据导入审计策略和审计日志管理规范，并保存导入过程中的出错数据处理记录，以辅助安全事件的处置、应急响应和事后调查。
d) 制定远程数据通道加密等技术措施，保证远程数据安全导入。
e) 在导入完成后对数据导入通道缓存的数据进行清除且保证不能被恢复。
f) 定期检查或评估数据导入通道的安全性和可靠性。

2.增强要求

大数据服务提供者应：

a) 采取两种或两种以上组合的鉴别技术对请求导入数据的终端、用户或导入服务组件进行身份鉴别。
b) 为数据导入通道提供冗余备份能力，满足可靠性要求。
c) 确保数据导入通道设置的可识别性，满足数据引入监管的要求。
d) 对数据导入接口进行流量过载监控，以确保大数据系统的安全和稳定。

6.5.3 数据导出安全

1.一般要求

大数据服务提供者应：

a) 提供多粒度的数据导出策略配置，对数据导出的范围和方式进行限制。
b) 采取适当的措施对请求导出数据的终端、用户或导出服务组件进行身份鉴别，验证终端、用户或系统的真实性。
c) 制定数据导入审计策略和审计日志管理规范，为数据导出安全事件的处置、应急响应和事后调查提供帮助。
d) 制定数据导出通道加密等技术措施，防止数据泄露。
e) 在导出完成后对数据导出通道缓存的数据进行清除且保证不能被恢复。
f) 定期检查或评估数据导出通道的安全性和可靠性。

2.增强要求

大数据服务提供者应：

a) 采取两种或两种以上组合的鉴别技术对请求导出数据的终端、用户或导出服务组件进行身份鉴别。
b) 为数据导出通道提供冗余备份能力，满足可靠性要求。
c) 提供数据导出过程中数据脱敏等数据安全保护的接口或服务。

6.5.4 数据共享安全

1.一般要求

大数据服务提供者应：

a) 明确数据共享范围和共享数据的安全控制机制，避免数据共享带来安全隐患，比如数据共享者应具备与大数据服务提供者相当的安全防护能力。
b) 明确约束大数据服务提供者与其数据共享对象的数据保护责任。
c) 审核数据的开放和共享场景，确认没有超出服务商的数据所有权和使用权范围。
d) 审核开放和共享的数据内容，确认属于满足业务场景需求的最小范围内。
e) 采用适当的安全控制措施保护数据共享过程中的敏感数据，提供数据脱敏服务，保证敏感数据的安全。
f) 提供有效的数据共享访问控制机制，明确不同机构或部门、不同身份与目的的用户的权限，保证访问控制的有效性。

g) 审计数据共享全过程，审计记录应能对安全事件的处置、应急响应和事后调查提供帮助。
h) 对共享数据及数据共享服务过程进行监控，确保共享数据的使用未超出授权范围。

2.增强要求

大数据服务提供者应：

a) 提供共享数据文档格式规范或机器可读的格式规范，保证被授权的大数据使用者能高效获取共享数据。
b) 提供专业的数据共享工具或平台，且满足数据共享过程的访问控制和数据内容保护要求。
c) 确保涉及国家秘密或国家安全的数据共享仅限于脱敏或者处理过的数据结果。
d) 定期评估数据共享平台的数据安全防护能力，确保平台满足最低数据安全防护水平。

6.5.5 数据迁移安全

1.一般要求

大数据服务提供者应：

a) 依照机构业务重组、流程再造等业务需求或系统升级、兼并和收购的 IT 系统整合需求建立数据迁移策略与规范，确保数据迁移安全符合相关法律法规要求。
b) 对数据迁移安全进行分析，制定数据迁移计划。
c) 配置必要的数据迁移工具，记录数据迁移过程，以确保数据迁移过程的可审计性。
d) 具备迁移数据完整性检测和迁移数据可溯源能力。

2.增强要求

大数据服务提供者应：

a) 建立专业化数据迁移团队，明确项目发起人、目标大数据应用团队、大数据平台团队、外部审计师、迁移实施人员等不同角色责任与义务。
b) 建立兼并和收购机构的数据流向安全管理策略与规范，确定数据流向或共享到哪里，机构相应的安全控制就应该应用到哪里。

6.5.6 数据披露安全

1.一般要求

大数据服务提供者应：

a) 建立大数据应用数据公开审核制度，严格审核发布信息符合相关法律法规要求。
b) 明确应用数据公开内容、权限和适用范围，信息发布者与使用者的权利与义务。
c) 建立应用数据公开安全事件应急处理流程，并采取必要措施保障处理流程快速有效。
d) 依法公开应用数据公告、资格审查、成交信息、履约信息等数据公开信息。
e) 建立大数据应用数据公开数据库，通过大数据平台服务实现公开数据资产登记、用户注册等共享数据和共享组件的验证互认机制。
f) 指定专人负责大数据应用数据发布的公开信息，并且对数据披露人员进行培训，确保公开的数据信息符合国家相关法律法规要求。
g) 明确公开数据信息与共享数据信息内容、各自权限和适用范围及规范。
h) 发布信息前应进行审查，防止含有非公开信息。
i) 应定期审查公开发布的信息中是否含有非公开信息，一经发现，立即删除。

2.增强要求

大数据服务提供者应：

a) 履行好信息公开职能，公开有关公共资源交易项目审核、市场主体资质资格、行政处罚等监管信息。

b) 建立大数据服务资源公开与共享市场主体信用信息库，并将相关信息纳入大数据服务系统，实现市场主体信用信息交换共享。
c) 允许授权用户判断共享伙伴的访问授权是否符合信息共享环境中的信息访问限制策略，以促进信息共享。
d) 使用自动机制协助数据披露人员做出信息共享决策。

6.5.7 隐私与合规要求

1.一般要求

大数据服务提供者应：

a) 使用职责分离原则、最小权限原则和深度防御原则，确保个人数据、重要数据等敏感数据内部控制合规与可控制。
b) 依据隐私与合规建立规范化的数据流程，并通过信息技术手段自动的管理数据流向，避免因人工管理模式或通过业务重组、兼并等方式规避隐私和合规性要求。
c) 具备个人信息与重要数据的去标识化能力，并提供采用多种匿名化技术及其有效性评估机制。
d) 重视隐私法规的意识培训，避免未来出现潜在的不合法问题。

2.增强要求

大数据服务提供者应：

a) 提供匿名化、差分隐私等去标识技术，确保个人信息、用户隐私行为数据泄露。
b) 设计和实现互连的匿名数据存储。
c) 实现数据汇聚隐私保护。

6.5.8 操作监控

1.一般要求

大数据服务提供者应：

a) 使用开放数据处理服务平台对被监控的全流量数据进行数据安全分析。
b) 采用预警平台的及时处置与人工审计相结合对高风险操作进行监控。
c) 记录操作事件中的操作人、操作内容、操作时间等信息，并将这些信息进行收集和数据清洗；并设置操作行为规则，对上述操作事件进行识别，从客户信息查询风险、操作风险、权限风险等多个角度判断操作行为是否存在风险。
d) 在办公网终端和办公网络出口部署数据防泄漏系统实时监控工具，监控及阻止敏感信息的外发行为。
e) 定期对所有办公设备上存储的敏感个人信息进行扫描，并及时采取删除或加密等处理措施。
f) 记录对开放接口的每一次调用事件，事件日志内容应包括调用者、调用接口、调用对象、调用信息类别、调用时间等；并设置接口调用和应用场景匹配识别工具，识别并监控是否存在恶意数据获取、数据盗用等风险。

2.增强要求

大数据服务提供者应：

a) 对内部系统的基础数据和事件日志，机构本地终端留存敏感数据存储情况，以及外部内部数据进行全流量监控。监控对象包括：与数据有关的内部人员的意识与行为、与业务有关的数据、与客户与合作伙伴有关的数据流动、与业务生态有关的数据安全态势。
b) 确保操作日志记录了所有数据查询系统、报表系统的访问、数据文件下载等事件，日志中包含了操作人、操作内容、操作时间等信息。
c) 具备对异常或高风险操作实现自动化实时预警的能力。

6.6 数据销毁

6.6.1 数据销毁处置

1.一般要求

大数据服务提供者应：

a) 建立数据销毁策略和管理制度，明确销毁对象和流程。
b) 建立数据销毁审批机制，设置销毁相关监督角色，审计操作过程。
c) 依照数据分类分级建立相应的数据销毁机制，明确销毁方式和销毁要求。
d) 针对存储设备和存储网络，建立基于安全策略、基于 DHT 网络等硬销毁和软销毁的数据销毁方法和技术。
e) 针对 U 盘、磁带、硬盘、光盘、闪存、固态硬盘等不同存储介质,建立硬销毁和软销毁的数据销毁方法和技术。
f) 配置必要的数据销毁工具，确保以不可逆方式销毁数据内容。
g) 按照国家相关法律和标准销毁涉密数据。

2.增强要求

大数据服务提供者应：

a) 建立基于销毁策略的数据销毁管理系统，支持大数据使用者的个性化数据销毁。
b) 建立数据销毁效果评估机制。

6.6.2 介质销毁处置

1.一般要求

大数据服务提供者应：

a) 建立存储介质销毁处理策略、管理制度和机制，明确销毁对象和流程。
b) 依据介质存储内容的重要性确定销毁要求，建立磁介质、光介质和半导体介质的销毁处理方法和机制。
c) 制定对存储介质进行销毁的监管措施，确保对销毁的存储介质有登记、审批、交接等环节的记录，加强介质销毁过程监控和销毁人员监管。
d) 涉密介质销毁如使用外包销毁服务，应按照国家相关法律和标准执行。

2.增强要求

大数据服务提供者应：

a) 采取专业的存储介质物理销毁设备进行物理销毁。

7 平台与应用安全要求

7.1 安全规划

7.1.1 战略规划

1.一般要求

大数据服务提供者应：

a) 从机构的宗旨、目标和战略出发，对大数据系统、供应链及数据资源进行统一安全规划和管理，明确大数据服务业务模式和安全保障目标。
b) 制定大数据安全战略规划，内容包括大数据服务安全章程、安全组织架构、大数据服务角色、IT 和数据供应链体系、安全实施架构、安全服务模式等。

c) 成立安全战略评议小组，对机构内外部大数据服务进行安全分析，确保大数据服务安全政策、安全目标和战略规划内容的合理性。
d) 指定和授权专门的机构对大数据服务安全能力制定近期和远期的安全保障规划，并确保机构大数据服务安全规划与组织信息系统规划的一致性。

2.增强要求

大数据服务提供者应：

a) 建立大数据服务安全管理体系，并建立大数据安全规划管理信息化平台。
b) 明确大数据服务所涉及数据的纲领性要求，包括：数据所有权、开放与共享权限等。

7.1.2 需求分析

1.一般要求

大数据服务提供者应：

a) 识别大数据服务数据源、数据类型、数据规模、数据业务等资产，明确数据和主体机密性、完整性和真实性安全目标。
b) 识别数据生命周期关键业务和支撑大数据服务所需的安全能力需求，明确数据业务持续运行的安全策略和控制范围，以及大数据系统健康运行安全目标。
c) 分析大数据服务安全现状，准确理解数据服务和系统服务的安全要求，并基于风险分析等方法挖掘数据驱动的安全需求。
d) 成立大数据服务多方共同组成的需求分析评审机构，成员包括：大数据服务建设者、管理者、使用者、运营者等，确保需求分析的完整、合理和透明。

2.增强要求

大数据服务提供者应：

a) 依据数据资产的分类分级要求，明确大数据服务安全需求和安全控制措施实施的优先级。
b) 利用专业的第三方机构开展需求分析，并配置专职的安全需求分析人员，确保大数据服务相应安全需求的正确传递。

7.1.3 方案评估

1.一般要求

大数据服务提供者应：

a) 建立专门的安全方案评估组织，并规范方案评估流程和相关管理制度。
b) 具备大数据系统建设相关文档，如可行性分析报告、建设方案、实施方案等，并保证所提交材料的真实性并承担责任。
c) 明确大数据系统的安全评估依据，并确保方案评估符合国家相关法律、法规和相关规范的要求。
d) 开展方案评估检查工作，内容包括安全体系、安全要求、实施方式等。
e) 识别大数据系统相关的安全风险评估要素，并根据重要性程度划分等级。
f) 形成评估报告，报告内容包括：评估依据、安全评估项、结论和建议等。
g) 定期总结和完善现有评估安全方案，保证与产品服务的迭代更新相同步。

2.增强要求

大数据服务提供者应：

a) 建立系统安全规划评价指标体系，并形成安全评估关键指标和评估因素集。
b) 持续跟踪和评估系统安全方案的执行情况，并反馈到安全规划。

7.2 开发部署

7.2.1 安全架构

1.一般要求

大数据服务提供者应：

a) 建立大数据服务安全架构，并确保安全架构描述的大数据服务安全功能在设计过程和实现方面的正确性。
b) 确保安全架构描述与大数据系统设计文档中包含的安全功能抽象描述级别相一致。
c) 确保安全架构文档描述的安全域与大数据应用和大数据安全功能框架要求一致。
d) 确保安全架构文档描述大数据应用和大数据平台中安全功能初始化过程，以确保平台与应用初始化过程的安全性。

2.增强要求

大数据服务提供者应：

a) 确保安全架构描述文档中包含的信息足以证明大数据服务安全功能能够保护自身不受非可信主体的篡改。
b) 确保安全架构描述文档中提供了充分的分析以证明大数据服务安全功能的设计机制在实现中不能被绕过，并证明提供的大数据系统安全功能已经正确实现。

7.2.2 功能规范

1.一般要求

大数据服务提供者应：

a) 提供功能规范，并明确功能规范到大数据服务安全功能要求的追溯关系。
b) 确保提供的功能规范完整地描述大数据服务安全功能，并明确所涉及的数据供应链关系和服务组件。
c) 确保提供的功能规范描述了所有的大数据服务安全功能接口的设计目的和使用方法，并提供安全功能接口相关的所有参数。
d) 确保提供的功能规范能够证实安全功能到大数据服务安全功能接口的追溯要求。

2.增强要求

大数据服务提供者应：

a) 确定功能规范是安全功能要求的一个准确且完备的实例化。

7.2.3 开发与交付

1.一般要求

大数据服务提供者应：

a) 提供安全功能相关的详细设计文档，描述每一个安全功能模块，包括模块接口的返回值、与其它模块间的关系及调用的接口。
b) 设计和实现功能规范规定的安全功能，并提供内部描述和论证过程说明，以解释或证实内部结构的合理性。
c) 提供系统设计描述与实现表示示例之间的映射关系，证实功能规范、设计、实现和部署之间的一致性。
d) 采取适当的技术手段和（或）或管控措施，确保开发环境的隔离性。
e) 基于权限最小化原则为合作方分配权限，限制其权限局限于工作所需的数据资源，并保证重要、敏感信息应经过脱敏后方可提供给合作方使用。

f) 采取必要的物理的、程序的、人员的及其它方面的安全措施保护系统设计和实现的机密性和完整性。
g) 制定系统实现与编码安全规范，并在开发过程中严格遵循。
h) 对系统执行安全测试，确保所交付的系统满足安全要求。
i) 提供系统开发与交付的程序化文档，包括服务组件更新相关的所有程序。

2.增强要求

大数据服务提供者应：

a) 提供大数据系统交付文档,确保在向用户分发大数据服务组件期间大数据服务系统的安全性得到维护。
b) 根据系统的安全功能做相应的安全威胁分析，并针对威胁预备有相应的处理措施。
c) 确保交付使用的开源软件经过了安全性分析。

7.2.4 安全部署

1.一般要求

大数据服务提供者应：

a) 建立开发者交付程序至大数据服务系统的安全交付流程。
b) 描述大数据服务每种角色在安全部署过程中应被控制访问的功能和权限。
c) 对大数据服务每种角色描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时应指明安全值。
d) 对大数据服务的每一种用户角色进行描述,以保证可以充分实现安全策略与规范中描述的运行环境安全目的所必须执行的安全策略。

2.增强要求

大数据服务提供者应：

a) 提供明确的大数据系统安装部署的准备程序文档，确保大数据部署工作准备妥当；
b) 确保面向大数据服务每一角色的操作指南是明确合理的。
c) 对部署过程中需要安装加载的主要版本进行完整性校验，防止部署过程引入安全问题。
d) 在安装部署后清除部署产生的过程文件，防止部署过程使用的高权限文件泄露。

7.2.5 边界防护

1.一般要求

大数据服务提供者应：

a) 规划与安全级别相应的安全域和安全防护边界，包括安全控制策略和管理规则。
b) 规划与业务控制、应用隔离相关的安全域和安全防护边界，包括安全控制策略和管理规则。
c) 在安全域边界处部署安全防护设施，对异常事件、潜在侵害等进行检测及防护。
d) 在安全域之间采用较严格的安全防护机制，如身份鉴别、连接管理、网络访问控制安全策略、入侵防范、信息过滤、边界完整性检查等。
e) 制定安全防护设施更新管理规则，并采用必要手段确保规则落实。

2.增强要求

大数据服务提供者应：

a) 提供个性化的多租户边界防护措施和机制。
b) 提供安全域/子安全域定义、安全域间数据隔离机制和授权用户/角色的访问控制机制。

7.2.6 服务接口

1.一般要求

大数据服务提供者应：

a) 提供系统管理员、安全管理员、安全审计员等用户角色接口和监管角色接口。

b) 明确规定每类角色接口的安全需求和安全控制措施，如身份鉴别、授权访问、签名、时间戳和安全协议。

c) 明确每类接口的使用安全限制，如远程连接等被限制使用的功能和权限。

2.增强要求

大数据服务提供者应：

a) 支持对接口访问过程的审计需求，并对接口访问提供必要的审计和监管功能。

b) 对系统内跨安全域的接口传输应采用加密传输的方式。

7.2.7 文档管理

1.一般要求

大数据服务提供者应：

a) 对大数据服务系统实施文档管理，文档管理范围包括组织方针策略、规章制度、系统方案、实施手册等。

b) 确定文档的创建、评审、批准、发布、存档流程，明确文档管理流程各阶段相应责任人，明确安全责任。

c) 确定文档的保存介质要求和保存时间要求，确保文档的可用性和完整性。

d) 定期对文档进行评审、更新、批准和发布，确保用户使用最新版本的文档。

e) 指定责任机构负责建立和维护文档管理体系，并负责文档版本变更维护。

f) 为系统文档进行分类分级管理。

2.增强要求

大数据服务提供者应：

a) 在服务商内部提供平台进行文档管理，并根据不同角色的权限确定查看权限。

b) 确保相应文档在产品或服务进行升级时进行必要的更新和版本标识。

7.3 应用安全

7.3.1 应用程序管理

1.一般要求

大数据服务提供者应：

a) 建立大数据应用注册和大数据应用安全元数据管理策略与规程,包括相关的外部服务组件与数据源安全接入管理规程。

b) 建立大数据应用安全评估策略与规程，依据国家法律法规、行业规范、业务需求以及合同要求等明确对关键基础设施的采购、开源程序与组件使用和外部数据供应链的安全评估流程、方法和要求。

c) 建立大数据服务应用程序上线管理规程，明确书面授权流程和相关角色职责，授权单应详细标明应用程序名称、版本、来源、开发者、功能、部署位置、第三方安全报告、内部安全评估结果和特别安全要求等有效表征应用程序身份的签名信息和软件属性信息。

d) 明确应用程序在与大数据平台、其他可信 IT 产品之间数据传输过程的保护方式，如使用 SSL、TLS 等对所有传输的数据或所传输的敏感数据进行加密。

e) 登记和管理大数据应用服务终端和网络设备，确保安全地管理如如物联网设备、移动终端等终端设备。
f) 建立和维护大数据应用相关的终端设备、使用用户、设备参数、终端数据等安全要素。
g) 检查应用程序安装包及升级包的电子签名，确保在安装应用组件前通过大数据平台从密码学的角度验证应用程序。
h) 确保应用程序能够自己实现或利用大数据平台提供的功能来查询运行软件的当前版本。
i) 确保应用程序能处理可预知的错误操作，不应影响大数据生态系统的正常工作。
j) 建立大数据应用程序更新和补丁安装管理规程，明确书面授权流程和相关角色职责，确保应用程序自己实现或者利用大数据平台提供的功能来检查更新并安装应用组件补丁。
k) 建立大数据应用程序下线管理规程，明确书面授权流程和相关角色职责，应制定下线工作方案，明确应用下线过程中的数据迁出、转移等处置方案和操作规范，并将数据销毁记录作为应用程序安全下线的必要性验收材料之一。应用程序卸载时应确保同时删除应用配置、审计/日志和应用数据输出文件外的其它运行信息。

2.增强要求

大数据服务提供者应：

a) 确保大数据应用程序自身的安全性，不应设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。
b) 确保应用程序具备防止漏洞利用能力，如不分配任何同时具有写权限和执行权限的内存空间、只为进行即时编译的函数分配同时具有写权限和执行权限的内存空间等。
c) 确认第三方服务组件库给出了完备的技术文档和操作指南，以保证应用程序在打包时只包含了必要的第三方库。

7.3.2 缺省配置安全

1.一般要求

大数据服务提供者应：

a) 确保在使用默认身份凭证或没有配置身份凭证时，应用程序只能提供用于设置新身份凭证所必须的功能，如使用默认口令登录系统时，仅允许用户进入修改口令界面，且未完成默认口令修改，应用程序不能提供其他功能。
b) 要求应用程序在默认安装模式下提供更安全的功能模块、开启更安全的安全配置。如应用程序同时提供口令登录和数字证书登录两个模块，则在默认安装模式下，应用程序选择安装数字证书登录功能模块。
c) 确保在应用程序默认配置下，未授权用户无法访问应用程序和大数据平台相关的文件及数据。
d) 限制应用程序缺省用户的默认访问权限，如默认使用非 root 的最小权限用户启动程序。
e) 确保应用程序默认启用用户账号安全配置功能，包括口令长度、口令复杂性、使用期限限制、账号锁定策略等。
f) 确保应用程序在默认安装配置下，开启组件安装更新、参数修改等必备的日志审计功能。

2.增强要求

大数据服务提供者应：

a) 确保应用程序只调用大数据平台提供商推荐的机制来存储以及设置应用程序的配置选项。
b) 确保应用程序只使用大数据平台支持的服务和应用编程接口（API）。

7.3.3 身份凭证存储

1.一般要求

大数据服务提供者应：

a) 明确应用程序身份凭证持久化存储方法，如不存储身份凭证、使用平台提供的功能来安全存储所有身份凭证或应用程序自己实现安全存储所有身份凭证的功能。
b) 明确应用程序用身份凭证信息内容，如密钥、PKI 私钥、口令等。
c) 明确用户个人信息采集、存储和使用的安全保护方法和管控措施。
d) 建立应用程序身份凭证存储方法的评估程序，确保其符合大数据服务系统的安全策略和规程要求。

2.增强要求

大数据服务提供者应：

a) 确保安全规范文档中列出了身份凭证持久化存储方法的目的以及存储方法。

7.3.4 身份标识与鉴别

1.一般要求

大数据服务提供者应：

a) 建立身份标识和鉴别管理规范，并指定专职安全管理人员对大数据服务相关的人、组、角色、设备、应用等标识符信息和鉴别凭证信息进行管理。
b) 建立个人、组、角色、设备、应用等大数据应用相关的身份鉴别机制，确保正确标识和鉴别大数据服务用户。
c) 具备终端用户层身份管理能力，能自动判断大数据应用中用户身份信息，确保用户标识与应用层授权信息之间的映射关系。
d) 使用安全协议完成身份鉴别过程，避免用户鉴别相关信息泄露，给出鉴别失败采取的安全控制措施。
e) 建立用户口令长度、口令生存期、口令复杂度等口令管理策略，确保基于口令的身份鉴别安全性。
f) 对存储和传输的用户口令等鉴别凭证信息进行加密。
g) 定期对用户帐号的使用情况进行审核和安全性分析，确保用户身份和帐号合法性。
h) 确保使用的密码模块对操作人员设置了鉴别机制，且满足国家密码管理的有关规定。
i) 对重要数据或重要模块的操作应采用两种或两种以上组合的鉴别技术对用户身份进行鉴别。
j) 对用户账号的建立、更改、授权、禁用和终止行为进行安全审计。
k) 对公众可访问的大数据系统服务，向用户显示必要的用户使用系统的信息，如显示前一次登录日期和时间、近期登录地点等。
l) 应在准予用户访问系统之前，向用户显示系统使用通知消息或旗标，根据有关法律、法规、政策、标准等提供隐私和安全通知。
m) 使用密码验证及加密传输机制，以保证远程访问会话的机密性和完整性。

2.增强要求

大数据服务提供者应：

a) 在所有应用中对关键岗位的用户采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，其中至少一种属于基于生物特征或基于数字证书的方式。
b) 支持分布式计算技术、虚拟计算技术等计算方式的身份鉴别，例如基于硬件安全模块支持下的可信计算体系，从而提高大数据服务用户身份鉴别的安全性。
c) 建立统一身份管理和鉴别平台，实现对应用层用户的证书、账户、授权、认证和审计的集中管理、整合大数据服务资源、实现应用数据共享和全面集中管控目标。

d) 使用安全性断言标记语言来定义身份和角色，添加安全和隐私保证等要求，以支持多个服务身份使用大数据服务。
e) 提供可插拔身份验证模块的支持。

7.3.5 平台资源获取

1.一般要求

大数据服务提供者应：

a) 确保让大数据使用者知道应用程序要访问的系统资产，并向用户发出通知，如网络连接、位置服务、USB、蓝牙等硬件资源清单。
b) 确保让大数据使用者知道应用程序要访问的系统敏感数据资产,并向用户发出通知,如地址簿、系统日志等敏感信息源。
c) 确保应用程序只访问有足够理由访问的资源，如检查应用程序开发者提供的文档，以确认每个需要访问的资源的访问理由。

2.增强要求

大数据服务提供者应：

a) 确保应用程序依据业务需求限制了必要的内部与外部网络通信或由用户初始化的网络通信。
b) 确保应用程序依据个人信息保护或重要数据保护需求,在应用程序启动时弹出对话框告知用户应用程序要传输个人信息等通知。

7.3.6 授权与访问控制

1.一般要求

大数据服务提供者应：

a) 建立大数据应用的物理与逻辑访问授权粒度、规范和控制机制，确保大数据服务相关的数据和系统资产的访问得到正确授权。
b) 依据资产管理策略和资产标签、安全属性设置授权和访问控制措施，确保大数据应用具有细粒度授权访问控制管理能力。
c) 制定信息流控制策略，控制大数据平台不同大数据应用之间或大数据应用与外部 IT 系统间的数据导入、导出与共享操作（信息流动）。
d) 正确地为大数据服务相关的个人、组、角色、设备、应用访问数据和系统资产实施经批准的授权。
e) 提供用户根据业务需求自定义的授权访问策略的能力,并根据业务需求对各角色授予的权限进行审核，确保限定在满足业务场景需求的最小范围内。

2.增强要求

大数据服务提供者应：

a) 提供基于属性访问控制引擎，提供策略编辑点、策略决策点、策略执行点和政策访问点等面向数据对象的授权管理和访问控制功能。
b) 自动监视和控制远程访问会话，以检测网络攻击，确保远程访问策略得以实现。

7.3.7 多租户数据安全

1.一般要求

大数据服务提供者应：

a) 建立多租户环境大数据服务程序隔离策略与规范,采用经评审的多租户技术保护各租户的应用程序运行环境。

b) 建立租户数据资源隔离策略与规范，利用如切割数据库、切割存储区等机制来隔离租户数据资源，并采用必要的数据加密策略保护租户的敏感数据。
c) 建立租户大数据服务可伸缩性管理策略与规范，利用虚拟化技术来保证多租户并发访问海量数据服务的可靠性和高效性要求。
d) 建立租户数据剩余信息保护、租户数据物理清除等规范与机制，确保租户数据存储的文件/对象删除后，防止被删除租户数据的非法恶意恢复。
e) 建立多租户大数据服务可用性保障策略和机制，采用如租户服务组件故障转移、租户数据存储容量扩展、快照数据一致性检查、租户数据存储管理、租户数据多副本自动管理等保障措施。

2.增强要求

大数据服务提供者应：

a) 提供透明的租户数据隔离机制，允许租户使用不同技术实现租户数据的安全保护。
b) 提供可定制的多租户架构应用软件，通过大数据平台层服务接口或工具的支持，提升租户特定安全要求。
c) 支持在虚拟网络中隔离租户应用程序或租户数据，并使用符合国家密码相关标准的安全连接方式构建大数据平台。

7.3.8 敏感数据处理

1.一般要求

大数据服务提供者应：

a) 根据业务需求和安全策略建立敏感数据清单，明确敏感数据识别规则与机制。
b) 具备应用敏感数据加密存储和计算能力，明确使用的方法，如使用平台提供的功能来加密敏感数据或应用程序实现自身对敏感数据的加密。
c) 对敏感数据传输、存储和使用进行监控，确保在数据收集、存储、处理、归档和销毁过程中个人信息、重要数据等敏感数据保护符合相关的法律法规要求。
d) 能针对不同应用场景的敏感数据使用提供多种数据脱敏算法。
e) 建立覆盖数据生命周期的审计机制，确保敏感数据使用的合规性。

2.增强要求

大数据服务提供者应：

a) 制定基于数据特征学习等技术的敏感数据识别自动方法与算法。
b) 建设数据脱敏自动化处理平台，提供如匿名、泛化、随机和加密等脱敏机制。
c) 建立数据脱敏效果评估机制，结合数据和应用场景评估脱敏效果，定期执行。
d) 提供密码数据透明处理技术，如提供属性加密、同态加密等功能机制。
e) 提供虚拟化数据处理安全机制，隔绝虚拟系统间敏感数据的交叉泄露。
f) 建立数据沉淀评估和防控机制，评估和防范数据使用通过积少成多，积部分成整体等数据沉淀的方法获得敏感数据。

7.3.9 数据导入导出

1.一般要求

大数据服务提供者应：

a) 综合存储容量、数据量增长速度、业务需求、存储介质、性能等因素制定数据导出导入策略与规程，防止重要数据丢失，最大程度减少数据损失。
b) 建立导出数据管理策略和机制，建立数据导入导出安全评估机制和授权审批流程。

c) 使用不同的存储介质满足数据分门别类存储管理需求，并定期验证到处数据的完整性和可用性。
d) 建立存放导出数据介质的标识规范。标识必须符合统一的命名规则，注明介质编号、导出时间和有效期等重要信息。
e) 提供多种粒度的数据逻辑数据导出与导入方式，如数据库、模式、用户指定对象等不同粒度的数据导入与导出。
f) 执行导入导出数据结果检查，确保数据的完整性和正确性。
g) 记录数据导出与导入操作信息，例如作业信息，作业周期、介质型号、介质容量、转存情况、相关变更记录等信息。
h) 采用加密机制、访问控制等技术手段保障导出数据的机密性、完整性和可用性。
i) 定期验证导出数据的完整性和可用性。

2.增强要求

大数据服务提供者应：

a) 掌握数据自动备份管理所需的平均失效前时间、平均恢复前时间、平均故障间隔时间指标参数计算依据，配置相应的数据导入导出自动化软件。
b) 具备异地的数据在线导入与导出能力，定期略自动的对用户数据进行异地存储。
c) 依照数据使用热度等自动的对备份数据进行重组和压缩，保证海量数据的可用性。
d) 具备按照数据备份和恢复频度对用户备份数据进行自动压缩存储功能。

7.3.10 用户隐私保护

1.一般要求

大数据服务提供者应：

a) 建立应用程序用户隐私保护相关的策略和规程，明确应用程序开发、运营和运维等环节涉及个人隐私行为数据监管责任。
b) 建立用户隐私行为数据收集和使用授权审批机制，明确用户行为数据采集范围和用途，并应按照法律规定和监管部门的技术规范予以记录和妥善保存。
c) 在大数据应用及关联业务组件下线、设备退网时，妥善转移、转存、销毁保存的个人隐私行为数据，避免发生隐私泄露事件。
d) 收集、使用用户隐私数据时，应遵循知情同意和单独同意原则，不得用于与业务无关的用途，不得非法出售或者提供给其他组织和个人。
e) 建立用户投诉处理机制，公布有效的联系方式，接受与用户隐私数据保护和和更新用户隐私数据有关的投诉。

2.增强要求

大数据服务提供者应：

a) 发生隐私泄露立即采取补救措施，并告知可能受影响的用户。
b) 提供用户隐私自定义级别设置，并制定各级别隐私保护信息内容。

7.3.11 应用行为监测

1.一般要求

大数据服务提供者应：

a) 建立覆盖数据生命周期的大数据应用行为监控策略和规程。
b) 支持用户自定义监控规则设置，能够对个人信息和重要数据异常操作行为进行监测和告警。
c) 具备对应用异常行为信息记录、统计和分析能力。

2.增强要求

大数据服务提供者应：

a) 建立面向监管机构和有特定要求用户的应用行为监测管理机制，授权审批后提供在线监管接口。

b) 建立基于大数据的应用行为记录和分析平台，提供安全性分析能力。提供面向大数据服务通信协议的用户行为识别和提取组件或接口。

c) 提供端到端业务模型和行为监控规范体系和操作指南。

7.4 安全运维

7.4.1 系统配置管理

1.一般要求

大数据服务提供者应：

a) 制定并实施系统配置管理规程，建立系统配置管理组织结构，明确配置管理人员的角色和职责，如系统管理员、系统操作员、系统安全员、系统审计员、数据库管理员等角色。

b) 依据业务需求和管理对象，规定配置管理的审批、操作和审计流程，如主机配置项、网络配置项、应用服务组件配置项等系统配置标识及内容配置与变更有关活动。

c) 依据风险评估结果制定大数据系统安全功能基线配置清单，制定日常配置检查内容清单，并按照最小特权原则对大数据系统安全功能进行必要的配置。

d) 按照大数据服务水平协议，对大数据系统中所使用的信息技术产品的配置项进行参数设置，记录并维护大数据系统当前的安全配置信息。

e) 按照所采购软件使用与限制策略和对软件使用的授权规则，禁止或限制使用大数据系统特定功能、端口、协议或服务。

f) 明确需要定期变更的受控配置列表，并定期对大数据系统的病毒库、入侵检测规则库、防火墙规则库、漏洞库等与信息安全相关的重要配置项进行更新。

g) 审查所提交的大数据系统受控配置的变更事项，根据安全影响分析结果进行批准或否决，并记录变更决定。

h) 限制系统开发方和集成方对生产环境中的大数据系统及其硬件、软件和固件进行直接变更，并对配置和变更动作进行审计。

i) 在实施配置或变更之前，对受控配置项和变更项进行测试、验证和记录，对系统变更项进行分析，以判断该变更事项对大数据服务安全带来的潜在影响。

j) 监控配置项设置参数的变更，合理启用安全设备的监测、预警及防护等功能。

k) 提供应对未授权变更有相关响应措施，包括：更换有关人员，恢复已建立的配置，或在极端情况下中断受影响的信息系统的运行等。

2.增强要求

大数据服务提供者应：

a) 定期或在业务、系统架构发生重大变更时，开展配置管理效果风险评估，依据评估结果修订基线配置要求和配置内容，如至少每年开展一次风险评估和修订配置要求。

b) 定期或在业务、系统架构发生重大变更时，对风险评估策略和效果进行评估，根据评估结果重新修订系统配置管理规程、调整组织管理结构、配置管理流程等。

c) 定期对大数据系统配置进行审查，以标识不必要或不安全的功能、端口、协议或服务配置项。

d) 使用系统配置工具或自动机制对配置项的参数进行集中管理、应用和验证。

e) 能实时感知大数据基础设施与虚拟资源状态的变化，具有自动调整系统服务安全策略配置的能力。

7.4.2 系统补丁管理

1.一般要求

大数据服务提供者应：

a) 建立补丁管理规程，至包括下载、测试、分析、分发、安装、归档等流程和内容，确保系统补丁的规范化管理。
b) 建立补丁管理团队，建立和上级安全主管部门、外部安全机构的畅通沟通渠道，及时了解漏洞爆发信息和响应信息安全事件，及时处置补丁下载、测试和安装等工作。
c) 建立系统补丁分发与管理框架，明确补丁下载与更新机制，如补丁管理可以由系统安全事件触发，也可以按设置的周期定期触发。
d) 具备补丁部署安装前的补丁兼容性测试能力，记录补丁更新过程中产生的问题。
e) 具备补丁检查功能，确认补丁安装成功。

2.增强要求

大数据服务提供者应：

a) 建立系统补丁管理系统，通过软件进行系统更新与补丁安装。

7.4.3 IT 供应链安全

1.一般要求

大数据服务提供者应：

a) 建立 IT 供应链安全管理规程，明确 IT 供应链筛选机制，明确筛选指标和评价方法。
b) 对 IT 供应链涉及的参与方进行安全背景审计，明确他们参与数据采集和系统服务相关的角色和业务。
c) 建立对数据供应链中数据源规范化机制和接口使用规范，并对供应链重要操作进行日志记录和审计等。
d) 采取必要的技术和管理措施落实供应链替代措施，确保供应链出现意外情况时进行响应。
e) 建立供应链运营管理组织结构、供应链主数据模型、数据质量和数据溯源处理机制。

2.增强要求

大数据服务提供者应：

a) 建立供应链数据源数据信息萃取、整合与优化利用等数据聚合信息链模型。
b) 建立供应链考核评价机制，定期对供应链进行风险评估和安全考核，如每年至少考核一次。
c) 建立数据供应链质量管理和评价反馈机制。

7.4.4 外部组件使用

1.一般要求

大数据服务提供者应：

a) 建立外部服务附件合作方安全管理制度。
b) 建立外部服务商准入机制、考核和评分机制，建立黑名单和惩罚机制。
c) 与外部服务组件提供商签订服务组件合作协议，明确与外部服务组件提供商的义务和责任，如避免同一合作方参与大数据系统安全运营过多环节。
d) 保外部服务组件理解大数据系统的信息安全策略和正确实现了要求的安全措施，并通过了第三方评估机构的测试

e) 与外部服务组件提供商建立组件使用安全策略，明确外部组件使用的条件和访问范围。
f) 采取必要的技术手段或安全管控措施确保大数据使用者通过这些服务组件对系统和数据资源进行授权和使用。
g) 对外部服务组件的使用者、使用目的、实际操作等信息进行审计，确保大数据服务可追溯性。

2.增强要求

大数据服务提供者应：

a) 对外部服务组件提供商进行资质和安全能力评估，并应与外部服务组件供应商形成应急联动机制。
b) 确保外部服务组件正确实现了大数据系统的信息安全策略和安全计划所要求的安全措施，并通过了第三方评估机构的测试。
c) 限制授权人员在外部服务组件使用由大数据服务提供者控制的存储介质、数据文件等敏感数据资源。

7.4.5 安全事件管理

1.一般要求

大数据服务提供者应：

a) 建立并实施安全事件预警通报制度，及时向大数据服务安全管理部门报告相关安全事件，并根据预案实施应急措施。
b) 建立安全事件预警、舆情监控和应急处置规程，确保安全事件预警预防、应急保障准备、应急响应和跟踪总结。
c) 建立和上级安全主管部门、外部安全机构的畅通沟通渠道，建立安全事件报告渠道，及时报告影响较大的安全事件、获得最新信息安全事件通报和处置办法。
d) 为安全事件的处理提供必需的资源和管理支持。

2.增强要求

大数据服务提供者应：

a) 建立安全事件处理最佳实践知识库、以用于未知安全事件处理、培训及演练计划。
b) 建立专门负责应急响应的组织，负责收集安全事件相关信息，并传递给开发运维团队进行处理。

7.4.6 安全风险评估

1.一般要求

大数据服务提供者应：

a) 识别系统面临的威胁、存在的弱点、造成的影响等风险评估要素，建立大数据服务安全风险评估机制。
b) 定期、在系统与运行环境发生重大变更、或在出现其他可能影响系统安全状态的条件时开展风险评估，并根据评估结果落实安全整改措施。
c) 及时向大数据服务安全管理部门报备系统安全风险评估情况，给出相应的安全加固措施或改进建议。
d) 接受大数据服务安全管理责任部门定期开展的系统服务安全评估情况抽查。

2.增强要求

大数据服务提供者应：

a) 具备安全风险分等级处理能力。

7.4.7 系统备份与容灾

1.一般要求

大数据服务提供者应：

a) 根据业务目标和整体安全策略建立系统容灾备份策略和规程,支持大数据使用者制定自身的系统和数据备份策略。

b) 设立系统灾难备份恢复组织机构，明确各岗位职责及人员需求，参与人员至少包括由业务、技术、后勤等相关部门工作人员，涉及灾难恢复规划建设、运行维护、应急响应和灾难恢复等各阶段工作所需的人员。

c) 根据长期可持续发展和业务战略目标，评估大数据服务信息系统面临的灾难风险，明确灾难恢复需求、恢复策略，并划分系统的灾难恢复能力等级，制定和实施相应的灾难备份规划。

d) 结合系统运行状态实际情况开发包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册，并定期组织灾难恢复预案的教育与培训，确保相关人员熟知预案，培训后保留培训的记录。

e) 具备异地系统与数据备份系统，并定期对系统和用户数据进行远程备份。

f) 定期进行系统灾难恢复演练以证明系统灾备方案有效性，根据演练情况修订灾难恢复预案。

g) 制定措施，及时将大数据服务系统和相关数据面临的风险信息告知用户。

2.增强要求

大数据服务提供者应：

a) 在灾难备份恢复组织机构中的数据备份、安全监控、应急响应等关键岗位设立专职人员，其余人员可为兼职，重要岗位的人员应有备份。

b) 根据信息系统和分支机构情况设立不同级别的灾难备份恢复组织机构,如设立总部和分支机构的多级灾难备份恢复组织机构。

c) 建设或租赁异地灾难备份中心，包括备用数据处理系统、备用网络系统、备用基础设施等。

d) 每年应至少组织一次实战演练。

7.4.8 系统应急响应

1.一般要求

大数据服务提供者应：

a) 建立大数据服务安全应急响应的工作机构，如包括应急响应领导小组、应急响应专家小组、应急响应技术保障小组、应急响应实施小组、应急响应日常运维小组等工作小组，明确应急响应个小组相关岗位角色及职责。

b) 建立应急响应策略和规程，根据业务重要性和影响程度制定信息安全事件分级分类章程，明确不同级别事件处置要求。

c) 与相关管理部门、设备设施及软件服务提供商、安全机构、新闻媒体等利益相关方保持联络和协作，以确保在信息安全事件发生时，能及时通报相关情况并获得适当支持。

d) 制定应急响应预案，明确应急响应处理流程和人员、工具、联系方式等资源。

2.增强要求

大数据服务提供者应：

a）依照主管部分要求制定系统应急响应实战演练策略,如每年应至少组织一次实战演练。

7.4.9 业务连续性计划

1.一般要求

大数据服务提供者应：

a) 应建立并执行符合国家相关标准的业务连续性计划。

b) 定期对业务连续性带来的风险进行评估，并将相关的风险信息告知客户。
c) 根据业务战略目标，制定和实施相应的灾难备份规划，明确系统的灾难恢复能力等级、灾难恢复需求、恢复策略。
d) 定期开展业务影响分析和风险评估，落实业务连续性相关内容的培训。

2.增强要求

大数据服务提供者应：

a) 对所涉及的大数据服务关键基础设施定期进行系统切换试验，并根据实际需求优化数据与系统资源备份方案。
b) 进行业务连续性计划演练，以检验业务连续性计划的完整性、可操作性和有效性，验证业务连续性及数据和系统资产的可用性。

7.4.10 密钥管理与服务

1.一般要求

大数据服务提供者应：

a) 采用符合国家、行业或机构要求的密码管理相关标准或规范的密钥生成算法，并采用合规的密钥长度或域参数来生成密钥。
b) 对密钥可能拥有关联的元数据，如使用的时间段、身份验证约束、密钥建立约束、域参数和它们使用的源验证、完整性和机密性保护等安全服务进行关联，确保密钥可以关联到正确的密码资源数据。
c) 提供密钥状态管理功能，包括但不限于密钥激活、密钥失效、密钥挂起、密钥更新、密钥撤回、密钥归档、密钥销毁等涵盖从密钥产生到最终销毁过程操作。
d) 执行密钥管理功能的各方身份应被正确验证，并且对于给定的密钥，它们的授权方执行密钥管理功能时也要被正确验证。
e) 执行密钥管理操作之前要优先执行源验证，保护所有密钥管理命令和相关联的数据，防止它们被伪造。
f) 所有密钥管理命令和相关数据都应被审计和保存，不允许未经授权地修改审计踪迹，即需要提供操作日志完整性保护。
g) 所有密钥和元数据都应被检测，不允许未经授权地修改，即需要提供完整性保护。
h) 在存取密钥和元数据之前执行源验证，防止密钥和元数据被伪造。
i) 提供密钥封装等秘密密钥、私钥保护机制，使它们免受非法泄露。
j) 支持数据写入、读取、修改、删除、传输等一切涉及数据加密的需求。

2.增强要求

大数据服务提供者应：

a) 提供存储用户密钥装置或密钥管理服务器操作接口，数据库密钥存储位置应是安全且有据可查的，包括提供与其数据本身具有同类型的密钥备份和恢复机制。
b) 提供数据库用户密钥和数据密钥与加密的数据库本身分离存放管理接口与管理工具。
c) 提供密钥属性配置管理，密钥属性的例子包括用户密钥类型、有效期和使用用途（数字签名、密钥加密、密钥协商、数据加密等）。
d) 提供密钥的存储及其使用接口，允许评估对象与外界连接的数据库应用程序接口与加密设备进行交互。
e) 对大数据应用和大数据平台、大数据不同安全域之间数据访问、传输等操作均要进行加密处理。
f) 制定相关策略来管理密钥存储，限制实体单独访问密钥存储，确保给定密钥的使用实体不能为存储该密钥的实体。

7.4.11 服务水平协议

1.一般要求

大数据服务提供者应：

a) 建立与大数据服务需求对应的服务水平协议，对服务水平协议涉及到的术语、指标等参数进行定义。

b) 与大数据使用者签订大数据服务水平协议，明确服务相关的技术参数和管理指标，防止因多义性或理解差异造成违约纠纷或客户损失。

c) 在服务水平协议中对数据所有权，数据交易等内容进行明确的规定。

d) 在服务水平协议对服务能力保证指标、网络接入性能等系统可伸缩性进行明确的规定。

2.增强要求

大数据服务提供者应：

a) 提供服务水平协议验证相关的证据，如基础架构、大数据平台、应用服务相关的溯源数据。

7.4.12 介质访问和使用

1.一般要求

大数据服务提供者应：

a) 建立大数据存储介质访问和使用安全策略和管理规定。

b) 从可信渠道购买或获得存储介质，并在接入系统之前进行安全扫描和检查。

c) 落实介质访问控制机制，明确介质存储数据对象，明确能够访问介质的人员或角色。

d) 对各类介质进行标记，并对介质访问和使用行为进行记录和审计。

e) 进行常规和随机检查，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。

f) 根据存储数据敏感程度，支持对存储介质中敏感数据进行加密存储。

g) 根据存储数据敏感程度，采取有效的介质净化技术和规程对介质进行净化。

2.增强要求

大数据服务提供者应：

a) 建立介质管理系统，自动管理介质资产信息和访问权限，确保各类介质的使用和传递过程得到记录。

7.5 安全审计

7.5.1 审计策略管理

1.一般要求

大数据服务提供者应：

a) 制定覆盖大数据系统行为和大数据服务数据活动的审计策略与规程，包括审计目的、审计对象、审计操作、审计方法、审计频度、相关角色和职责、管理层承诺、供应链上各参与方协调、合规性分析等内容。

b) 制定针对审计策略与规程的变更管理流程，详细记录审计策略与规程的变更起止状态、变更实施规范及变更说明等内容，定期审查和更新审计策略与规程。

c) 明确审计策略与规程中各授权用户的权限和责任，并建立审计策略与规程、审计策略实施、审计数据管理角色相关权限的授予规程。

2.增强要求

大数据服务提供者应：

a) 建立数据供应链安全审计规程与协调机制，确保审计事件的可追溯性。

b) 定期对审计策略与规程的实施情况进行检查和评价。
c) 设置独立的系统安全审计员，安全审计员应定期开展大数据服务安全审计。
d) 具备基于审计数据对审计策略与规程的合规性进行分析的技术和工具。

7.5.2 审计数据产生

1.一般要求

大数据服务提供者应：

a) 制定审计数据记录规范，明确审计数据组织结构和格式。
b) 明确与大数据系统行为相关的可审计事件，如用户登录、账号管理、客体访问、策略变更、特权功能授权、服务组件更新等。
c) 明确与大数据服务数据活动相关的可审计事件，如数据采集、数据访问、数据存储、数据传输、数据处理、数据维护和数据销毁等。
d) 确保审计数据记录内容至少包括：操作时间、操作主体、操作类型、操作对象、操作结果。
e) 具备细粒度的数据操作和系统服务行为审计能力。
f) 为审计记录维护可靠的时间标记，时间粒度应满足审计要求。
g) 具备选择和查看可审计事件的能力。
h) 定期维护审计数据记录规范、可审计事件和审计记录。

2.增强要求

大数据服务提供者应：

a) 提供允许第三方审计数据接入的系统接口。
b) 采用密码技术保证审计数据的抗抵赖性。

7.5.3 审计数据保护

1.一般要求

大数据服务提供者应：

a) 提供海量审计数据的持久化安全存储管理方法和机制。
b) 具备审计数据的访问授权能力，将审计数据访问权限授权给指定的审计管理员。
c) 采用安全技术或控制措施确保审计数据的真实性。
d) 提供审计数据归档功能，支持审计数据离线加密保存方法和机制。
e) 提供审计数据存储的时效性、数据压缩等管理策略和方法。
f) 加强审计数据访问管理，记录对审计数据的所有操作。
g) 具备对导出的审计数据进行脱敏处理的能力。
h) 在审计存储耗尽、失效、受攻击等情况下确保所保存的审计记录的有效性。

2.增强要求

大数据服务提供者应：

a) 具备审计数据异地灾备的能力。
b) 能提供证明所提供审计数据的真实性和完备性的凭据。

7.5.4 审计分析报告

1.一般要求

大数据服务提供者应：

a) 制定对审计记录进行审核、分析、报告的策略与规程。
b) 定期对审计记录进行审核和分析，并生成审计分析报告。

c） 将审计分析报告上报给机构内指定责任人，如果在审计过程中发现重大安全隐患或违规行为，应及时向机构内管理层汇报。

2.增强要求

大数据服务提供者应：

a） 对可审计事件进行实时监控分析，以支持对可疑活动的监测和响应。

b） 具备对不同来源的审计记录进行关联分析的能力。

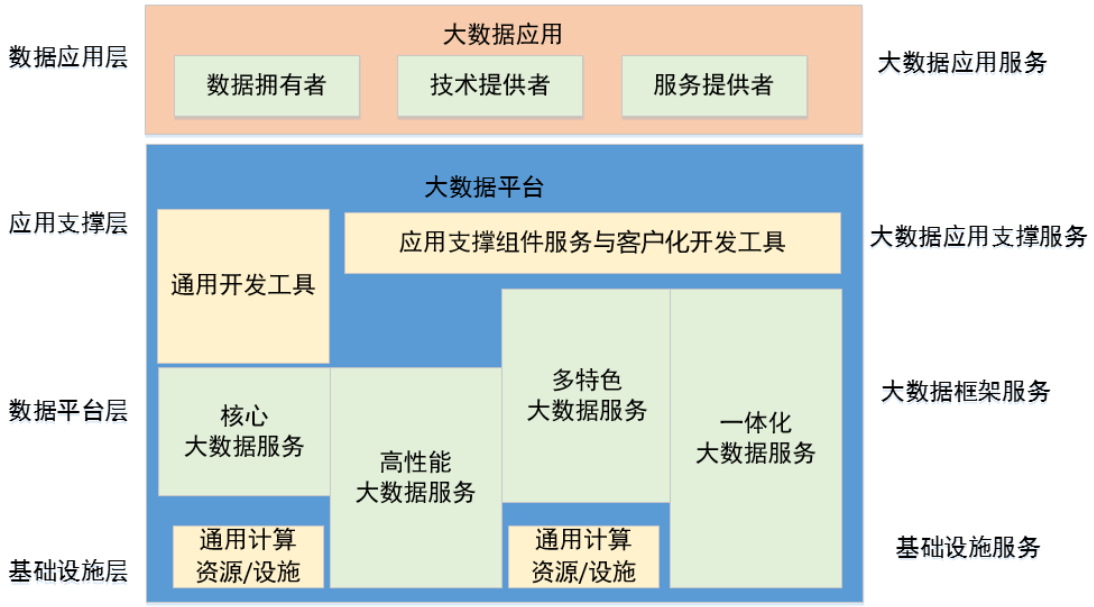
附 录 A
（资料性附录）
大数据服务模式与角色

A.1 大数据服务类型

支持大数据服务的大数据系统主要由大数据应用和大数据平台两部分组成（图4-1所示）。大数据应用为数据提供者和大数据使用者提供数据采集、数据预处理、数据整合、数据存储、数据处理、数据分析、数据可视化、数据销毁等覆盖数据生命周期的数据服务。大数据平台提供对不同来源数据聚合、不同数据类型融合、各种类型数据实体操作封装、分布式数据存储和并行处理等数据集成和分析技术，并使用多种协议简化各数据源之间的数据接口，编程接口和数据提供者接口之间的映射，以及可伸缩服务过程中异常处理，使大数据使用者透明地访问或更新大数据系统中多源数据，以通用的、可互操作的、灵活的使用模式管理这些海量、异构、快速变化的结构化、半结构化和非结构化数据资源。

A.1.1 大数据服务框架

按照基础设施、数据平台与应用支撑的层次结构，大数据平台服务细分为大数据应用支撑服务、大数据框架服务和基础设施服务。通用基础设施服务一般包括计算硬件或虚拟机计算资源、网络通信资源和数据存储资源等组成，它为大数据框架服务提供可扩展的计算、通信和存储基础设施；大数据框架服务主要为海量、复杂、异构、动态变化的大数据计算与分析提供可扩展的各种数据处理和数据存储服务；大数据应用支撑服务主要指通过集成领域业务和数据模型、数据挖掘与分析套件、大数据可视化套件、集群自动化调度、面向应用的数据生命周期管理等大数据应用领域相关的服务组件和开发接口，用以简化大数据应用开发和部署。



图A.1 大数据服务类型与服务内容

不同业务模式下对大数据服务基础设施资源选择、大数据框架计算和分析资源调度与管理、覆盖数据生命周期的数据服务组件部署等控制范围不同，从而大数据服务提供者在为大数据使用者提供大数据服务时所要求的安全能力也不同。例如在云计算支撑环境下，大数据平台的健康运行变得更为重要。基于云计算技术的大数据基础设施服务应参照GB/T 31168-2014 《信息安全技术 云计算服务安全能力要求》及其他国家、行业或机构的有关信息安全标准规范落实相关的安全责任。

大数据服务提供者应依据其大数据服务业务目标和支撑大数据服务的大数据平台应担当的角色和责任，选择合适的大数据服务类型，制定相应的安全策略和规范；挑选适合机构大数据服务安全目标的安全控制措施，识别机构大数据服务安全能力现状并分析与安全目标的差距；在此基础上不断的改进大数据安全控制措施和整改服务安全能力提升计划，可持续的保证大数据服务安全目标。

A.1.2 大数据平台服务类型

大数据平台的核心功能是提供关系、键值、文档、XML、文本、流数据等多种结构化数据和非结构化数据组织和访问服务，提供面向海量数据的分布式数据存储服务和可伸缩的数据并行处理和分析与可视化服务。大数据平台的基础设施、数据管理服务和大数据应用支撑服务存在多种业务模式和部署实施方式。依据大数据平台的数据服务模式，大数据平台提供者主要提供四种数据管理服务：

——**核心大数据服务**：大数据平台提供者一般采用虚拟化技术或云计算技术，向大数据应用提供可扩展存储结构、分布式计算、内存计算等支持海量、异构数据存储管理和数据快速交互式分析处理的通用服务能力。大数据框架服务是核心大数据服务，它应具有能与其它开放的通用基础设施/计算资源进行数据存储和计算交互的能力，并具备必要的大数据应用开发工具。大数据应用提供者可通过这些开发接口组合使用大数据框架服务和通用基础设施/计算资源，来构建他们所需的大数据应用程序。

——**高性能大数据服务**：面向批量数据分析、流式数据分析、海量数据联机事务处理等高性能、高可用、可伸缩大数据存储和计算服务需求，通过向下集成大数据框架服务所需的服务器、存储与网络设备、虚拟化软件等通用基础设施和计算资源，简化大数据服务性能开销问题，减少大数据服务基础设施部署和运维管理复杂度。具备高性能大数据服务的大数据平台提供者一般都为大数据使用者提供集成的服务器、存储设备、操作系统、虚拟化管理软件、数据管理系统以及一些为数据查询、处理、分析用途而特别预先安装相关的数据服务组件，并提供特定应用编程接口、数据访问服务等应用开发环境和系统健康监测服务解决方案，大数据应用开发者需使用这些个性化的编程接口与服务组件开发相应的大数据应用程序。

——**多特色大数据服务**：面向电子政务、电子商务、移动应用、金融业务、医疗健康、安全数据分析等不同领域大数据服务需求，通过向上集成领域相关的大数据分析与挖掘算法、业务数据模型、生命周期管理等面向应用的多种特征的数据业务服务，并提供包括软件即服务（如 Web 服务）、应用编程接口、数据存储适配器等面向应用领域增强的特色大数据服务组件/构件。提供这种特色服务的大数据平台提供者一般在大数据框架服务中集成了大数据应用相关的数据服务基础功能，即提供支持大数据应用、具备领域特征的大数据建模、管理、处理和分析服务，使大数据应用提供者可借助这些特色大数据服务组件快速构建其大数据应用，启用大数据领域相关的特色服务。

——**一体化大数据服务**：大数据平台提供者向下集成可扩展的大数据基础设施和数据服务平台，向上集成面向应用领域的大数据采集、组织、存储、分析、可视化等多特色大数据应用服务组件，一体化大数据服务将核心大数据服务拓展为性能好、宜部署、大数据平台与应用基础功能特色兼备的大数据存储和计算平台服务，为大数据使用者提供可扩展和完整的一站式大数据平台与应用支撑服务。

大数据平台服务提供者应通过系统冗余和数据备份、备用等高可用解决方案，保证大数据服务水平

协议的实现。此外，大数据服务者应该部署相关的服务安全管控组件，实时地监控大数据服务中数据主体、数据拥有者、大数据使用者及系统服务组件对大数据处理的各种属性，以保证实现数据服务过程中数据安全目标。

A.1.3 大数据应用服务类型

大数据应用服务主要提供数据业务活动相关的数据收集、传输、存储、处理（如计算、分析、可视化等）、使用、交换、共享和销毁服务。大数据应用存在数据自营模式、数据租售模式、数据平台模式、数据仓库模式、数据众包模式、数据外包模式等商业模式。从大数据应用提供者信息技术处理能力、是否拥有和控制大数据资源、提供者技术服务能力和大数据服务业务模式角度，本标准将大数据应用提供者的数据服务分为三种应用服务：

——**数据拥有者的大数据应用服务：**大数据应用提供者聚合数据提供者的数据源，拥有服务所需的数据资产，并可面向企业机构、政府部门、社会公众等大数据使用者提供数据分析服务，数据租售、数据共享或数据交易服务。

——**技术提供者的大数据应用服务：**技术提供者可提供大数据基础设施服务技术、大数据平台服务技术或者面向大数据应用数据融合与分析技术解决方案服务、基于大数据平台的单点技术服务、大数据平台出租服务或面向个人信息保护的数据脱敏、数据匿名化等隐私保护技术服务。

——**服务提供者的大数据应用服务：**服务提供者提供两种大数据应用服务，一种是大数据利用和分析服务，另一种是大数据咨询服务。大数据利用和分析服务面向企业或者政府部门，服务提供者利用他们开发的大数据应用提供数据分析结果服务；大数据咨询服务提供技术支持服务、技术（方法、商业等）咨询服务，或者为企业和政府机构提供类似数据科学家的数据增值咨询服务。

A.2 大数据服务角色

本标准参考GB/T XXX《信息技术大数据技术参考框架》中的角色定义，将大数据服务中的参与者分为数据提供者、大数据使用者、大数据平台提供者、大数据应用提供者和大数据服务协调者五种角色。本标准主要关注五种大数据服务角色的安全责任和义务。

A.2.1 数据提供者

数据提供者将机构外部公共网络数据资源、外部合作企业私有数据资源、机构内部数据资源或大数据服务提供者系统运行过程中的各种日志、事件等系统行为数据资源进行抽象和建模，按照国家和行业数据安全标准与规范对这些数据源数据进行整合后引入到大数据平台中，供大数据平台和大数据应用发现、访问、转换和分析这些数据资源。依据数据来源不同，数据提供者可进一步分为外部公共数据资源提供者、外部机构私有数据提供者、内部数据提供者、机器或系统数据提供者等数据提供角色。

A.2.2 大数据平台提供者

大数据平台提供者提供必要的网络、计算、存储等大数据服务所需的IT运行环境资源，和必要的基础设施应用程序开发接口或服务组件，以支持大数据组织、存储、分析和基础设施部署和运维管理，响应大数据应用提供者提出的大数据服务请求。大数据平台提供者应通过大数据平台提供的身份标识与鉴别、授权与访问控制、密文处理与密钥管理、安全审计与数据溯源等安全功能保护数据处理的机密性和完整性、数据处理的可信性和真实性、数据处理过程中个人隐私保护等数据安全目标。鉴于大数据复杂性、多样性、快速变化等特点，为上层大数据应用提供分布式、可扩展的数据存储管理和分布式并行计算服务是大数据平台提供者的核心目标，这需要通过对存储资源和计算资源的高效管理和有效调度来实

现。因此，大数据平台提供者可进一步分为大数据基础设施服务提供者、大数据存储管理服务提供者和大数据应用支撑服务提供者。

A.2.3 大数据应用提供者

大数据应用提供者将整合的大数据资源及其应用组件以软件服务方式部署到大数据平台上，并通过应用终端安全接入、数据分类分级、输入数据验证等安全策略配置和安全控制措施实施，给大数据使用者提供安全的数据组织、存储、分析和可视化服务。大数据应用提供者可分为数据、技术和服务三种产业链角色，其服务安全能力依赖于其商业模式所处的角色和义务，需要依据大数据生命周期各阶段中所负责的数据活动进行定义，确保满足数据安全和隐私保护需求。大数据应用提供者应采用机器学习、数据挖掘等技术帮助大数据使用者开拓诸如精准营销等各种分析与咨询服务等。

A.2.4 大数据服务协调者

大数据服务协调者规范和集成机构大数据服务所需的大数据平台和各类大数据应用数据业务活动，配置和管理大数据平台和大数据应用支撑安全功能组件，以构建一个可安全运行的大数据服务生态系统，确保大数据应用的各项数据服务能在大数据平台上安全高效地正确运行。大数据服务协调者负责为大数据服务组件分配对应的物理或虚拟节点，合理分配和调度大数据服务所需要的计算和存储资源，确保大数据服务运行效率达到所需要求，并通过资源的自动化按需分配，保证大数据服务可用性；通过不同的安全技术手段和安全措施，构筑大数据服务安全防护体系，实现覆盖硬件、软件和上层应用的安全保护；按照信息系统安全防护要求，从网络安全、主机安全、应用安全、数据安全等方面来保证大数据服务平台的安全性；通过配置合理的大数据平台和数据容灾框架，提升大数据系统服务资源灾备和恢复能力。

A.2.5 大数据使用者

大数据使用者可以是一个真实的终端用户或机构角色，也可以是一个其它应用系统，它使用大数据平台提供者或大数据应用提供者提供的数据和服务。大数据应用和大数据平台提供给大数据使用者的数据应经过数据脱敏、数据合规性控制等安全控制措施，并通过合适的授权和访问控制，以保证敏感数据机密性、数据完整性和个人信息保护。大数据使用者的数据服务安全要求一般通过与大数据服务提供者的服务契约和服务水平协议体现，大数据服务水平协议中应规范性描述大数据应用服务各方面的安全属性，包括输入/输出等数据完整性和机密性属性，服务安全约束和响应时间等服务质量约束，以及在数据业务层面的诸多服务质量属性，如涉及的业务规则、数据依赖关系、时间/人员消耗可用性等。服务水平协议中还要规范描述大数据服务参与方相关的关系，如服务间依赖关系，数据服务和数据资源约束关系，数据服务和应用组件间关系、服务消息间关系等。

参 考 文 献

[1] 中华人民共和国网络安全法，中华人民共和国全国人民代表大会常务委员会，2016年11月7日.
[2] 国务院关于大力促进信息化发展和切实保障信息安全的若干意见，国发〔2012〕23号，2012年6月28日.
[3] 国务院关于促进大数据发展行动纲要的通知，国发〔2015〕50号，2015年8月31日.
[4] 国务院关于国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见，国发〔2015〕51号，2015年07月01日.
[5] NIST Special Publication 800-1500-4,NIST Big Data Interoperability Framework: Volume 2, Taxonomies, September 2015.
[6] NIST Special Publication 800-1500-4,NIST Big Data Interoperability Framework: Volume 4, Security and Privacy, September 2015.
[7] NIST Special Publication 800-1500-4,NIST Big Data Interoperability Framework: Volume 6, Reference Architecture, September 2015.
[8] CSA Big Data Security and Privacy Handbook:: 100 Best Practices in Big Data Security and Privacy,2016,CLOUD SECURITY ALLIANCE Big Data Working Group Guidance.
[9] NIST Special Publication 800-57 Recommendation Key Management General(Revised), March, 2007.
[10] Christian Prokopp, Four Big Data as a Service Business models. http://www.semantikoz.com/blog/big-data-as-a-service-definition-classification/.