H.3.5 安全运维管理

应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。

H.4 第三级可参考安全控制措施

H.4.1 安全物理环境

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

H.4.2 安全通信网络

本方面控制措施包括：

a) 应保证大数据平台不承载高于其安全保护等级的大数据应用；
b) 应保证大数据平台的管理流量与系统业务流量分离。

H.4.3 安全计算环境

本方面控制措施包括：

a) 大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；
b) 大数据平台应能对不同客户的大数据应用实施标识和鉴别；
c) 大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力；
d) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理；
e) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；
f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
g) 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；
h) 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
i) 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；
j) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；
k) 涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
l) 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复；
m) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求；
n) 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。

H.4.4 安全建设管理

本方面控制措施包括：

a） 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；

b） 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容；

c） 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

H.4.5 安全运维管理

本方面控制措施包括：

a） 应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；

b） 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；

c） 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；

d） 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

H.5 第四级可参考安全控制措施

H.5.1 安全物理环境

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

H.5.2 安全通信网络

本方面控制措施包括：

a） 应保证大数据平台不承载高于其安全保护等级的大数据应用；

b） 应保证大数据平台的管理流量与系统业务流量分离。

H.5.3 安全计算环境

本方面控制措施包括：

a） 大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；

b） 大数据平台应能对不同客户的大数据应用实施标识和鉴别；

c） 大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力；

d） 大数据平台应对其提供的辅助工具或服务组件，实施有效管理；

e） 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；

f） 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；

g） 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；

h) 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；
i) 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求；
j) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；
k) 涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作；
l) 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复；
m) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求；
n) 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；
o) 大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。

H.5.4 安全建设管理

本方面控制措施包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容；
c) 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

H.5.5 安全运维管理

本方面控制措施包括：

a) 应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；
b) 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；
c) 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；
d) 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

参 考 文 献

[1] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型

[2] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

[3] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

[4] NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
网络安全等级保护基本要求
GB/T 22239—2019
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019 年 4 月第一版
*
书号:155066·1-62416

GB/T 22239-2019