

中国移动通信集团设计院有限公司企业技术标准

YB xxx-2024

中台能力安全测评作业指导书

版本号：V1.0.0

2024-xx-xx实施

2024-xx-xx发布

中国移动通信集团设计院有限公司发布

目 录

[前言 1](#_Toc14021)

[1. 范围 2](#_Toc24465)

[2. 规范性引用文件 2](#_Toc7944)

[3. 术语、定义和缩略语 2](#_Toc22096)

[4. 能力中台概述 3](#_Toc17250)

[5. 中台能力安全防护举措 4](#_Toc10137)

[5.1 厘清各方安全责任 4](#_Toc3098)

[5.1.1推进统一安全管理 4](#_Toc12502)

[5.1.2厘清安全责任界面 5](#_Toc31446)

[5.1.3落实能力使用职责 5](#_Toc10091)

[5.1.4加强能力使用申请管理机制 5](#_Toc10328)

[5.2 加强数据安全组织管理能力 6](#_Toc24128)

[5.2.1加强组织人员管理 6](#_Toc27758)

[5.2.2落实数据安全管理规范 6](#_Toc25696)

[5.3 巩固基础安全防护 7](#_Toc16007)

[5.3.1强化基础设施防护 7](#_Toc11723)

[5.3.2构建安全通信网络 7](#_Toc23493)

[5.3.3完善安全运维能力 7](#_Toc16308)

[5.4 保障能力安全基线水平 8](#_Toc26305)

[5.4.1严格落实安全设计： 8](#_Toc25529)

[5.4.2规范外部组件安全管理： 8](#_Toc5732)

[5.4.3确保开发供应链安全： 8](#_Toc16860)

[5.4.4定期开展升级与维护排查漏洞： 8](#_Toc29816)

[5.4.5规范日志结构，维护日志记录，增强入侵防范能力： 9](#_Toc32583)

[5.4.6完善接口访问控制与授权管理： 9](#_Toc29158)

[5.4.7强化算法备案： 9](#_Toc12314)

[5.5 落实上台安全评估 9](#_Toc1464)

[5.5.1落实系统安全评估 9](#_Toc7390)

[5.5.2落实能力安全评估 9](#_Toc30042)

[5.5.3落实数据安全评估 9](#_Toc8270)

[5.5.4落实算法安全评估 10](#_Toc6060)

[5.6 做好能力安全管控 10](#_Toc18573)

[5.6.1严格身份管理和内容审核 10](#_Toc12776)

[5.6.2加强注册上台能力授权管控 10](#_Toc32527)

[5.6.3强化用户认证机制 10](#_Toc17508)

[5.7 优化统一安全监测 11](#_Toc21687)

[5.7.1构建安全监测体系 11](#_Toc3768)

[5.7.2证日志安全完整 11](#_Toc15354)

[5.7.3统一安全管控与指挥调度 11](#_Toc3541)

[5.8 完善新技术安全防控 11](#_Toc2313)

[5.8.1区块链安全 11](#_Toc3087)

[5.7.2人工智能安全 12](#_Toc4170)

[5.7.3 隐私计算安全 12](#_Toc23074)

[5.9 加强能力输出接口防护 13](#_Toc15791)

[5.9.1构建业务流程管理机制 13](#_Toc16827)

[5.9.2落实接口防护机制 13](#_Toc5034)

[5.9.3强化传输安全保障措施 13](#_Toc1306)

[5.9.4加强信息服务管控 13](#_Toc14024)

[5.10 开展不良信息治理 14](#_Toc7346)

[5.10.1做好能力源头管控 14](#_Toc4935)

[5.10.2强化不良信息监测 14](#_Toc11009)

[5.10.3加强应急处置机制 14](#_Toc21527)

[5.11 开展算法安全防控 14](#_Toc8182)

[5.11.1加强算法使用行为监测 14](#_Toc24360)

[5.11.2落实算法生成内容监测 14](#_Toc4243)

[5.12 健全数据生命周期安全能力 15](#_Toc26875)

[5.12.1数据收集阶段 15](#_Toc11451)

[5.12.2数据存储阶段 15](#_Toc450)

[5.12.3数据使用阶段 15](#_Toc19526)

[5.12.4数据传输阶段 16](#_Toc20641)

[5.12.5数据共享阶段 16](#_Toc5580)

[5.12.6数据销毁阶段 16](#_Toc5575)

[5.13 提升数据安全风险管理能力 17](#_Toc5328)

[5.13.1风险识别 17](#_Toc4728)

[5.13.2安全防护 17](#_Toc555)

[5.13.3安全监测 17](#_Toc11840)

[5.13.4安全响应 18](#_Toc22761)

[5.13.5安全恢复 18](#_Toc10981)

[6. 编制历史 18](#_Toc25335)

# 前 言

本标准编制的目的在于规范中国移动能力中台上台能力安全测评的技术要求和标准，为能力中台安全评估的规划和具体实施提供参考。

本标准的主要内容包括中国移动能力中台整体架构和能力中台安全防护举措。

本标准的结构、名称或预计的名称如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 标准编号 | 标准名称 |
| [1] | YB xxx-2024 | 中台能力安全测评作业指导书 |

XX号印发。

本标准由移设院行〔2024〕xxx号印发。

本标准由中国移动设计院网络规划与设计优化研发中心提出，技术部归口管理。

本标准起草单位：网络规划与设计优化研发中心

本标准主要起草人：杜雪涛、张晨、周顶、赵蓓、常玲、黄凯、谷天航、薛姗、常潇、于少中、于雷、杜刚、王奕夫、谢仪頔、王红雨、刘胜兰、闫鑫、白岩、任珍。

# 范围

本标准在中国移动多项相关网络安全标准的指导下，制定当前中国移动能力中台架构下，能力中台上台能力日常运营过程中的安全防护举措，目的是提高能力中台上台能力安全运营工作质量，为能力中台降本增效提供安全稳定的运营环境。

# 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款，其最新版本适用于本标准。如果本标准中条款与下列文件或其修订版本不一致的，以下列文件或其修订版本的规定为准。

表1 引用的规范性文件

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 标准编号 | 标准名称 | 发布单位 |
| [1] | QB-Y-107-202301 | 中台能力标准化技术规范 | 中国移动通信集团有限公司 |
|  |  |  |  |
|  |  |  |  |

# 术语、定义和缩略语

下列术语、定义和缩略语适用于本标准：

表2 术语、定义和缩略语说明

|  |  |  |
| --- | --- | --- |
| 术语 | 英文全称 | 解释 |
| 能力中台 | Integration Platform | 中国移动能力中台是一套能力服务体系，是应用软件、硬件设备、规范标准、组织、文化、流程等一系列元素有机结合并形成运行机制。能力中台以积淀能力、支撑发展、注智赋能为总体目标，以业务中台、技术中台.数据中台三台能力为核心基础，对内助力提升资源配置和生产经营水平加快公司数智化转型，打造慧企业，对外推动产业数字化、数字化产业促进经济社会数智化转型。 |
| 中台能力 | Integration Platform Ability | 中台能力是一个或一组服务的集合，通过服务编排组合而成，向应用提供某特定领域的一套功能。中台中台能力应具备可共享、可复用的特点。 |
| API | Application Programming Interface | 应用程序编程接口 |
| SDK | Software Development Kit | 软件开发工具包 |
| DaaS | Data-as-a-Service | 数据即服务 |
| PaaS | Platform-as-a-Service | 平台即服务 |
| AaaS | Ability-as-a-Service | 能力即服务 |
| SaaS | Software-as-a-Service | 软件即服务 |

# 能力中台概述

能力中台是实现世界一流信息服务科技创新公司“新定位”的核心着力点，是创世界一流“力量大厦”新的战略基石。能力中台以积淀能力、支撑发展、注智赋能为目标，对内实现能力沉淀复用、推进自主可控，实现降本、增效、提质；对外输出优质能力、助力千行百业，实现合作、共赢、赋智。

能力中台与5G、算力网络共同构成中国移动新型信息基础设施，是“连接+算力+能力”新型信息服务体系、“BASIC6”科创计划的重要组成部分。能力中台不仅仅是具体的平台和系统，而是一项软硬结合的系统工程，是将应用软件、硬件设备、规范标准、组织、文化、流程等元素有机结合的一套AaaS能力服务体系，通过中台服务体系的流畅运转，让各单位（部门）在中台建设运营过程中有贡献、有获益，充分发挥全集团积极性。

能力中台是公司贯彻落实中央推动治理体系和治理能力现代化决策部署的重要抓手，是充分发挥数据、技术要素作用的有效手段，是公司数智化转型升级、实现价值经营的关键基础设施。能力中台对内可实现降本、增效、提质，形成内部资源、产品服务、用户需求的正向循环，为生产经营、管理、服务等各环节注智赋能；对外可实现合作、共赢、赋智，支撑社会信息的多维采集、海量分析、实时处理，助力提升生产生活、社会治理数智化水平。

能力中台以多元化的能力，面相不同角色、不同特点的用户开放适配各类解决方案，支撑业务应用快速搭建、能力复用、敏捷迭代。主要通过3种方式提供服务：

**1.能力、数据模式：**主要面向具备的自主开发能力开发团队提供提供API、Daas、SDK调用。提供封装编排后的API或SDK，由使用者自行调用后完成开发；或者依据数据调用安全审计流程，提供DaaS数据调用服务。

**2.入驻开发模式：**主要面向具备一定的前台开发能力，对开发环境、资源有需求的开发团队提供PaaS平台和配套组件。在提供能力、数据等基础上，提供应用开发平台、大数据平台、AI机器学习及推理平台等；或者提供平台运行资源、访问环境、接口；或者配套提供环境内调用的标准化组件、镜像、代码等。

**3.应用提供模式：**主要面向直接使用软件应用服务时长的市场运营人员提供类似SaaS的能力组合。通过对中台能力封装，向使用者提供模板化运营配置；或者自助式实现需求的使用环境、运营界面、应用平台，如IOP、轻量化营销工具等。

# 中台能力安全防护举措

中台能力安全工作的目标是实现能力中台安全保障要求，即管理运营责权明晰、上台能力风险可控、能力使用安全合规、数据价值有效提升。

在实际安全工作中，在传统应用系统安全的基础上，按照“谁主管，谁负责；谁运营，谁负责；谁使用，谁负责；谁接入，谁负责；谁开发，谁负责”的原则，构建责任共担的安全保障体系，以实现能力中台平台安全工作目标。

根据中台能力面临的各种安全风险，针对性的制定了十三条防护举措，如图1所示，供能力中台安全测评过程中进行参考。

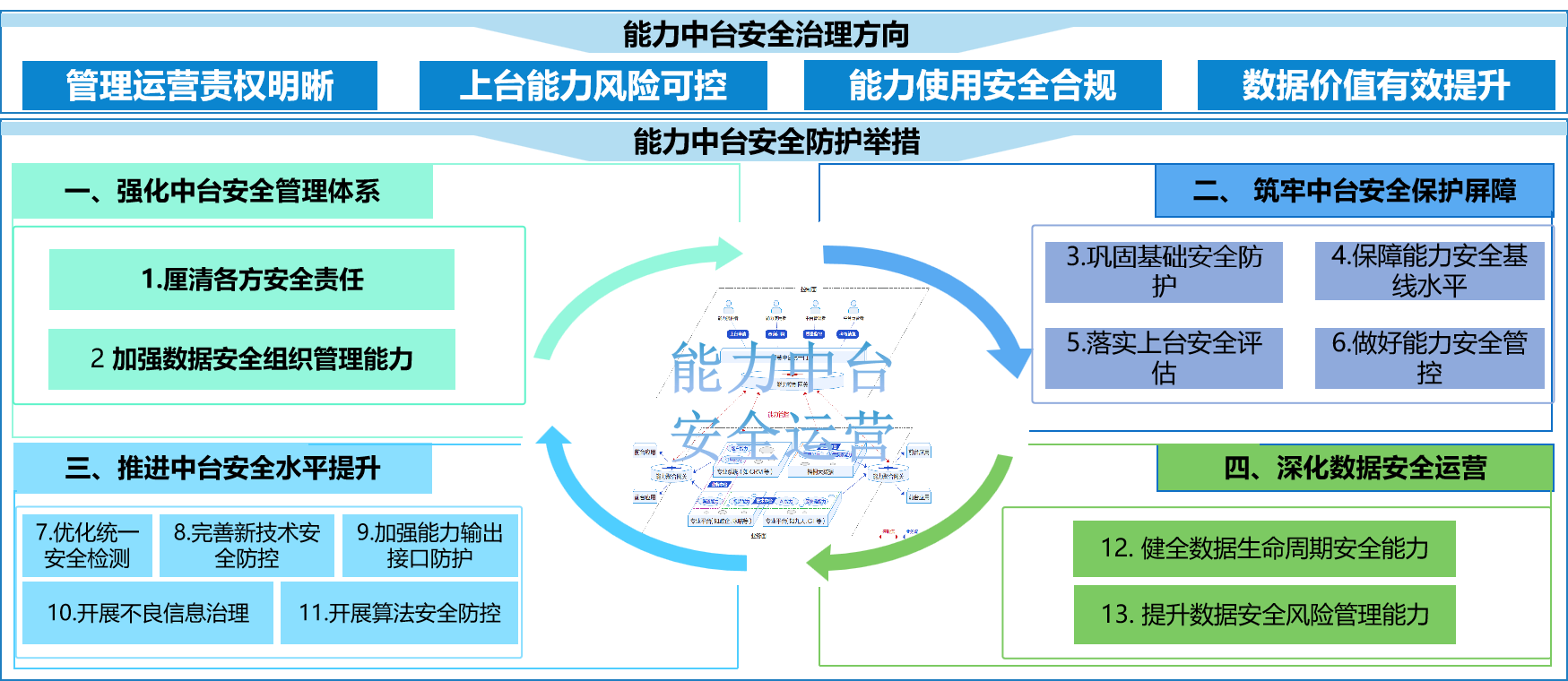


图1 能力中台安全防护举措概览图

## 厘清各方安全责任

### 5.1.1推进统一安全管理

推进统一安全管理，需要从以下三个方面进行：

1. **制定安全工作指引：**制定统一的能力中台安全工作指引，防范中台、能力建设运营过程的安全风险。
2. **健全闭环管理机制：**落实”三同步“、新技术新业务安全评估要求，建立覆盖能力全生命周期的安全管理机制；做好关键节点安全管控，建立能力上台管理和评测制度。
3. **建立应急响应机制：**制定能力紧急下线等突发事件的应急处置措施，定期进行应急事件演练。

### 5.1.2厘清安全责任界面

厘清安全责任界面，需要从以下两个方面进行：

1. **制定安全责任矩阵：**梳理中台管理者、中台运营者、能力提供者以及能力使用者的安全责任，制定安全责任矩阵，明确各相关方安全责任。
2. **明确安全责任划分：**明确能力提供者，内外部使用者的安全责任划分，增加安全责任条款。

### 5.1.3落实能力使用职责

落实能力使用职责，需要从以下三个方面进行：

1. **落实责任机制：**落实“谁使用，谁负责；谁接入，谁负责”，建立安全可控、可溯源的能力使用体系。
2. **建立责任管理体系：**建立能力使用者责任管理体系，加强对外部能力使用者的信息登记管理。
3. **制定问责机制：**做好能力使用安全监测，建立能力违规使用问责机制。

### 5.1.4加强能力使用申请管理机制

加强能力使用申请管理机制，需要统一管理能力使用者信息，即明确能力调用的具体业务场景、明确能力调用最终面向的用户、能力调用涉及的相关数据是否为敏感信息、是否需要进行脱敏处理、能力调用有效期等内容，防止客户信息泄露等数据滥用风险。

## 加强数据安全组织管理能力

### 5.2.1加强组织人员管理

加强组织人员管理，需要从以下四个方面进行：

1. **明确参与方责任：**厘清能力提供方、能力使用方、能力运营方、中台运营方责任与义务，切实履行数据安全保护义务，落实数据安全责任。
2. **加强人员管理：**明确接触个人信息、重要数据等数据的人员管理规范，落实第三方人员管理制度。
3. **加强角色管理：**人员、岗位的角色清单管理和授权机制，对人员角色分配和角色授权定期审核，及时更新用户角色及角色授权信息。
4. **推进人员教育培训：**组织开展相关人员的数据安全教育培训，包括法律、法规、政策、标准、技术、技能、安全意识等内容的培训，并依据培训反馈效果定期对教育培训计划进行审核和更新。

### 5.2.2落实数据安全管理规范

落实数据安全管理规范，需要从以下五个方面进行：

1. **落实分类分级管理制度：**梳理中台收集、处理、存储的数据清单，参照数据分类分级要求，实施相应保护措施。
2. **加强权限管理：**落实系统账号权限分配、开通、使用、销毁等安全保障原则和审批流程要求，明确各账号分配、开通、使用、变更、注销规则。账号权限分配遵循“权限明确、职责分离、知其所需、最小特权”的原则。
3. **严格合作管理：**通过梳理合作清单、业务清单，签订数据安全协议、核查数据安全保护措施、明确数据使用范围，监督接口关闭、数据销毁等措施加强对合作前、合作中、合作后的监督管理。
4. **加强日志管理：**对数据收集、使用、共享、销毁等环节的操作日志进行留存，日志记录信息应包括主要信息并确保日志记录完整、准确。
5. **落实安全审计：**开展数据安全审计，记录并形成数据安全审计报告。

## 巩固基础安全防护

### 5.3.1强化基础设施防护

强化基础设施防护，需要从以下八个方面进行：

1. **物理设备安全：**对服务器、交换机等设备本地访问接口增设访问控制机制，利用用户名和口令进行身份认证。
2. **账号及口令安全：**支持安全配置设账号和口令，包括设置口令复杂度、密码有效期、登录失败重试次数；设备安装后，及时更改设备中供应商的默认账号和口令。
3. **授权管理：**能力中台系统应支持基于角色的权限管理。
4. **日志管理：**应支持记录对设备配置日志功能，并且与日志服务器对接，实现日志的集中安全存储。
5. **证书安全：**应保障证书及私钥的安全存储、避免非授权访问。
6. **系统安全：**对物理服务器、虚拟机的操作系统、中间件和数据库进行安全加固，采用安全的协议进行通信。
7. **虚拟机安全：**vCPU，虚拟内存，I/O进行安全隔离；虚拟机之间相互访问需进行认证，授权和日志审计。
8. **容器安全：**采用最小授权原则对容器运行的资源和权限进行限制；针对容器进行网络隔离；容器运行安全检测和防护。

### 5.3.2构建安全通信网络

构建安全通信网络，需要从以下三个方面进行：

1. **划分安全域：**根据承载业务和数据重要敏感程度，对平台实施分区分域管理。
2. **安全隔离：**管理、业务、存储三平面物理隔离，支持微隔离实现端口级别的安全隔离，防止横向攻击。
3. **访问控制：**制定不同区域间访问控制策略，部署边界防护措施。

### 5.3.3完善安全运维能力

完善安全运维能力，需要从以下四个方面进行：

1. **资产管理：**支持多角度、多维度准确识别中台平台所有资产。
2. **容灾备份：**对重要系统和数据库进行容灾备份。
3. **安全基线合规及漏洞补丁管理：**定期针对中台平台操作系统、数据库和中间件等安全配置、变更操作进行核查；引入漏洞知识库，对漏洞发现、分析、整改、符合等全生命周期进行管理；管理漏洞补丁，验证与业务无冲突后才能入网。
4. **安全管理平台：**由安全管理平台对安全设备和安全策略进行统一管理和编排，对安全日志、安全事件等进行分析并给出安全策略。

## 保障能力安全基线水平

### 5.4.1严格落实安全设计：

在能力设计过程中需要严格遵守基本安全原则，如尽可能减少攻击面，权限最小化，预处理各种异常，业务隔离，简化系统，使用白名单等。尽可能避免安全缺陷。

### 5.4.2规范外部组件安全管理：

明确安全评估责任，使用开源组件前先对其许可证及协议进行合规检查。对其可传染性，兼容性，安全性进行审计。

### 5.4.3确保开发供应链安全：

制定供应商选择、评定和日常管理的程序。建立供应链各环节核心要素（技术知识产权、开发工具等）的追溯体系。以确保关键部件和核心要素满足安全要求。

### 5.4.4定期开展升级与维护排查漏洞：

在开发过程中定期对软硬件版本进行确认，检测其运行状态，排除潜在漏洞，处理检测出的漏洞。定期升级保证程序功能正常运转。

### 5.4.5规范日志结构，维护日志记录，增强入侵防范能力：

建立结构化日志，规范其格式和功能。定期维护并检测自身运行状态和重要操作记录，检测到恶意程序入侵时能自动发出安全警告或阻断访问。

### 5.4.6完善接口访问控制与授权管理：

完善接口访问控制，对数据包进行有效分析筛查。确保程序能正确验证身份并分配权限，完善资源访问规则，实现管理用户的权限分离。

### 5.4.7强化算法备案：

算法备案内容包括算法流程、算法数据、算法模型、干预策略、结果标识等必要内容，提升算法透明度，确保算法安全问题随时可回溯、可管控。

## 落实上台安全评估

### 5.5.1落实系统安全评估

梳理上台能力涉及的各种资产，如主机、中间件、端口等，形成资产清单。采用可靠的技术隔离手段明确划分网络内部安全域。

### 5.5.2落实能力安全评估

严格落实安全三同步要求。对上台能力中所使用的外部组件进行安全评估，形成软件物料清单统一进行管理，确保不存在侵权行为。采取措施进行有效的接口管控。规范化安全防护设施，具有WAF、IDS、DDOS、APT等设备。

### 5.5.3落实数据安全评估

梳理能力中涉及的各类数据，形成清晰完整的数据资产清单。在数据收集阶段，确保用户数据采集经过用户同意知晓。在数据存储阶段，对涉敏信息进行去标识化、模糊化处理。在数据使用阶段，确保数据使用行为具有明确授权，敏感信息已纳入金库管控。在数据传输阶段，对传输信道实施加密措施。在数据共享阶段，构建数据防泄漏装置。整体上具备数据备份、归档与恢复措施。

### 5.5.4落实算法安全评估

对备案范围内的算法进行规范备案，确保备案流程完整合规。设立算法安全评估监测机制，组织开展算法安全评估与监测。设立算法安全应急处理机制，能够响应紧急情况下的算法安全需求。对算法生成内容中的虚假、敏感和不良内容进行有效识别和防控。

## 做好能力安全管控

### 5.6.1严格身份管理和内容审核

严格身份管理和内容审核，需要从以下四个方面进行：

1. 落实账号管控措施：定期对账号进行检查与管理，对长期非活跃账号进行清除，防止能力滥用和冒用。
2. 强化用户操作限制：对账号登录、注册、找密操作进行次数及频率上的限制，减少恶意登录，预防能力被攻击者恶意利用。
3. 加强访问流量控制：针对外挂高频访问，采取限流和熔断措施，通过流量控制策略和API管理来实现限制能力滥用风险。
4. 制定内容审计机制：应配套健全开放接口安全审计、第三方权限管理的机制规范确保不被外部威胁入侵导致违法有害信息注入和传播。

### 5.6.2加强注册上台能力授权管控

对于注册上台业务能力，要进行严格授权管理，保证非授权用户无法访问需要授权应用及业务。确保授权用户无法访问所授权限外应用及业务，防止由于中台的横向扩展导致能力违规调用。

### 5.6.3强化用户认证机制

强化用户认证机制，需要从以下两个方面进行：

1. **完善标识验证功能：**在交互过程中，需要加强用户账号和标识（cookie等）验证功能，防止用户身份被篡改和伪造，从而避免用户身份冒用。
2. **关键业务二次认证：** 关键业务受理，需要向用户进行二次认证校验，防止用户身份被冒用造成不知情订购。

## 优化统一安全监测

### 5.7.1构建安全监测体系

构建安全监测体系，需要从以下两个方面进行：

1. **通信、数据隔离：**能力中台自身的数据隔离（如敏感数据的收集使用等全生命周期的管理）、通信隔离（如管理面与业务面的分离）。
2. **集中日志审计：**能力中台应对独立上台的能力调用进行日志记录，并能同步记录注册上台的能力调用日志，对能力调用日志进行安全审计。

### 5.7.2证日志安全完整

证日志安全完整，需要从以下两个方面进行：

1. **制定日志完整推送流程：**从能力调用网关以及能力所在系统多位置多维度收集安全日志，统一推送至能力中台进行日志审计。
2. **完善日志保护机制：**利用日志防篡改技术进行完整性保护，确保日志准确有效；监控日志缺失情况，如有缺失及时产生告警信息。

5.7.3统一安全管控与指挥调度

统一安全管控与指挥调度，需要从以下两个方面进行：

1. **统一安全管控：**对于所有上台能力，能力中台应能够对其运行的容器、主机进行相同粒度的监控。对独立上台的能力需纳入PaaS防病毒机制等统一管控要求注册部署。对注册上台的能力需要求能力提供方单独在其所运行的容器及主机上运行基线、合规、终端管控工具、定期提供渗透测试报告。
2. **统一指挥调度：**安全事件统一指挥、安全专家统一调度、安全风险统一处置。

## 完善新技术安全防控

### 5.8.1区块链安全

加强区块链安全防护，需要从以下四个方面进行：

1. **执行安全责任划分，加强业务流程管控：**针对业务特点，制定数据生命周期全流程的管理机制。增强区块链业务全生命周期业务流程的管控，对交易过程中的数据进行必要的保护。
2. **使用有安全证明的共识机制和开发框架：**区块链平台提供的相关智能合约开发框架应具备开发安全规范，智能合约运行环境（虚拟机/容器等）做好资源隔离和指令限制，防范漏洞。
3. **规范智能合约开发执行代码审计与测评：**向用户提供智能合约安全开发规范，在智能合约代码上链前，进行合约代码安全审计和评测。
4. **增强链上数据与线下资产的关联：**引入数据感知和数据采集技术，加强物联网技术与区块链技术的协同和信息采集能力，增强链上数据的源头可信度。

### 5.7.2人工智能安全

加强人工智能安全防护，需要从以下三个方面进行：

1. **在应用框架及算法前对其进行风险评估：**排查产品应用的深度学习框架及算法中的安全漏洞。检测其是否容易遭受拒绝服务攻击，任意代码执行攻击，对抗样本攻击等。
2. **规范模型训练数据集：**对数据集采取标准化处理，实现技术标准化，包括统一的格式与储存方式。一方面可提高数据集的质量水平，另一方面降低了数据被毒化的可能。
3. **构建风险防御策略：**现阶段某些深度学习模型依然缺乏可解释性，因此需要严格控制模型输出结果取向，预防不良结果给业务带来的安全隐患。

### 5.7.3 隐私计算安全

加强隐私计算安全防护，需要从以下四个方面进行：

1. **从技术层面满足数据最小化、完整性和机密性原则要求：**数据最小化要求即对个人数据的处理数量以满足业务需要的最小数量为限。完整机密性要求即避免数据被非法处理、篡改、毁损或者不当泄露。
2. **隐私计算应用过程中需重视数据安全风险：**尽管无需参与者直接共享原始数据，但模型仍然可能泄露数据的相关信息。企业需要从模型隐私、输入隐私、训练数据隐私、输出隐私四方面保障数据的安全。
3. **采用隐私计算需明确用户授权同意机制：**个人信息的匿名化标准尚存争议，因此做好告知同意的授权管理，对企业数据合规具有重要意义。
4. **明确隐私计算参与各方权利义务的边界：**现阶段，参与各方宜通过协议方式，事先约定彼此的数据安全权力和义务边界，明确责任。

## 加强能力输出接口防护

### 5.9.1构建业务流程管理机制

构建业务流程管理机制，需要从以下两个方面进行：

1. **加强业务流程管理：**加强对业务流程的管理，严格限定业务调用的前提条件，避免业务调用乱序问题，确保能力不会由于关联关系被违规调用。
2. **强化服务器后端验证：**在能力交互确认阶段，需要进行对操作行为和数据在后台服务端进行验证，经确认方可执行，若无法确认可拒绝交互流程。

### 5.9.2落实接口防护机制

落实接口防护机制，需要强化接口细粒度管控，防止业务关联调用。即根据接口业务属性不同，划分为公共型接口、私有型接口，再根据粒度粗细、业务需求、服务数量、权限划分，采用不同的身份认证和授权技术。

### 5.9.3强化传输安全保障措施

强化传输安全保障措施，需要采用可靠的传输协议，防止敏感信息泄露。即 应对数据传输过程实施数据完整性校验措施，采用安全可靠的传输协议；防止关联调用产生的信息泄露。

### 5.9.4加强信息服务管控

加强信息服务管控，需要从以下两个方面进行：

1. **完善信息服务授权机制，确保用户授权执行：**明确授权规则，需获得最终客户明确授权后，方可执行调用能力操作，防止定位，信用等客户信息泄露。
2. **引入4A等技术措施，防止后台非授权能力使用：**定期对4A的后台日志和能力自身日志进行对比审计验证能力调用操作是否一致，以检测是否存在后台非授权能力使用。

## 开展不良信息治理

### 5.10.1做好能力源头管控

做好能力源头管控个，需要在能力上台阶段、调用阶段，加强能力源头评估，明确能力用途和调用范围，不得用于传播垃圾短彩信、色情低俗信息、骚扰诈骗电话等违法国家法律法规的不良信息。

### 5.10.2强化不良信息监测

强化不良信息监测，需要在在能力调用过程中，加强短彩信、电话、图片、音频、视频等所含不良信息的日常监测，严防传播不良信息的行为。严防利用电信资源、号码传送、信息传播等业务的不良信息违法活动。

### 5.10.3加强应急处置机制

加强应急处置机制，需要对于上级单位、集团公司通报的不良信息，要立即处置，阻断不良信息的传播；对于自行监测发现的不良信息，要立即清除，防止扩散。

## 开展算法安全防控

### 5.11.1加强算法使用行为监测

加强算法使用行为监测，需要在能力使用过程中，加强对算法运行情况的监测，发现并记录内存溢出、死循环、数值溢出、网络异常等算法异常，及时告警。严防因为算法使用而造成大数据杀熟、致瘾性推荐、恶意搜集信息等危害用户的情况。

### 5.11.2落实算法生成内容监测

落实算法生成内容监测，需要规范内容生成式能力生成内容的使用，对于使用能力生成内容的场景，进行用户告知和提醒，防止用户使用能力生成内容从事违法违规活动。

## 健全数据生命周期安全能力

### 5.12.1数据收集阶段

在数据收集阶段，需要从以下三个方面进行：

1. **合法正当采集数据**：严格落实数据的获取源及其数据格式、获取目的和用途、范围、期限和频次，规范数据获取渠道、获取流程和获取方式的要求。
2. **告知同意**：采集用户信息前征取用户同意，并将采集数据用途明确告知用户。
3. **加强数据清单管理**：利用数据识别和数据清洗技术，并根据数据分类分级对数据进行标记。

### 5.12.2数据存储阶段

在数据存储阶段，需要从以下三个方面进行：

1. **完善存储保护手段：**对重要数据实施差异化脱敏存储、加密存储等措施，涉及个人敏感信息考虑去标识化、模糊化等存储技术手段。
2. **加强存储介质管理：**严格落实对物理介质（磁阵、硬盘等）的维护、更换、升级、转移和报废等操作要求。
3. **落实数据备份管理：**根据数据级别实施不同的数据备份策略，并根据数据恢复方案进行数据恢复性验证。

### 5.12.3数据使用阶段

在数据使用阶段，需要从以下三个方面进行：

1. **加强账号管理：**账号角色权限最小化，并及时清除无用、默认账号等；对高权限账号进行操作审计。
2. **加强脱敏场景管理：**利用动态脱敏、静态脱敏和隐私保护等技术严格按照数据脱敏规则对涉敏场景进行数据脱敏。
3. **再次征求同意：**严格控制数据使用与数据收集时告知用户目的一致，数据用于其他目的时要再次征得用户同意。

### 5.12.4数据传输阶段

在数据传输阶段，需要从以下三个方面进行：

1. **完善传输策略：**根据安全域内、安全域间不同的数据传输场景制定不同的数据传输策略。
2. **强化传输通道安全：**安全通道、可信通道、数据加密等，保证数据在大数据系统中传输数据的保密性和完整性；利用冗余链路、断点续传、超时重新连接等技术保障数据传输的可靠性。
3. **提升身份鉴别能力：**严格按照数据安全传输密钥管理和接口规范，构建对数据传输两端主体身份进行标识和鉴别的能力。

### 5.12.5数据共享阶段

在数据共享阶段，需要从以下两个方面进行：

1. **落实开放共享规范：**严格落实数据开放共享过程中的数据保护制度和安全措施，加强数据共享前评估、共享中监测、共享后数据安全删除的全流程管理，落实双方数据保护责任与义务。
2. **完善数据共享技术措施：**通过数据加密、安全通道、内容加密、数字水印、数字签名、文件打开次数限制、文件修改权限限制、文件打开终端限制等技术防止共享数据泄漏。

### 5.12.6数据销毁阶段

在数据销毁阶段，需要从以下两个方面进行：

1. **落实数据删除规范：**在业务需求或用户提出要求销毁删除数据时，严格按照数据删除规范的处理策略和操作规程，对数据、包括数据处理过程中备份数据、衍生数据及操作日志数据等进行删除销毁。
2. **完善数据销毁技术措施：**根据删除策略对数据进行物理删除（硬删除）和逻辑删除，同时对数据销毁删除效果进行验证，确保相关数据不可访问或不可识别。

## 提升数据安全风险管理能力

### 5.13.1风险识别

进行数据安全风险识别，需要从以下两个方面进行：

1. **构建数据资产的识别能力：**及时对数据处理活动相关的数据源信息、数据资产等进行识别，形成数据资产目录，并及时更新。
2. **安全风险评估：**对数据资产及其数据处理活动进行威胁及脆弱性识别，形成数据安全风险分析报告。定期进行数据处理活动安全管控措施的隐患排查和治理，提升对数据安全风险应对措施的识别能力。

### 5.13.2安全防护

进行数据安全防护，需要从以下三个方面进行：

1. **加强区域边界防护：**对跨区域边界的数据处理活动防护措施进行检查，确保在不同区域间的数据安全策略实施效果保持一致，并实施严格的逻辑访问控制措施。
2. **加强数据操作防护：**严格落实数据操作执行规范，建立数据高风险操作清单并加强其管控措施。
3. **重要数据防护：**利用数据脱敏、个人信息去标识化等能力，避免通过数据抓取、数据分析等造成重要数据、敏感个人信息和泄漏。

### 5.13.3安全监测

进行数据安全监测，需要从以下两个方面进行：

1. **构建数据处理活动监测能力：**对数据处理活动及其服务接口的访问进行自动化监控，并根据监测规则和安全基线，对数据处理活动异常行为进行告警。
2. **加强对重要数据监测：**采取技术措施加强对重要数据和敏感个人信息流转监测，对异常、高风险、跨区域边界的交换、共享等数据提供行为进行实时监控，发现异常能提供阻断和预警措施。

### 5.13.4安全响应

进行数据安全响应，需要从以下两个方面进行：

1. **完善应急预案：**制定数据安全事件应急预案，明确数据泄露、被篡改、被损毁、违规使用等场景的应急处置流程，并在定期演练中不断完善。
2. **增强数据溯源能力：**利用数字水印、数据标记、可信存证或血缘分析等技术加强数据处理过程的可追溯性。

### 5.13.5安全恢复

进行数据安全恢复，需要完善数据备份计划，即制定数据备份、归档与恢复的计划，配置必要的备份、归档与恢复工具，并定期组织演练。

# **编制历史**

表3 编制历史

|  |  |  |
| --- | --- | --- |
| 版本号 | 更新时间 | 主要内容或重大修改 |
| V1.0.0 | 2024-10-08 | 完成该规范的初版 |