附件

互联网数据中心客户数据安全保护实施指引

一、互联网数据中心业务基本情况及数据安全风险挑战

（一）互联网数据中心基本情况及分类

互联网数据中心业务（以下简称IDC业务，见《电信业务分类目录》）主要包括传统数据中心业务和互联网资源协作业务。结合业务产品功能，细分为三类业务场景：**一是**服务器托管业务场景，指IDC业务经营者为客户提供机房、机柜、设备租赁，以及设备维护等服务的业务模式。**二是**数据存储业务场景，指IDC业务经营者为客户提供数据存储服务，以及相关数据上传、下载、访问等服务的业务模式。**三是**数据计算业务场景，指IDC业务经营者为客户提供数据清洗、集成、分析、加工、展示、模型训练以及算力调度等服务的业务模式。

（二）IDC业务面临的客户数据安全风险挑战

1. 通用安全风险。一方面，IDC业务经营者、客户甚至第三方供应商等可能接触、处理客户数据的各方主体未明确划分数据安全责任边界，导致各方数据安全保护权责不清、责任义务落实不到位。另一方面，IDC业务经营者针对客户数据安全管理制度机制不健全、安全防护措施配备不完善，增加客户数据被窃取、泄露等的安全风险。

2.典型业务场景安全风险。一是服务器托管类业务场景

下，IDC业务经营者主要负责保障机房基础设施安全，可能存在的客户数据安全风险情形主要包括：自然环境灾害（地震、洪水）、物理设施故障（如断电、温湿度失调等）等引发服务器等设备宕机、损毁和失窃等，导致客户数据破坏和丢失。网络设备、服务器等由业务经营者提供的，需要防范因设备安全管理不健全，存在设备漏洞、后门等导致设备被攻击入侵，进而引发客户数据被窃取或破坏等风险。**二是**数据存储和计算类业务场景下，IDC业务经营者主要通过提供安全可靠的计算、存储平台，可能存在的客户数据安全风险情形主要包括：在数据存储、传输，以及算力调度、人工智能训练等环节，因数据安全保障措施配备不足，风险监测、资源监控和负载均衡等相关管理和技术手段不完善等，导致数据被窃取、泄露、丢失等风险。

二、提升客户数据安全保障能力

（三）通用保障能力

1. 客户数据处理要求。IDC业务经营者按照《数据安全法》《网络安全法》《网络数据安全管理条例》《工业和信息化领域数据安全管理办法（试行）》等法律法规和政策要求，履行客户数据安全保护责任，未经客户授权，不得以任何形式收集、存储、使用、加工、传输、提供、公开、销毁客户数据。其他法律法规另有规定的除外。

2. 明确责任界面。在与客户签署的合同协议中，参照有关行业标准，根据业务模式和服务内容，明确双方数据安全保护责任义务。涉及通过采购第三方服务商设备、服务等，

处理客户数据的，需明确各方数据安全保护责任义务。

3. 管理制度建设。建立客户数据安全管理制度，明确工作职责分工、配套机制、管理与技术保障措施等内容。

4. 机构与人员设置。明确数据安全负责人和管理部门，结合业务模式，设立数据安全管理岗位并明确岗位职责，配备相应人员，统筹负责客户数据处理活动安全管理。

5. 客户管理。建立客户管理机制，加强对党政机关等重点客户的数据安全风险提示，依据客户类别和数据保护需求，提供差异化安全防护能力，并配合采取相应保护措施，提升IDC承载信息系统和数据的安全保护能力。

6. 数据分类分级保护。在提供服务前，通过合同协议等方式，提示客户按照国家及行业有关法规、政策要求、标准规范识别重要数据，加强个人信息保护，履行数据分类分级保护责任义务。根据数据类别级别，具备差异化安全保护能力，依据客户数据分类分级保护要求，配合做好相应的数据安全保护。

7. 数据访问安全。规范对客户数据的访问流程，配合客户建立访问控制策略，配备技术措施防范客户数据未授权访问等安全风险。

8. 数据操作安全。健全客户数据操作登记、权限审批、账号动态核验等机制。经客户授权，开展客户数据处理活动的，按照最小必要原则合理分配操作权限，做好权限监控，留存权限申请、审批、数据操作等相关日志记录，及时回收到期权限；开展数据批量下载、批量访问或客户重要数据、

个人信息操作处理的，单独履行内部审批程序。

9. 数据销毁安全。明确客户数据销毁安全策略和操作规程，针对不同类型的存储介质提供差异化数据销毁措施。未经授权，不擅自销毁客户数据。应客户要求销毁数据的，做好销毁记录，不得以任何理由、任何方式进行恢复。

10. 数据隔离安全。配备数据隔离安全策略，提供物理、逻辑等数据隔离方式，保障客户数据在各环节处理的独立性。

11. 高危操作安全。建立覆盖网络与设备更换、运维、升级，以及数据迁移等可能导致客户重大数据安全风险的高危操作台账，形成高危操作安全规范。开展高危操作前，告知相关客户涉及的系统范围、操作行为、时间、原因、可能存在的重大风险等，并取得客户授权。

12. 数据对外提供。涉及对外提供客户数据的，提前告知客户提供数据的目的、方式、范围、保障措施等，并取得客户授权。

13. 业务可用性保障。根据业务实际情况，通过冗余设计等，提高业务连续性和稳定性。

14. 安全事件应急处置。建立客户数据安全事件应急预案，覆盖客户数据丢失、损毁、泄露等安全事件场景，明确事件分级处置方法、流程等，定期组织开展应急演练，提升客户数据安全事件应急处置能力。因IDC业务经营者原因引发客户数据安全事件的，立即启动应急处置，及时告知客户，并结合事件影响程度，根据相关法规和标准要求向电信主管

部门报告。同时，根据事件类型、级别等，及时配合客户开展事件应急处置和上报。

15. 安全防护能力提供。根据业务实际情况，提供数据加密、脱敏、访问控制、鉴权与校验、日志记录与审计、数据备份与恢复等数据安全技术能力，以及防火墙、堡垒机、非法入侵检测、防篡改、漏洞扫描、病毒防范、安全升级等网络安全防护产品或服务供客户选择。

（四）服务器托管业务场景保障能力

1. 机房管理要求。规范机房安全管理，明确机房设施、客户设备、人员进出等安全管理要求。

2. 机房物理安全。配备机房物理安全保障措施，对关键区域实施 7*24 小时监控，具备对异常进出行为的识别、报警、拦截、处置等能力。

3. 机房权限管理。设置机房进出权限清单，明确权限范围、有效期及审批人等信息。对清单外人员机房进出实施严格审批，经客户授权进入机房开展设备、数据运维管理的，配备相应的管理和技术措施，留存机房进出记录，严格限制非授权人员进入。

4. 机房值守管理。安排 7*24 小时人员值守，建立基础设施巡检、风险处置规程，实施常态化巡逻、检查，及时发现、消除风险隐患。

5. 消防系统安全。配备消防供电设施、火灾自动报警系统、应急照明系统、双重水电系统等，保障极端情况下机房快速恢复和运转。

6. 设备供应管理。涉及提供服务器、网络设备等售卖、租赁服务的，做好设备安全管理，建立设备台账，记录设备品牌、型号、关键性能参数、采购时间、来源，以及安全应用情况等。设备上架前做好安全检查，并定期开展维护更新，加强安全漏洞、设备及系统配置等安全管理。涉及为党政机关等重点客户提供服务的，鼓励IDC业务经营者使用自主可控的网络与数据安全设备。

（五）数据存储与计算业务场景保障能力

1. 数据存储安全。加强客户数据存储安全管理，提供容灾备份、校验技术、密码技术等数据安全保护能力，以满足客户不同的数据储存安全需求。

2. 数据安全风险监测。加强数据安全风险监测预警，梳理掌握流量节点，配备流量分析、过滤等技术手段，具备发现数据安全风险能力，及时排查、整改数据安全问题隐患。

3. 资源监控和负载均衡。配备存储和计算资源监控技术能力，实时监控、统计分析资源使用情况，及时预警发现异常使用情形。配备存储和计算资源负载均衡技术能力，根据资源负载情况实时动态调整资源分配，保障资源的安全可用。

4. 数据传输安全。加强客户数据传输安全管理，根据传输客户数据级别和应用场景，配合客户制定安全传输策略，并提供数据加密、接口鉴权、安全审计等保护措施。满足客户数据传输安全需求和定期接口安全审计需要，及时调整接口状态，回收、关闭废弃接口。

5. 人工智能训练数据安全。涉及提供人工智能训练数据集管理功能的，需提供保障客户自有训练数据集安全的能力，避免客户自有训练数据集被泄露、污染。

6. 算力调度安全。涉及提供算力调度服务的，配备安全可靠的算力调度策略，做好策略配置管理和变更审批，保障算力按需合理分配。涉及提供算力服务的，具备对算力使用情况的实时监测能力，发现并预警算力资源异常使用情形，及时采取策略调整、资源停用等措施。