数据安全从业人员能力基本要求

编制说明

标准起草工作组

2024 年 12 月

目　录

1 必要性

随着数字化进程的加速推进，数据在各行业各领域发挥着愈发关键的作用，与此同时，数据安全面临的挑战也日益严峻。为了规范数据安全从业人员的能力水平，提升相关从业者专业素养，确保其能够有效应对各类数据安全风险，保障数据全生命周期的安全性、完整性与保密性，进而推动各行业在数字化转型浪潮中健康、稳定发展，特编制《数据安全从业人员能力基本要求》标准。该标准的出台，有助于明确数据安全从业人员的能力基线，为人才培养、选拔、评价等环节提供科学依据，对筑牢数据安全防线、维护国家安全和社会公共利益以及促进数字经济高质量发展都有着至关重要的意义。

2 工作简述

2.1 任务来源

本标准根据四川省网络空间安全协会数据安全团体标准制修订计划立项，由四川省网络空间安全协会归口，由成都信息工程大学牵头组织编制。

2.2 起草单位

本标准牵头起草单位：成都信息工程大学；

本标准参加起草单位：成都卓越华安信息技术服务有限公司、四川省数字产业有限责任公司、中国民用航空西南地区空中交通管理局。

2.3 起草过程

2024 年 7 月，成都信息工程大学向四川省网络空间安全协会提交《数据安全从业人员能力基本要求》团体标准项目建议书；

2024 年 8 月，由四川省网络空间安全协会邀请专家对《数据安全从业人员能力基本要求》立项评审，标准立项，成立标准起草工作组。

2024 年 10 月，召开《数据安全从业人员能力基本要求》团体标准启动会议，会议讨论了本标准的框架，确定了标准起草的总体框架、主要内容、人员分工；

2024 年 11 月，完成了数据安全团体标准《数据安全从业人员能力基本要求》草案稿编写；

2024 年 12 月，专家对标准征求意见稿进行了评审，《数据安全从业人员能力基本要求》标准质量达到征求意见稿发布要求。

3 标准编制原则和主要内容

3.1 编制原则

本标准的制定工作遵循的原则如下：

(1) 合规性原则。在标准制订过程中，紧密依据国家已颁布的相关法律法规，包括但不限于《网络安全法》《数据安全法》《个人信息保护法》以及《网络数据安全管理条例》等，

确保标准内容完全符合法律要求，同时与现行的相关国家标准（如 GB/T 42446—2023 信息安全技术 网络安全从业人员能力基本要求及 GB/T 43697—2024 数据安全技术 数据分类分级规则）和职业标准（如 《数据安全工程技术人员 国家职业标准》及《网络与信息安全管理员(数据安全管理员) 国家职业标准》）协调一致，避免出现任何与上位法和其他标准相冲突的条款，保障标准的合法性与兼容性，使其能够在合法合规的框架内为数据安全从业人员能力建设提供坚实的依据和指导。

(2) 科学性原则：运用科学的方法和严谨的逻辑，对数据安全领域的工作内容、流程、技术等进行深入分析和系统研究，充分借鉴国内外先进的理论成果和实践经验，结合我国数据安全行业的实际发展状况和特点，合理确定从业人员的能力要素、能力等级划分以及能力评价方法等关键内容，确保标准内容具有高度的科学性、合理性和前瞻性，能够准确反映数据安全行业对从业人员能力的本质需求和发展趋势，为数据安全人才的培养、选拔和评价提供科学可靠的衡量尺度。

(3) 实用性原则：标准的编制紧密围绕数据安全从业人员的实际工作场景和业务需求，以解决实际工作中的数据安全问题为导向，注重标准内容的可操作性和可落地性。各项能力要求和指标设定均力求具体、明确、实用，便于从业人员理解和掌握，同时也方便企业和相关机构在人员招聘、培训、考核等

方面能够直接应用该标准，确保其能够切实有效地提升数据安全从业人员的工作能力和实践水平，为数据安全工作的实际开展提供有力的支持和保障。

(4) 动态适应性原则：考虑到数据安全技术的快速发展和法律法规的不断完善，标准在编制过程中充分预留了更新和优化的空间，建立了动态调整机制。通过持续关注行业动态、技术演进和法规变化，定期对标准进行评估和修订，使其能够及时适应数据安全领域的新情况、新问题和新要求，保持标准的时效性和有效性，始终为数据安全从业人员能力建设提供与时俱进的指导和规范。

3.2 主要内容

本标准共分为六章，如下：

1．适用范围

2．规范性引用文件

3．术语和定义

4．通则

5．通用知识和技能要求

6．专业知识和技能要求

4 技术论证与效果

4.1 技术要求和指标来源依据

本标准中各项技术要求和指标的确立，是在深入研究国内

外数据安全领域的先进技术实践、广泛调研行业发展现状以及充分借鉴相关国际标准和国内已有的类似标准基础上形成的。

(1) 法规与政策导向：紧密结合国家出台的一系列数据安全相关法律法规，如《网络安全法》《数据安全法》《个人信息保护法》等，确保技术要求符合法律规范，保障数据在合法合规的框架内进行处理与保护。例如，在数据访问控制技术要求方面，严格遵循法规中对数据授权访问的规定，明确不同级别数据访问的权限设置和审批流程技术指标，防止未经授权的数据访问和泄露。

(2) 行业最佳实践：对金融、电信、互联网等数据密集型行业的头部企业进行了深入调研，分析其在数据加密、存储安全、传输安全、应急响应等方面的成熟技术方案和操作流程。例如，参考金融行业在数据加密算法选择和密钥管理方面的实践经验，确定了适用于全行业的数据加密技术强度和密钥管理技术指标，包括加密算法的类型、密钥长度、密钥更新频率等，以保障数据的保密性和完整性。

(3) 学术研究成果：积极引入数据安全领域的前沿学术研究成果，如新型的数据隐私保护技术、人工智能驱动的安全监测技术等，为标准的技术先进性提供支撑。例如，在数据泄露检测技术指标中，纳入了基于机器学习算法的异常行为检测敏感度和误报率等指标，使标准能够跟上技术发展的步伐，引导行业采用更高效、智能的数据安全防护技术。

4.2 技术路线

本标准在制定过程中，遵循了系统性、可行性和前瞻性相结合的技术路线。

(1) 政策法规与学术资料归集

组建专业的资料收集小组，通过多途径广泛搜集国内外与数据安全相关的政策法规文本，涵盖国家层面的数据安全法、个人信息保护法等核心法规，以及各地区、各行业为细化落实上位法出台的配套政策。同时，系统梳理权威研究报告中涉及数据安全从业人员知识体系、技能范畴的前沿理论。将这些资料汇总整理，构建起丰富且完备的法规政策与学术理论资源库，为标准设计提供坚实的法理依据与理论支撑。

(2) 行业现状与需求实地探察

运用问卷调查、案例剖析等手段，全方位了解不同行业的数据业务运转模式、所面临的数据安全风险挑战，以及在当前复杂多变的数据安全环境下对从业人员专业素养的迫切需求。精准掌握各行业数据从采集、存储、传输到使用、共享、销毁全生命周期中关键节点的安全保障诉求，从而确保标准紧密贴合行业实际，切实可行。

(3) 多维能力维度界定

基于前期深入调研成果，抽丝剥茧提炼出数据安全从业人员所需具备的关键能力维度。首先，确立知识维度，囊括数据安全领域的基础法律法规知识，从通用的国家大法到极具行业

针对性的规范细则；深入至密码学基础知识，涵盖加密算法原理、密钥管理机制等；以及各类数据安全技术原理，像网络防护技术、数据存储安全技术等。其次，聚焦技能维度，涵盖数据安全规划设计技能，诸如为企业量身定制贴合业务流程的数据安全整体架构；技术开发与运维技能，保障数据安全系统的稳定运行与持续升级；监测与应急处置技能，能在第一时间察觉数据异常并迅速采取有效措施化解危机；审计和评估技能，以严谨的态度与专业的方法审查数据安全体系的合规性与有效性。

(4) 工作任务与能力精准匹配

详细拆解数据安全领域的各类工作任务，按照数据安全规划、技术开发、运维监测、应急处置、审计评估、科研教育等主要工作类别逐一罗列细分任务。针对每一项具体任务，深度剖析其所需的知识、技能、素养支撑，将任务要求与能力框架中的相应层级进行精准对接。例如，对于数据安全应急处置任务中的数据泄露事件处理，明确要求应急人员具备中级及以上的法规知识，熟悉数据泄露相关法律责任界定；拥有高级的应急处置技能，能迅速启动应急预案，有条不紊地开展溯源、止损、恢复等系列操作；并具备较强的沟通应变素养，及时向内外各方准确通报事件进展，安抚人心。通过这种一一对应的方式，确保标准内容紧密围绕实际工作需求，为从业人员提供极具针对性的能力指南。

4.3 社会效益估计

提升公众数据安全意识：通过在全行业推行统一的数据安全从业人员能力标准，促使企业更加重视数据安全工作，进而加强对公众的数据安全宣传教育，提高公众对数据隐私保护的认知和重视程度，增强公众在数字生活中的安全感和信任感，营造全社会关注数据安全的良好氛围。

4.4 对产业发展的作用

促进人才培养与产业协同发展：本标准为数据安全人才培养提供了明确的方向和目标，有利于高校、职业院校等教育机构优化相关专业设置和课程体系，培养出更多符合市场需求的数据安全专业人才，缓解当前人才短缺的局面。同时，人才的汇聚又将进一步推动产业的技术创新和发展，形成人才与产业相互促进、协同发展的良好局面，为数据安全产业的可持续发展提供坚实的人才保障和智力支持。

5 对标情况

5.1 国内外标准对比分析

在本标准的制定（修订）过程中，编制团队对国内外相关数据安全标准进行了全面、深入的研究与对比分析，旨在充分借鉴国际先进经验，同时结合我国国情与行业实际需求，确保本标准的科学性、先进性与实用性。

(1) 国际标准参考：对国际标准化组织（ISO）、国际电

工委员会（IEC）等国际权威机构发布的数据安全相关标准，如 ISO/IEC 27001（信息安全管理体系标准）、ISO/IEC 27002（信息安全控制实践指南）等进行了详细研究。在数据安全管理体系框架构建方面，参考了 ISO/IEC 27001 中的管理体系要求，包括风险评估、安全策略制定、人员管理等要素，结合我国数据安全行业特点进行了本土化调整与细化，确保本标准既与国际通行做法接轨，又能满足国内企业实际运营环境的需求。例如，在人员管理方面，根据我国数据安全从业人员的技能现状和职业发展路径，对人员资质认证、培训教育内容与频次等指标进行了更具针对性的规定，使其更具可操作性。

(2) 国外先进标准借鉴：同时，对美国国家标准与技术研究院（NIST）发布的一系列数据安全标准，如 NIST SP 800-53（信息系统和组织的安全与隐私控制）、NIST SP 800-171（保护非联邦系统和组织中的受控非机密信息）等进行了深入分析。在数据安全技术要求方面，借鉴了 NIST 标准中关于数据加密、访问控制、网络安全防护等技术领域的先进理念和方法。例如，在数据加密技术指标上，参考了 NIST 对加密算法强度、密钥管理机制等方面的要求，结合我国密码技术发展现状和应用场景，制定了符合国内密码政策法规且具有同等安全性水平的加密技术标准，确保我国数据安全防护技术在国际上具有一定的竞争力和兼容性。

(3) 国内现有标准协调：与国内已发布的数据安全相关标

准，如《信息安全技术 网络安全等级保护基本要求》《信息安全技术 数据安全能力成熟度模型》等进行了充分协调与整合。在标准适用范围和技术要求上，注重避免重复与冲突，实现互补与协同。例如，在数据安全能力评估方面，与《信息安全技术 数据安全能力成熟度模型》相互呼应，本标准侧重于从从业人员能力角度出发，为企业数据安全能力建设提供人员层面的衡量标准和指导，而该模型则从企业整体数据安全能力成熟度等级划分的角度，为企业提供全面的能力提升路径规划，两者共同构成了企业数据安全能力建设的标准体系，为企业在不同发展阶段的数据安全建设提供了全方位的支持。

5.2 与现行法律法规和强制性国家标准的关系

本标准严格遵循国家现行的法律法规和强制性国家标准，确保标准内容的合法性和合规性，同时积极响应国家政策导向，为法律法规的有效实施提供技术支撑和人员能力保障。

(1) 法律法规遵循：紧密围绕《网络安全法》《数据安全法》《个人信息保护法》等法律法规的要求，将法律规定的各项数据安全义务和责任细化为对从业人员的具体能力要求。例如，依据《数据安全法》中关于数据分类分级保护的规定，本标准明确了数据安全从业人员应具备的数据分类分级方法制定、实施与维护的能力，包括如何根据数据的重要性和敏感程度进行合理分类、如何针对不同级别数据采取相应的安全防护措施以及如何定期对数据分类分级情况进行评估和调整等，确

保企业在数据处理活动中能够切实履行法律规定的分类分级保护义务，防止因人员能力不足导致的数据安全违法行为。

(2) 强制性国家标准衔接：与相关强制性国家标准，如《信息安全技术 信息系统安全等级保护定级指南》《信息安全技术 信息系统安全等级保护基本要求》等保持高度一致和紧密衔接。在标准的技术指标和能力要求设定上，充分考虑了等保要求对数据安全防护措施的规定以及对从业人员专业技能的需求。例如，在网络安全防护能力方面，对应等保标准中对网络边界防护、入侵检测与防御等技术要求，本标准规定了数据安全从业人员应具备的网络安全技术知识和操作技能，包括网络设备配置与管理、网络安全漏洞检测与修复、网络攻击事件应急响应等能力，使从业人员能够熟练掌握并实施符合等保要求的网络安全防护措施，保障信息系统的安全稳定运行，实现本标准与强制性国家标准在技术要求和人员能力保障上的无缝对接。

6 标准实施建议

鼓励各行业协会积极参与标准实施工作，发挥行业自律和桥梁纽带作用。行业协会应组织开展本行业的数据安全培训、技术交流和经验分享活动，帮助企业深入理解和贯彻本标准；同时，收集企业在实施过程中遇到的问题和反馈意见，及时向相关部门汇报，为标准的持续优化提供参考依据。

考虑到部分企业在人员能力、技术水平和管理体系等方面可能与本标准存在一定差距，为确保标准平稳落地实施，设定合理的过渡期。在过渡期内，企业应按照“分步实施、逐步达标”的原则，制定详细的整改计划，明确各阶段的工作目标和任务，有序推进标准实施工作。相关部门应加强对企业过渡期实施情况的监督检查和指导服务，及时发现并解决问题，确保企业在过渡期结束后能够达到标准要求。

7 需要说明的主要问题

本标准在编制过程中未出现需要说明的主要问题

8 其他说明事项