《网络安全人才实战化训练环境建设团体标准》

编制说明

2024 年 8 月

一、工作简况

（一）任务来源

本标准由奇安信科技集团股份有限公司、湖北经济学院共同提出，报武汉市网络安全协会批准。

本文件规定了网络安全人才实战化训练环境建设的基本要求，包括网络安全人才实战化训练环境建设框架、实训设施、训练环境建设、实训管理等方面的要求。

本文件适用于应用型本科院校、高职院校、校企合作网络安全公司等信息安全类专业实训室的规划设计、建设和运营。网络安全公司、中等职业学校及其他类型学校可参考执行。

（二）起草单位情况

本标准起草单位包括奇安信科技集团股份有限公司、湖北经济学院、武汉市网络安全协会、湖北省教育装备行业协会、武汉职业技术学院、武汉软件工程职业学院、湖北科技职业学院、武汉商贸职业学院、武汉交通职业学院、湖北国土资源职业学院、鄂州职业大学、长江职业学院、湖北职业技术学院、武汉东西湖职业技术学校、武汉同德兴信息技术有限公司、武汉铁路职业技术学院、江汉大学、武汉商学院、汉口学院、湖北华育智远信息科技有限公司、武汉科云信息技术有限公司等。

（三）标准编制过程

（1）成立标准编写组，技术调研和资料收集

本标准立项后，起草单位和主要技术专家针对湖北实际情况与国内网络安全发展现状，对网络安全人才、实战公训练内容、相关技术事宜进行调查分析、实验和验证等工作，并着手成立标准编写组。

2024 年 3 月 29 日，由起草单位和相关技术专家共同组建了标准编写组，并召开了本团体标准编写组成立会议暨第一次团体准备工作会议。

在本次工作会议上，对相关标准的范围、框架、技术要素、编制内容和技术等内容进行了确定。通过工作会议，通过了制订工作方案、团体标准的目录结构，团体标准编写组进一步明确了目标要求、工作思路、人员分工和工作进度等。

（2）修订标准草案，完善标准文档

2024 年 7 月 4 日，团体标准编写组召开了第二次团体标准工作会议。在此次工作会议上，

主要是对团体标准初稿的框架、结构和目录内容进行了研讨，例如范围、规范性引用文件、术语和定义、网络安全人才实战化培养定位、网络安全人才实战化训练环境建设的基本要求、网络安全人才实战化训练环境设施的基本要求、网络安全人才实战化训练平台系统的基本要求、网络安全人才实战化对抗赛的基本要求、网络安全人才实战化师资队伍的基本要求、网络安全人

才实战化训练环境建设的考核体系以及网络安全人才实战化实训室管理的基本要求等。最后明确了修改意见和计划。

（3）形成标准征求意见稿，开展征求意见

2024 年 8 月 10 日，团体标准编写组对标准草案进行修改完善，包括调整整体框架结构、修改错误用词和格式，完善相关技术指标、管理要求等，在反复讨论和论证的基础上，修改形成了标准征求意见稿。

二、标准制定目标与意义

1）制定目标

（1）提升网络安全人才实战能力：团体标准的主要目标是构建一个贴近实战的网络安全人才训练环境，使学员能够在高度仿真的网络攻防场景中接受训练，从而提升其应对真实网络安全威胁的能力。

（2）促进标准化与规范化：通过制定团体标准，推动网络安全人才实战化训练环境的标准化和规范化，确保不同训练机构之间的训练内容和质量保持一致，提高整体训练水平。

（3）适应国家网络安全需求：紧密结合国家对网络安全的要求和当前网络空间安全的环境，制定具有前瞻性和实用性的标准，确保训练内容紧跟时代步伐，满足国家网络安全建设和发展的需要。

（4）推动技术创新与应用：鼓励在训练环境中引入最新的网络安全技术和方法，如人工智能、大数据、区块链等，促进技术创新和应用，提高训练的科学性和有效性。

2）制定意义

（1）满足国家重大战略需求：网络安全是国家安全的重要组成部分，制定团体标准有助于培养一支高素质、专业化的网络安全人才队伍，满足国家网络安全建设和发展的需要，为国家经济发展保驾护航。

（2）提升网络空间安全防御能力：通过实战化训练，使学员掌握先进的网络攻防技术和策略，提升国家在网络空间的安全防御能力，有效应对各类网络威胁和挑战。

（3）推动网络安全产业发展：团体标准的制定和实施将促进网络安全产业的发展，为网络安全企业提供标准化的产品和服务，推动技术创新和产业升级。

（4）促进国际合作与交流：在制定团体标准的过程中，可以借鉴国际先进经验和做法，促进国际合作与交流，提升我国在国际网络安全领域的影响力和话语权。

（5）提高社会认知与意识：团体标准的发布和实施将提高社会各界对网络安全重要性的认识，增强公众的网络安全意识，推动形成全社会共同维护网络安全的良好氛围。

3）具体实施措施

（1）明确指导思想和基本原则：制定团体标准时，应明确指导思想、目标任务和基本原则，确保标准制定的科学性、系统性和有效性。

（2）构建实战化训练环境：将网络安全实验平台与网络安全仿真系统相结合，为学员提供更加逼真的实验环境，提高实验的趣味性和有效性。同时，建立健全实验平台的管理和维护机制，确保实验平台的正常运行和安全使用。

（3）加强师资队伍建设：组织具有丰富网络安全实战经验和教学经验的专家、学者参与标准制定和教学工作，提高师资队伍的整体素质和教学水平。

（4）推动技术创新与应用：鼓励在训练环境中引入最新的网络安全技术和方法，如生成式人工智能、零信任体系等，促进技术创新和应用，提高训练的科学性和有效性。

（5）加强标准宣贯与实施：依托国家网络安全宣传周、世界标准日等重要活动平台，举办网络安全标准主题宣贯培训活动，促进标准实施应用。同时，开展网络安全标准系列宣讲活动，推进网络安全标准进企业、进校园，以标准促进网络安全技术、教育、产业融合发展。

综上所述，《网络安全人才实战化训练环境建设团体标准》的制定目标与意义在于提升网络安全人才的实战能力、促进标准化与规范化、适应国家网络安全需求、推动技术创新与应用以及

提高社会认知与意识。通过具体实施措施的实施，将有力推动我国网络安全事业的发展。

三、标准编制原则和主要内容

（一）标准编制原则和依据

在编制团体标准《网络安全人才实战化训练环境建设团体标准》时，团体标准编写组主要遵循科学性原则、规范性原则、一致性原则和可操作性原则，以确保标准的科学性、权威性、适用性和有效性。以下是从这四个方面给出的标准编制原则和依据:

1）科学性原则。本文件的主要指标是根据国内外先进标准和技术文献，并结合国家法律法规规定、国际标准化组织（ISO）、国家标准、行业标准、地方标准、团体标准等要求确定的，以及国内外权威技术文献，确保标准内容与国际接轨，反映网络安全领域的最新研究进展和实际应用情况，将最新的研究成果融入标准之中，提高标准的科学性和前瞻性。同时还组织网络安全领域的专家学者对标准草案进行咨询和评审，确保标准内容的科学性和合理性。

2）规范性原则。一是国家和行业相关法律法规，依据《网络安全法》、《数据安全法》、《个人信息保护法》等国家法律法规，以及网络安全行业的相关规定和要求，制定符合法律法规要求的标准内容。二是标准化工作导则，遵循国家标准《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》

（GB/T1.1—2020）的有关规定，确保标准的编制过程规范、严谨，符合标准化工作的基本要求和程序。三是术语和定义统一，对标准中涉及的术语和定义进行统一规范，确保标准内容的准确性和一致性。

3）一致性原则。一是现有相关标准。保持新编制的标准与现有标准在内容、要求等方面保持一致，避免重复和矛盾。二是国家和行业政策导向。紧密跟踪国家和行业在网络安全方面的政策导向和发展趋势，确保标准内容符合国家和行业的总体要求和规划。三是跨领域协调。加强与相关领域（如信息技术、数据安全等）的协调沟通，确保标准内容在跨领域应用时的一致性和协调性。

4）可操作性原则。一是实际需求调研。通过广泛的调研和需求分析，了解网络安全人才实战化训练环境建设的实际需求和使用场景，确保标准内容贴近实际、具有可操作性。二是案例分析和示范。结合国内外成功的网络安全人才实战化训练环境建设案例进行分析和示范，为标准的实施提供具体指导和参考。三是技术实现路径明确。明确标准内容的技术实现路径和具体方法步骤，确保实施者能够按照标准要求进行操作和实施。

（二）标准主要内容

本标准通过构建网络安全人才实战化训练环境建设体系，深入讨论了网络安全人才实战化训练环境建设框架的基本要求，包括实战化训练环境建设的具体说明和实施步骤。讨论了如何通

过网络安全人才实战化培养定位、实战化训练环境建设、师资队伍建设、竞赛和考核管理等步骤，系统地进行实战化训练环境建设工作。

1）网络安全人才实战化训练环境建设要求。一是讨论了建设硬件与软件配置。规定训练环境所需的基础硬件设施和软件平台，包括模拟网络拓扑结构、攻防工具集、靶机系统等。二是讨论了安全隔离与监控。确保训练环境与实际生产环境的安全隔离，并设置有效的监控机制，防止训练活动对外部网络造成潜在威胁。三是讨论了数据保护与隐私。明确在训练过程中数据的采集、处理、存储和销毁的安全要求，保护个人隐私和敏感数据。

2）网络安全人才实战化训练内容。一是课程体系。构建涵盖网络攻防基础、渗透测试、漏洞挖掘、应急响应、安全运维等实战化课程模块。二是案例与场景。设计贴近实际的网络攻击案例和模拟场景，包括 APT 攻击、勒索软件攻击、供应链攻击等，提升学员应对复杂威胁的能力。三是攻防对抗演练。定期组织红蓝对抗演练，模拟真实网络攻防场景，提升学员的实战对抗能力。

3）网络安全人才实战化训练师资队伍与教学资源。一是师资要求。规定从事实战化训练的教师应具备的资质、经验和技能要求，确保教学质量。二是教学资源。整合国内外优质的网络安全教材、视频教程、在线课程等教学资源，为学员提供丰富的学习材料。

4）网络安全人才实战化训练的评估与认证。一是考核标准。制定详细的考核标准和评价体系，对学员的学习成果进行客观、公正的评估。二是认证机制。建立网络安全人才实战化训练认证机制，为通过考核的学员颁发认证证书，提升其在就业市场的竞争力。

5）网络安全人才实战化训练的持续改进与反馈。一是持续改进。建立训练环境的持续改进机制，根据技术发展和实战需求不断更新和完善训练内容。二是反馈机制。设置学员反馈渠道，收集并分析学员对训练环境、课程内容和师资质量的反馈意见，及时进行调整和优化。

（三）解决的问题

本标准主要解决5个方面问题

1）实战能力不足的问题。

问题描述：传统的网络安全教育往往侧重于理论知识传授，缺乏实战化训练，导致学员在面对真实网络攻击时缺乏应对能力。

解决方案：通过构建实战化训练环境，提供贴近实际的网络攻防案例和模拟场景，让学员在实战中学习和成长，有效提升其应对复杂威胁的实战能力。

2）网络安全人才短缺的问题

问题描述：随着网络技术的快速发展，网络安全威胁日益严峻，但网络安全专业人才却供不应求，难以满足行业需求。

解决方案：通过制定和实施团体标准，规范网络安全人才培养体系，提高培训质量和效率，从而加快网络安全人才的培养速度，缓解人才短缺问题。

3）网络安全教育体系不完善的问题

问题描述：现有的网络安全教育体系可能存在课程设置不合理、教学资源匮乏、评估机制不健全等问题，难以满足实战化训练的需求。

解决方案：团体标准将明确训练环境建设的要求、训练内容、师资队伍和教学资源等方面的标准，推动网络安全教育体系的完善和发展。

4）网络安全技术创新与应用不足的问题

问题描述：网络安全技术的快速发展要求从业人员具备不断学习和创新的能力，但当前的教育培训体系可能无法及时跟上技术发展的步伐。

解决方案：通过实战化训练环境的建设，引入最新的网络安全技术和工具，让学员在实战中学习和掌握新技术，推动网络安全技术的创新与应用。

5）网络安全防护水平不高的问题

问题描述：由于网络安全人才实战能力不足和培训体系不完善等问题，导致许多组织在面对网络攻击时无法有效防护。

解决方案：通过提升网络安全人才的实战能力和技术水平，提高组织的网络安全防护意识和能力，从而降低网络安全事

件的发生率和影响范围。

综上所述，团体标准《网络安全人才实战化训练环境建设团体标准》的制定和实施，将有效解决当前网络空间安全环境下存在的实战能力不足、人才短缺、教育体系不完善、技术创新与应用不足以及防护水平不高等问题，为提升国家网络安全整体实力提供有力保障。

四、与现行法律、法规、标准的关系

该标准的内容符合《中华人民共和国标准化法》等法律法规，符合安全性要求及有关强制性标准要求。本文件规范性引用文件包括

JY/T 0595-2019　基础教育装备　分类与代码

T/CAS 375-2019　网络安全服务机构等级评定规范

GA/T 1717.1-2020　信息安全技术　网络安全事件通报预警 第 1 部分：术语

GB/T 25069-2022　信息安全技术　术语

GB/T 29264-2012　信息技术服务　分类与代码

GB/T 32921-2016　信息安全技术　信息技术产品供应方行为安全准则

GB/T 20984-2022　信息安全技术　信息安全风险评估方法

GB/T 22240-2020　信息安全技术　信息系统安全等级保护

定级指南

GB/T 25058-2019　信息安全技术　信息系统安全等级保护实施指南

GB/T 41479-2022　信息安全技术　网络数据处理安全要求

GB/T 20275-2021　信息安全技术　网络入侵检测系统技术要求和测试评价方法

GB/T 28458-2020　信息安全技术　网络安全漏洞标识与描述规范

GB/T 40652-2021　信息安全技术　恶意软件事件预防和处理指南

GB/T 39680-2020　信息安全技术　服务器安全技术要求和测评准则

GB/T 37932-2019　信息安全技术　数据交易服务安全要求

GB/T 28450-2020　信息技术　安全技术　信息安全管理体系审核指南

GB/T 36342-2018　智慧校园总体框架

因为国内外网络安全人才实战化训练场景和要求存在较大差异，因此本标准在起草过程中没有采用国际相关标准

五、标准中涉及专利的情况

不涉及

六、重大分歧意见的处理经过和依据

本文件编制过程中无重大意见分歧。

七、贯彻标准的措施建议

本文件一经批准发布，编制组单位应组织相关高等学校、机构和企业开展标准宣贯培训，使标准得到有效运用，并跟踪调查该地方标准的执行情况，及时发现和收集执行中的问题清单，不断修改完善，进一步提高本文件的科学性、适用性。

八、其他应予说明的事项

无