vinchin

逐条精解新网络安全法中的“灾备密码”

vinchin

PART 01

新网络安全法整体解读

一次立足全局的重要升级

vinchin

2026年1月1日起施行的重大修订，系2017年以来首次，旨在应对数字中国与人工智能时代的新挑战

实施时间

自2026年1月1日起正式施行，标志着近年来网络与数据治理领域最为关键的一次制度调整，具有显著的时效性与前瞻性

修订背景

面对数字中国建设加速推进和人工智能技术广泛应用带来的新风险与新问题，此次修订应运而生，回应时代发展需求

历史节点

这是自2017年以来对该制度的首次重大修订，凸显当前技术变革背景下法律法规更新的紧迫性与必要性

核心基调

以统筹发展与安全为根本指导原则，推动技术创新与风险防控并重，实现高质量发展与高水平安全的动态平衡

监管支撑

为政府监管提供更加明确、有力的法律依据，增强对新兴技术应用场景下违法违规行为的识别与处置能力

全局影响

此次升级不仅关乎技术治理，更涉及国家数字战略全局，将深刻影响未来数年数字经济与社会发展的路径方向

本次修订释放的四大核心信号

vinchin

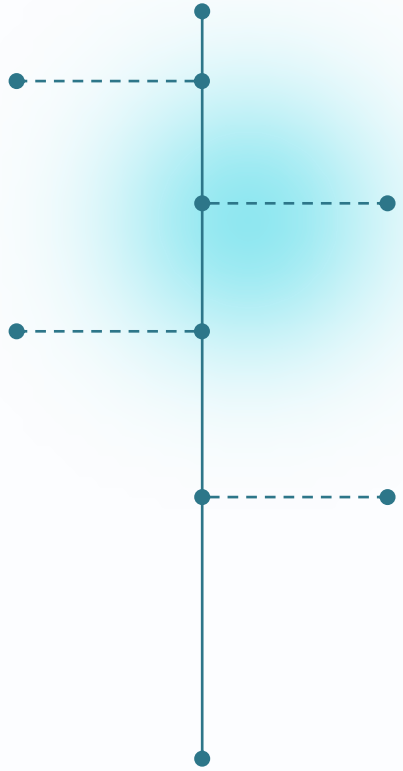
从罚则加码到治理协同的全面升级

威慑力飙升

本次修订大幅提高行政处罚上限，最高罚款金额提升至一千万元，显著增强法律威慑力，倒逼企业落实网络安全主体责任。

监管前瞻化

新增人工智能治理相关条款，明确对算法设计、训练数据来源与使用过程的合规要求，推动新技术应用在法治轨道上健康发展。



责任链条化

强调与《个人信息保护法》《网络安全法》等现行法律的衔接配套，厘清监管边界，构建跨领域、跨部门的协同治理责任体系。

源头强管控

首次将网络关键设备与安全产品的销售环节纳入处罚范围，强化对供应链源头的准入管理和全生命周期安全监管。

法律“牙齿”更锋利

vinchin

罚款上限从100万到1000万，强化网络安全责任

1

旧法规定

根据旧法第六十一条，单位未履行网络安全保护义务且造成后果的，最高仅可处以一百万元罚款，处罚幅度单一，缺乏针对性和威慑力。

2

新法突破

新法设立阶梯式处罚机制，依据违法情节轻重分层处理，实现过罚相当，提升执法精准性与公正性。

3

严重后果认定

对导致关键信息基础设施丧失主要功能、引发重大公共服务中断等特别严重后果的情形，明确列为最高处罚档，强化底线要求。

4

高额罚款标准

实施特别严重处罚时，罚款金额设定为二百万元以上一千万元以下，大幅提升违法成本，倒逼企业落实主体责任。

新法阶梯式处罚体系

vinchin

依据违法程度划分三级处罚标准，逐级加重惩戒力度

1

一般违法

责令改正+警告+罚款（1万至50万）

2

造成严重后果

如大量数据泄露、关键设施局部功能丧失，罚款50万至200万

3

造成特别严重后果

如关键设施主要功能丧失，罚款200万至1000万，个人最高罚100万

处罚递进逻辑

处罚层级依据危害程度递进设置，体现过罚相当原则，确保法律威慑力与公正性相统一

单位责任承担

各层级处罚均针对单位主体设定相应经济罚则，突出组织管理责任在违法行为中的核心地位

个人责任追究

在第三层级中明确对直接责任人最高处以100万元罚款，强化个体履职的法律责任约束

纠正与惩戒结合

首层处罚包含责令改正和警告措施，体现教育与惩戒相结合的执法理念，推动主动整改

筑牢供应链安全：销售/提供不合规产品将受重罚

vinchin

新增第六十三条强化网络产品合规监管

严厉处罚措施

- 对违法行为将没收违法所得，并处最高达违法所得5倍的高额罚款，情节严重者可责令停业整顿或吊销相关证照。

合规源头管控

- 通过从产品入网前端加强监管，有效防止“带病入网”现象，提升整体网络安全防护能力和运行稳定性。

禁止行为界定

- 明确禁止销售或提供未经安全认证、检测不符合要求的网络关键设备和网络安全专用产品，杜绝不合格产品进入网络系统。

供应商责任强化

- 要求产品供应商必须严格落实国家安全认证要求，承担起网络安全第一道防线的责任，确保所提供产品合法合规。

法律协同与责任豁免：更精细的治理

vinchin

法律衔接

第七十一条明确侵害个人信息等行为应直接依照《个人信息保护法》等专门法律进行处罚，有效避免法律适用上的重复与冲突，提升执法一致性。

豁免条款

第七十三条新增规定，对违反本法但符合《行政处罚法》中从轻、减轻或不予处罚情形的行为，如及时采取补救措施且危害后果轻微，可依法予以宽缓处理。

过罚相当

相关条款体现过罚相当原则，通过法律协同和责任豁免机制的结合，实现法律责任的精准化与人性化，促进守法激励与社会公平正义。

更精细的治理机制设计与法律适用逻辑

其他修订要点速览

本次修订涉及实名制、关基采购及域外效力等关键条款的扩展与完善

实名制扩展

第六十四条将实名制适用范围扩展至“应用程序”，并新增“关闭应用程序”作为处罚措施，强化对违规主体的约束力。

关基采购规范

第六十七条要求关键信息基础设施运营者使用未经安全审查产品时，须先限期改正并消除对国家安全的影响，体现审慎监管原则。

域外效力扩大

第七十七条将域外效力范围从“危害关键信息基础设施”扩展至所有“危害中华人民共和国网络安全的活动”，提升法律覆盖广度与威慑力。

修订总体方向与趋势

vinchin

党的领导强化 5

将“坚持中国共产党的领导”写入总则第三条，从法律层面确立“党管互联网”原则，确保网络安全工作的根本政治方向和制度保障

前瞻治理布局(AI) 3

新增第二十条，针对人工智能等新技术推行鼓励与监管并行策略，为AI发展划定法治轨道，防范技术滥用风险

重典治乱升级 1

全面提高违法成本，建立阶梯式处罚机制，增强法律威慑力，体现对严重网络违法行为的高压治理态势

法律体系协同 2

明确本法与《个人信息保护法》等相关法律的衔接关系，构建互补融合、协调统一的网络安全法治网络

源头管控加强 4

新增第六十三条，将关键信息基础设施设备的安全认证要求由政策层面上升为法定强制义务，强化供应链安全管控

柔性执法引入 6

新增第七十三条，引入《行政处罚法》中的豁免条款，体现过罚相当原则，鼓励企业主动合规与及时整改纠正

对关键信息基础设施行业的直接影响

vinchin

关基运营者面临更重责任与更严要求

责任加重

作为关键信息基础设施运营者，将适用《网络安全法》第六十一条规定的最严厉罚则，可能面临最高达千万元的行政处罚，并追究直接负责的主管人员个人法律责任

审查强化

根据第六十七条，采购网络产品和服务的安全审查要求被进一步强化，关基运营者须确保供应链安全，开展必要安全评估并配合主管部门审查

合规举证

在发生网络安全事件时，运营者需提供完整证据链，证明已履行“网络安全保护义务”，包括制度建设、技术措施落实和应急响应记录等合规行为

容灾备份

充分的容灾备份措施是履行保护义务的重要组成部分，必须建立数据备份机制、定期演练恢复流程，并留存操作日志以备核查

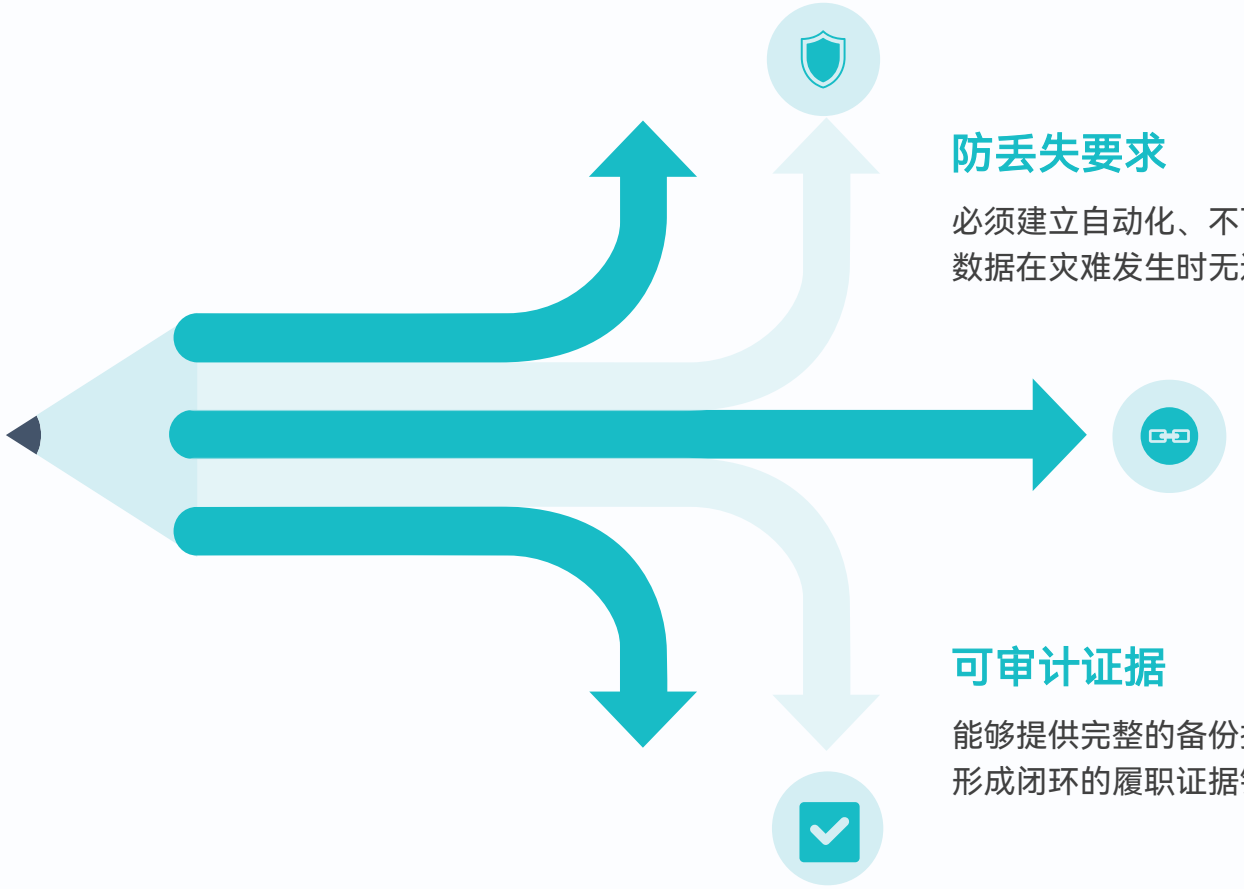
风险规避

通过建立健全网络安全管理体系、留存全过程合规记录，可有效证明尽职履责，在监管问责中降低被处以高额罚款的法律风险

“网络安全保护义务”的容灾备份解读

vinchin

如何构建法律认可的“必要措施”



防丢失要求

必须建立自动化、不可篡改且符合法规频率要求的数据备份机制，确保关键数据在灾难发生时无遗漏丢失，满足RPO指标并具备合规证明能力

保连续能力

需具备经过实际验证的业务恢复与应急响应方案，确保系统故障或安全事件后可在规定时间内快速恢复运行，切实达到RTO的技术与管理双重要求

可审计证据

能够提供完整的备份操作日志、定期恢复演练记录及第三方或内部审计报告，形成闭环的履职证据链以应对监管审查和法律责任认定

vinchin

PART 02

直面“监管之问”
掌握应对底气

直面监管之问：你的容灾备份体系能经得起问询吗

vinchin

监管典型五问

制度与策略之问

- 请出示的《容灾备份管理制度》和《业务连续性应急预案》。
- 备份策略（RTO/RPO）是如何制定的?
- 是否经过管理层的正式审批和定期评审?

1

备份有效性之问

- 核心业务数据（尤其是个人信息和重要数据）的备份频率是多少?
- 备份数据是否进行过完整性验证?
- 如何确保备份数据与生产数据一致且可用?

2

恢复能力之问

- 如果生产中心因故中断，你们承诺的恢复时间（RTO）和恢复点（RPO）具体是多少?
- 有何技术和管理措施来保障该承诺?

3

演练与验证之问

- 请提供最近1-2次的真实灾备演练记录和总结报告。
- 演练是否覆盖了关键业务场景?
- 是否验证了从备份数据成功恢复业务的全流程?

4

记录与审计之问

- 系统能否提供完整的备份操作日志、恢复操作日志和访问审计日志?
- 这些日志是否受到保护且留存周期符合法规要求?

5

备份策略（RTO/RPO）是如何制定的？

vinchin

科学制定RTO/RPO：业务需求与合规要求双轮驱动
有效的备份策略，需在业务可承受损失与法规强制要求之间取得平衡

业务需求层面：定义可承受的损失底线

从业务连续性的根本出发，回答两个核心问题：

关于时间（RTO）：
“当灾难发生时，业务最多能承受多长的中断时间？”
（这决定了恢复速度的底线）

关于数据（RPO）：
“当灾难发生时，业务最多能承受多长时间的数据丢失？”
（这决定了备份频率的底线）

此层面的目标是： 将业务影响转化为可量化的技术指标。

合规层面：满足监管的强制要求

遵循国家及行业权威标准，确保策略符合法规红线：

法律依据： 网络/数据安全法
通用基础： 网络安全等级保护2.0制度
行业深化： 金融、电力、电信等重点行业的专项监管条例
核心依据： 国家标准 《GB/T 20988-2007 信息系统灾难恢复规范》

此层面的目标是： 确保备份策略满足强制性的合规门槛。

直面监管之问：备份数据的“可用性”证明

vinchin

云祺以七大核心能力，为备份数据的终极可靠性、长期合规性与业务连续性提供闭环证明

核心维度	监管关切点	云祺解决方案
恢复闭环验证	备份数据是否真的能恢复？演练是否流于形式？	一体化验证与可审计的验证报告
长期合规归档	如何满足数据留存数十年的法规要求？如何防止历史数据被篡改或丢失	磁带库归档
基础设施韧性	备份存储本身是否成为单点故障？能否抵御区域性灾难？	异地副本容灾
存储安全底线	备份数据是否可能被勒索软件加密或人为误删？	WORM不可变存储
数据安全免疫	恢复的数据本身是否携带病毒，导致‘带毒恢复’？	防勒索杀毒
应用可用性保障	恢复的业务系统能否正常启动，数据是否逻辑一致？	快照
数据完整性	备份数据在存储中是否发生静默损坏？	完整性校验

三大支柱，兑现可信可用承诺

- 数据内生安全：保障备份数据的**完整性**、**一致性**、**洁净度**
- 架构韧性：通过**异地副本**、**不可变存储**、**磁带归档**，抵御各类风险
- 流程闭环：以**自动化恢复验证**形成可信证据链

直面监管之问：RTO/RPO承诺何以兑现？

vinchin

监管不只听承诺的数字，更要看支撑承诺的技术底气与管理证据。

云祺恢复方式	概述	RTO / RPO
复制容灾	提供整机、数据库、文件复制能力，实时复制数据到备机，支持手动/自动接管	RTO/RPO≈0
应急接管	支持虚拟机、物理机、云主机整机应急接管，无需外部资源	RTO<3分钟 备份频率越高RPO越低
瞬时恢复	支持磁盘、文件瞬时恢复，用于演练、验证、应急场景	RTO<1分钟 备份频率越高RPO越低
跨平台恢复	自由数据流动，如虚拟机、物理机、云主机之间的相互恢复，对象存储、文件服务器、HDFS、NAS之间的文件恢复等	支持应急接管与挂载恢复
细粒度恢复	整机、磁盘、文件等备份数据以细粒度方式恢复成文件，适合部分数据误删等场景	同上
数据恢复	将备份数据回迁至源环境	RTO主要与数据量和带宽相关 备份频率越高RPO越低

全域数据保护平台：云祺容灾备份系统

vinchin

vinchin

产品展示

vinchin

THANKS

云祺公众号

云祺视频号