ICS 35.040
L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 关键信息基础设施安全控制措施

Information security technology - Security Controls of Critical Information Infrastructure

在提交反馈意见时，请将您知道的相关专利连同支持文件一并附上。(征求意见稿)

（本稿完成日期：2018-6-13）

XXXX - XX - XX 发布　　XXXX - XX - 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本部分起草单位：中国信息安全研究院有限公司、中国电子技术标准化研究院、中国电子技术标准化研究院、国家工业信息安全发展研究中心、中国信息安全测评中心、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心、公安部三所、中国科学院软件研究所。

本部分主要起草人：

引　言

金融、能源、通信、交通等重点行业和领域的关键信息基础设施是经济社会运行的神经中枢，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益。当前，我国关键信息基础设施面临的网络安全形势严峻复杂，网络安全防控能力薄弱，难以有效应对网络攻击，《网络安全法》《国家网络空间安全战略》等提出建立关键信息基础设施安全保护制度。2017年7月，国家网信部门会同有关部门发布了《关键信息基础设施安全保护条例》（征求意见稿），条例明确了关键信息基础设施的具体范围，并提出了进一步的安全保护要求。此外，国家网信部门还会同有关部门起草了《网络产品和服务审安全审查办法（试行）》《国家网络安全事件应急预案》《个人信息和重要数据出境安全评估办法（征求意见稿）》，均对关键信息基础设施运营者提出了相关要求。

基于对《网络安全法》及相关法律法规要求的细化落实，围绕上述目标，结合目前已经开展的关键信息基础设施网络安全保护工作，全国信息安全标准化委员会组织开展了系列标准的制定，主要有以下五项标准。《关键信息基础设施网络安全框架》作为基础标准，阐明构成框架的基本要素及其关系，统一通用术语和定义；《关键信息基础设施网络安全保护基本要求》作为基线类标准，对关键信息基础设施运营者开展网络安全保护工作提出最低要求；本标准作为实施类标准，根据基本要求提出相应的控制措施；《关键信息基础设施安全检查评估指南》作为测评类标准，依据基本要求明确关键信息基础设施检查评估的目的、流程、内容和结果；《关键信息基础设施安全保障指标体系》作为测评类标准，依据检查评估结果、日常安全检测等情况对关键信息基础设施安全保障状况进行定量评价。

本标准将为关键信息基础设施保护工作的部门指导和监督关键信息基础设施运行安全保护工作提供技术参考，也可供关键信息基础设施运行安全保护工作的其他参与方参考，对提高我国关键信息基础设施安全保障水平具有十分重要的意义。

本标准与信息系统安全等级保护标准GB/T 22239-XXXX《网络安全技术 信息系统安全等级保护基本要求》不矛盾、不冲突、不重复，未修改或降低等级保护标准所规定的要求，在等级保护标准的基础上进一步提出关键信息基础设施安全保护的针对性要求。

信息安全技术 关键信息基础设施安全控制措施

1 范围

本标准规定了关键信息基础设施运营者在风险识别、安全防护、检测评估、监测预警、应急处置等环节应实现的安全控制措施。

本标准适用于关键信息基础设施的规划设计、开发建设、运行维护、退出废弃等阶段，可供关键信息基础设施保护工作部门、关键信息基础设施运营者以及关键信息基础设施安全保护中的其他参与者参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984-XXXX 信息安全技术 信息安全风险评估规范

GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

GB/T 22239-XXXX 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/T AAAAA-AAAA 信息安全技术 关键信息基础设施网络安全保护基本要求

GB/T BBBBB-BBBB 信息安全技术 数据出境安全评估指南

GB/T CCCCC-CCCC 信息安全技术 网络产品和服务安全通用要求

GB/T DDDDD-DDDD 信息安全技术 关键信息基础设施安全检查评估指南

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的信息设施。

3.2

控制措施 Controls

在管理、运行和技术等方面为关键信息基础设施规定的防护措施和对策。

3.3

重要系统 Important System

所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统。

3.4

重要数据 Important Data

与国家安全、经济发展以及社会公共利益密切相关的数据。

3.5

个人信息 Personal Information

以电子或者其他方式记录的能够单独或与其他信息结合识别自然人个人身份或者反映特定自然人活动情况的各种信息，包括但不限于自然人的姓名、出生日期、身份证号码、通信通讯联系方式、个人生物识别信息、住址、账号密码、财产状况、位置和行为信息等。

4 概述

4.1 关键信息基础设施保护相关角色和职责

关键信息基础设施正常运行是国家和社会正常运转的基础，国家采取措施，监测、防御、处置来源于我国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。关键信息基础设施网络安全保护中涉及到角色包括：关键信息基础设施运营者、关键信息基础设施安全保护工作部门以及关键信息基础设施安全保护中的其他参与者。

——关键信息基础设施运营者：负责关键信息基础设施的运行、管理，对本单位关键信息基础设施安全负主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。

——关键信息基础设施安全保护工作部门：即所属行业或领域的国家行业主管或监管部门，负责指导和监督本行业、本领域的关键信息基础设施运行安全保护工作。

——关键信息基础设施安全保护其他参与者：与国家关键信息基础设施安全相关的其他组织。包括但不限于：关键信息基础设施网络安全保护相关部门、关键信息基础设施网络安全服务机构、研究机构、网络产品和服务提供者以及用户等。

关键信息基础设施网络安全保护中的相关角色应按我国法律法规和政策规定履行各自职责。

4.2 关键信息基础设施安全控制措施的分类

本标准在落实网络安全等级保护的基础上，参照GB/T AAAAA从风险识别、安全防护、检测评估、监测预警、应急处置五个环节，提出关键信息基础设施运营者应满足的安全控制措施。

——风险识别： 围绕关键信息基础设施承载的关键业务，识别关键信息基础设施的资产并分类，建立资产清单，标识重要系统和数据库；识别关键信息基础设施的威胁、脆弱性、已有安全措施，进行风险分析。

注：本环节与 GB/T AAAAA 的“识别认定”环节不同，后者还包括关键信息基础设施识别和认定活动，本标准针对已认定的关键信息基础设施，围绕关键信息基础设施承载的关键业务，开展风险识别。本环节是开展安全防护、检测评估、监测预警、应急处置等环节工作的基础。

——安全防护：根据已识别的安全风险，实施相应的安全控制措施，包括等级保护合规性要求、网络安全与信息化同步要求、网络安全责任制、个人信息和重要数据保护、数据境内存储与出境评估、人员与组织安全、人员安全审查、安全培训与考核、维护、供应链保护、重要系统和数据库的灾难备份等，确保关键信息基础设施的运行安全。

——检测评估：通过建立健全关键信息基础设施检测评估制度，自行或委托网络安全服务机构对其网络的安全性和可能存在的风险进行检测评估，并分析潜在安全风险可能引起的安全事件。

——监测预警：制定并实施网络安全监测预警和信息通报制度，建立信息共享渠道，分析监测结果，针对即将发生或正在发生的网络安全事件或威胁进行预警通报。

——应急处置：根据检测评估、监测预警环节发现的问题，制定并实施适当的应对措施，并恢复由于网络安全事件而受损的功能或服务，动态识别关键信息基础设施的安全风险。

5 风险识别

5.1 资产识别

5.1.1 资产清单

关键信息基础设施运营者应：

a）参照 GB/T 20984，围绕关键信息基础设施承载的关键业务，识别关键信息基础设施的资产并进行分类，包括数据、服务、信息系统、平台或支撑系统、基础设施、服务、人员管理等。

b）建立和维护关键信息基础设施的各类资产清单，明确资产的管理责任人。

c）将所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统，标识为重要系统，重要系统的容灾备份应符合 6.5.1 灾难备份策略相关规定。

d）使用符合法律法规要求的资产定位技术手段，例如端口监控或自动位置跟踪技术，监控并追踪受控区域内资产的位置和转移情况，以确保重要设备和核心组件位于所授权的区域内。

e）建立关键信息基础设施信息系统组件列表并满足以下要求：

1） 如存在组件属于其他组织，应予以注明并说明原因。

2） 当检测到非授权的组件时应禁止其网络访问，对其进行隔离并通知相关人员或角色。

3） 当信息系统更新或组件变更时，更新其信息系统组件清单。

5.1.2 数据分类

关键信息基础设施运营者应：

a）按照 GB/T BBBBB 附录 A“重要数据识别指南”，识别关键信息基础设施数字资产清单中的重要数据，重要数据的存储和传输应符合 6.4.2 境内存储和跨境传输相关规定。

b）将存储重要数据的数据库标识为重要数据库，重要数据库的容灾备份应符合 6.5.1 灾难备份策略相关规定。

c）参照数据分类相关标准规范，对数据进行分类并制定符合其安全需要的保护策略。例如，根据数据来源不同，分为系统数据、用户数据、运行数据；根据敏感程度和保护需求不同，可将用户数据分为用户身份数据、用户服务内容数据、用户服务衍生数据。

5.2 威胁识别

关键信息基础设施运营者应参照GB/T 20984中的威胁识别方法，识别关键信息基础设施面临的威胁，并对威胁动机、能力、频率进行赋值，判断威胁可能性。

5.3 脆弱性识别

关键信息基础设施运营者应：

a）参照GB/T 20984中的识别方法，以资产为核心，针对每一项需要保护的资产，识别可能被威胁利用的弱点。

b）使用脆弱性扫描工具和技术，定期对关键信息基础设施网络、信息系统及应用程序进行脆弱性扫描。

c）在本组织范围内与相关人员或角色共享脆弱性扫描和安全评估过程得到的信息，及时消除其他系统中的类似弱点。

d）确保所使用的脆弱性扫描工具具有迅速更新漏洞库的能力，在启动新的扫描前、新的漏洞信息发布后或定期更新漏洞库。

e）确保所使用的脆弱性扫描工具能够清楚呈现扫描所覆盖的广度和深度，如已扫描的信息系统组件和已核查的漏洞。

5.4 漏洞管理

关键信息基础设施运营者应：

a）使用漏洞管理工具，能够自动识别、记录、处理、更新安全漏洞相关信息，包括漏洞名称、位置、影响、处理情况、隐患等。

b）对发现的安全漏洞及时进行修补或评估可能的影响后进行修补，确保漏洞补丁经过测试后才可使用。

c）确保漏洞管理过程不影响业务连续性。

5.5 已有安全措施识别

参照 GB/T 20984，关键信息基础设施运营者应在识别脆弱性的同时，识别组织已有安全措施，并对已有安全措施的有效性进行确认。

5.6 风险分析

关键信息基础设施运营者应根据识别的资产、威胁和脆弱性，进行风险分析。

6 安全防护

6.1 等级保护合规要求

关键信息基础设施运营者应：

a）确定关键信息基础设施安全保护的定级对象及其安全保护等级；其中，定级对象包括网络基础设施、信息系统、大数据、云计算平台、物联网、工控系统等。

b）根据定级对象的安全保护等级，按照GB/T 22239相应等级的安全要求，进行安全建设、管理和运维，确保定级对象具有相应等级的安全保护能力。

c）在落实GB/T 22239相应等级的总体安全策略基础上，对关键信息基础设施实施分区分域管理，并根据承载业务的重要程度和数据敏感程度，制定不同的安全策略，避免重要网络、系统和资产遭受未经授权的访问，防止重要数据泄露或者被窃取、篡改。

6.2 网络安全与信息化同步要求

6.2.1 同步规划

关键信息基础设施运营者应：

a）同步分析安全需求，即在关键信息基础设施建设或改建之初，从本组织的职能或业务的角度分析对关键信息基础设施实施网络安全的需求，形成安全需求说明书。

b）同步定义安全要求，即基于网络安全需求说明书，定义关键信息基础设施的网络安全要求，形成网络安全功能和性能说明书。

c）确保安全需求说明书得到网络安全责任部门签字认可。

6.2.2 同步建设

关键信息基础设施运营者应：

a）同步设计安全体系结构，即基于已经定义的关键信息基础设施的网络安全要求，设计网络安全体系结构，明确系统内的各类信息安全组件，说明各组件提供的信息安全服务及可能的实现机制。

b）同步开展详细的安全设计，即根据安全保护等级选择基本安全措施，细化安全机制在关键信息基础设施中的具体实现。

c）在建设或改建过程中，按照GB/T 22239工程实施相应等级的要求，同步建设符合其等级要求的网络安全设施，包括自行软件开发。

d）建设完成后，组织对关键信息基础设施进行验收并将网络安全作为验收的重要内容。

6.2.3 同步使用

关键信息基础设施运营者应：

a）同步运行安全设施，确保安全设施保持启用状态。

b）按照GB/T 22239安全运维管理相应等级的要求进行安全运维。

c）关键信息基础设施及其运行环境发生明显变化时，评估其风险，及时升级安全设施并实施变更管理。

d）对安全设施同步实施配置管理，包括制定配置管理计划，制定、记录、维护基线配置，保留基线配置的历史版本，便于必要时恢复历史配置。

e）在废弃安全设施时，采取以下措施，保护被废弃的安全设施中存储信息的安全：

1）妥善保存或采用安全方式处置介质。

2）对含有特别重要的敏感信息或涉密信息的重要介质，选择有资质的机构进行安全销毁。

3）对敏感组件或信息的处置保留详细记录。

f）如需要建设新的安全设施承接原有功能，应确保业务平稳、安全迁移，在新安全设施建设完成、通过验收并正式上线前，不得关闭原有安全设施。

6.3 网络安全责任制

6.3.1 责任主体

关键信息基础设施运营者应：

a）对本组织关键信息基础设施的安全承担主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。

b）明确主要负责人是本组织关键信息基础设施安全保护工作第一责任人，负责建立健全网络安全责任制并组织落实，对本组织关键信息基础设施安全保护工作全面负责。

6.3.2 岗位风险与职责

关键信息基础设施运营者应：

a）标识出所有岗位的风险。

b）定期评审和更新各岗位的风险标识。

c）根据岗位风险，明确所有岗位的网络安全职责。

d）标识关键岗位与关键职责，包括与重要系统直接相关的系统管理、网络管理、重要应用开发、系统维护、重要业务操作等岗位与职责。

6.3.3 职责分离

关键信息基础设施运营者应遵循职责分离原则进行访问授权，包括：

a）对关键职责进行分离，通过访问控制措施予以落实。

b）分离冲突的职责及其责任范围，以减少未经授权或无意的不当使用行为。例如，安全人员能够管理访问控制功能，但不能管理审计功能。

c）划分业务功能和信息系统支持功能，由不同的个人或角色执行信息系统支持功能，如系统管理、系统程序设计、配置管理、质量保证和测试、网络安全等功能。

6.3.4 最小特权

关键信息基础设施运营者应：

a）确保为用户提供的访问权限是其完成指定任务所必需的，且符合本组织的业务需求。

b）将特权功能的执行纳入信息系统需要审计的事件中。

c）确保信息系统能够阻止非特权用户执行特权功能，以防禁止、绕过或替代已实施的安全措施。

d）对于可能超越系统和应用控制的实用程序的使用予以限制并严格控制。

6.4 数据保护

6.4.1 个人信息保护

关键信息基础设施运营者应建立规范的个人信息保护制度，确保个人信息的收集、存储、使用、传输、披露符合GB/T 35273，并满足以下要求：

a）明确告知收集个人信息的目的、用途、范围和类型，在个人明示同意后，方可收集。

b）只收集实现功能所需的最少个人信息，收集的个人信息仅用于个人同意的目的和用途。

c）未经个人明示同意，不得向他人提供个人信息，经处理无法识别特定个人且不能复原的除外。

d）向个人信息主体提供查询、更正个人信息的功能.当发现提供者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，个人有权要求提供者删除其个人信息。

e）确保公开或对外披露的个人信息和重要数据范围，不超出法律、行政法规规定和与个人约定的范围。

f）建立个人信息安全事件的投诉和举报机制，并能够提供相关证明材料。

6.4.2 境内存储与出境评估

关键信息基础设施运营者：

a）应确保境内运营中收集和产生的个人信息和重要数据在境内存储。

b）应采取措施保护个人信息和重要数据的安全，防止信息泄露、篡改、损毁、丢失，安全措施可包括数据分类分级、数据备份、加密存储、加密认证和安全审计等。

c）因业务需要，确需向境外提供的，在数据出境前，应自行组织或报请行业主管或监管部门，按照个人信息和重要数据出境安全评估办法等相关规定和标准进行安全评估，并对评估结果负责。

d）按照GB/T BBBBB重点评估以下内容：必要性；涉及个人信息情况；涉及重要数据情况；数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；数据出境及再转移后被泄露、毁损、篡改、滥用等风险；以及可能对国家安全、社会公共利益、个人合法利益带来的风险等。

e）经评估安全风险高的不应向境外传输，法律、行政法规另有规定的，依照其规定。

f）针对个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。

g）根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，及时将评估情况报关键信息基础设施行业主管或监管部门。

6.5 灾难备份

6.5.1 灾难备份策略

关键信息基础设施运营者应：

a）确定灾难备份目标，制定灾难备份策略，根据系统重要性、业务特点、建设成本等因素选择合适的灾难备份机制。

b）根据灾难备份策略制定相应的灾难备份系统技术方案，包含数据备份系统、备用数据处理系统和备用的网络系统。

c）按照GB/T 20988中三级及以上灾难恢复能力的要求，对重要系统和数据库进行容灾备份，实现完全数据备份至少每天一次，至少每天多次利用通信网络将关键数据定时批量传送至备用场地；根据业务特点，数据更新快、完整性要求高的重要数据库，应满足GB/T 20988中的5级灾难恢复能力的要求，实现实时数据传输及完整设备支持。

6.5.2 灾难备份中心选址和建设

关键信息基础设施运营者应

a）按照GB/T 20988，选择灾难备份中心，避免灾难备份中心与主中心同时遭受同类风险，包括同城和异地两种类型，以规避不同影响范围的灾难风险。

b）建设灾难备份中心，计算机机房应符合有关国家标准的要求,工作辅助设施和生活设施应符合灾难恢复目标的要求。

c）确保为灾难备份中心提供与主场所同等的网络安全措施。

d）确保灾难备份中心位于中国境内。

e）控制灾难备份中心位置信息的知悉范围。

6.5.3 业务连续性

关键信息基础设施运营者应：

a）制定并实施业务连续性计划，确保关键信息基础设施对本组织职能和业务的核心支撑能力在重大信息安全事件中不受到明显影响，支持业务稳定、持续运行。

b）设置重要系统和数据处理设施冗余，满足系统可用性要求。

c）确保必要时关键信息基础设施有能力应用备用通信协议以保障业务连续性。

d）将网络安全连续性纳入业务连续性管理之中，确保在不利情况下网络安全连续性达到要求的级别。

6.6 人员与组织安全

6.6.1 安全组织

关键信息基础设施运营者应：

a）建立网络安全管理框架，设立专门的网络安全管理机构，负责健全完善网络安全管理制度，落实网络安全防护措施。

b）由本组织的主要领导担任安全管理负责人。

c）确保安全人员规模不能少于信息化人员的20%。

d）做好与本组织其他业务部门的协调，保持应急响应、信息通报等外部机构的沟通。

e）实施内部威胁防范程序，包括跨部门的内部威胁事件处理团队。

6.6.2 人员安全审查

关键信息基础设施运营者应：

a）确保安全管理负责人和关键岗位的人员上岗前、必要时或定期（如至少每年一次），实施人员安全背景审查，审查通过才可从事相关岗位工作。

b）制定人员安全审查准则，包括公民身份和国籍、政治审查、宗教信仰、从业经历、教育背景、犯罪记录、个人信用、家庭情况以及海外关系等。

c）通过访谈、调查问卷的方式自行审查，或委托第三方调查机构进行审查。

d）对调查问卷的真实性进行核对并备案，当国籍、家庭情况等发生变化时应及时更新，并根据情况重新组织安全审查。

6.6.3 人员筛选

关键信息基础设施运营者应：

a）确保授权访问关键信息基础设施的人员已经经过筛选，人员信息和筛选结果应可供关键信息基础设施安全保护工作部门查阅。

b）在需要时或定期对授权访问人员进行再筛选。

c）与授权访问关键信息基础设施的人员签订保密协议。

d）与关键岗位人员签署岗位责任协议。

e）参照国家相关规定，实行网络安全关键岗位专业技术人员执证上岗制度。

6.6.4 人员离职

关键信息基础设施运营者一旦决定终止与某位人员的雇佣关系，应：

a）在一定期限内，终止或撤销与该人员相关的任何访问权限、身份鉴别物或凭证。

b）与该人员进行离职面谈，包括商讨网络安全事宜，承诺离职后的保密义务。

c）收回该人员所有涉及安全的本组织相关资产。

d）确保之前由该人员控制的信息系统和数据仍然可用。

e）在一定期限内，通知相关人员或角色。

6.6.5 人员调动

关键信息基础设施运营者应：

a）在人员被再分配或调动至其他内部岗位时，评估是否保留其对关键信息基础设施的逻辑和物理访问权限。

b）根据评估结果，修改访问授权。

c）在一定期限内，通知相关人员或角色。

6.6.6 第三方人员安全

关键信息基础设施运营者应：

a）为第三方供应商（如服务组织、合同商、信息系统开发商、外部应用提供商）建立人员安全要求，包括安全角色和责任。

b）要求第三方供应商在一定期限内，将拥有本组织凭证或系统访问权限的第三方人员的任何调动或离职情况通知特定人员或角色；及时修改或收回第三方人员的访问权限、凭证和使用的本组织资产，确保之前由该人员控制的信息系统和数据仍然可用。

6.7 培训

6.7.1 培训制度

关键信息基础设施运营者应：

a）建立网络安全意识教育和培训制度，为关键信息基础设施从业人员及其他有关人员（如合同商、用户等）提供安全意识教育和基础安全培训，为承担安全角色和职责的人员提供基于角色的安全技能培训。

b）将安全意识教育和基础安全培训作为关键信息基础设施从业人员入职培训的一部分，以及系统发生重要变更时或定期为关键信息基础设施从业人员及其他有关人员（如合同商、用户等）提供基础的安全意识教育和安全培训。

c）承担安全角色和职责的人员在获得访问授权或执行职责之前，以及系统发生重要变更时或定期为其提供基于角色的安全技能培训。

d）确保关键信息基础设施从业人员每年参加一次网络安全培训，时长不少于1个工作日，网络安全关键岗位从业人员的年度培训时长不少于3个工作日。

6.7.2 培训对象

关键信息基础设施运营者应针对关键信息基础设施从业人员，做到全员安全意识教育、全员培训和全员考核。从业人员不仅限于网络安全岗位上的专业人员，还包括其他与关键信息基础设施运营安全相关的管理人员、操作人员、使用人员、服务人员等。

6.7.3 培训内容

关键信息基础设施运营者应针对不同岗位制定不同的培训计划，确定或编制配套培训教材。培训内容应包括网络安全相关制度和规定、网络安全基础知识、网络安全保护技术、网络安全风险意识、岗位操作规程，以及相关的安全责任和惩戒措施。

6.7.4 技能考核

关键信息基础设施运营者应定期开展网络安全技能考核，及时记录并保存培训和考核情况，作为从业人员综合评价的一部分。

6.8 维护

6.8.1 受控维护

关键信息基础设施运营者应：

a）审批和监视维护行为，包括现场维护、远程维护，以及对设备的异地维护。

b）在将关键信息基础设施设备转移到关键信息基础设施运营者外部进行非现场的维护或维修前，获得相关人员或角色的批准，并对设备进行净化，清除介质中的信息。

c）在对关键信息基础设施设备、网络和信息系统进行维护后，检查可能受影响的安全措施，以确认其仍正常发挥功能。

d）确保维护记录至少包括：维护日期和时间、维护人员姓名、陪同人员姓名、对维护活动的描述、被转移或替换的设备列表（包括设备标识号）等信息。

6.8.2 维护工具

关键信息基础设施运营者应：

a）审核并监视维护工具的使用。

b）检查由维护人员带入关键信息基础设施内部的维护工具，以确保维护工具未被不当修改。

c）在使用诊断或测试程序前，对其进行恶意代码检测。

d）为防止具有信息存储功能的维护设备在未授权情况下被转移出关键信息基础设施运营者的控制范围，采取以下一种或多种措施，并获得安全责任部门的批准：

1）确认待转移设备中没有关键信息基础设施运营者的信息。

2）净化或销毁设备。

3）将设备留在场所内部，规定不得移出。

6.8.3 远程维护

关键信息基础设施运营者应在境内实施关键信息基础设施的运行维护，因业务需要确需进行境外远程维护的，应满足以下要求：

a）按照法律法规要求，事先将远程维护机制报关键信息基础设施安全保护工作部门备案，报备内容应包括远程维护策略、规程以及使用的远程维护工具等。

b）采用自动化方式对远程维护活动进行管理、控制和审计。

c）限制远程维护访问权限，根据情况仅允许使用适当的维护策略和工具。

d）在建立远程维护会话时采取强鉴别技术。

e）在远程维护完成后终止会话。

f）形成远程维护日志，日志留存不少于12个月。

g）定期对远程维护日志进行审查。

6.8.4 维护人员

关键信息基础设施运营者应：

a）建立对维护人员的授权流程，对已获授权的人员建立列表。

b）确保只有列表中的维护人员，才可在没有人员陪同时进行系统维护；不在列表中的人员，必须在授权且技术可胜任的人员陪同与监管下，才可开展维护活动。

6.8.5 及时维护

关键信息基础设施运营者应建立系统组件的备品备件列表，确保备品备件能够在发生故障的一定时间段内投入运行。

6.9 供应链保护

6.9.1 选择网络产品和服务

关键信息基础设施运营者应：

a）在选择、安装或更新网络产品和服务前对其进行评估，确保使用的网络产品和服务满足 GB/T CCCCC 等相关国家标准要求。

b）对于可能影响国家安全的网络产品和服务，采购时宜确保其按照网络产品和服务安全审查办法的要求通过网络安全审查，不应采购审查未通过的网络产品和服务。产品和服务是否影响国家安全由关键信息基础设施安全保护工作部门确定。

c）列入《网络关键设备和网络安全专用产品目录》的设备和产品，确保其按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可采购。

6.9.2 选择网络产品和服务供应商

关键信息基础设施运营者应：

a）与网络产品和服务供应商签订以下协议：

1）安全保密协议，明确采购及后续合作过程中有关网络安全保密事项；

2）供应商协议，明确产品和服务供应链相关的网络安全风险处理要求；

3）服务水平协议（SLA），明确服务水平不低于关键信息基础设施拟对外提供的服务水平。

b）优先选择符合下列条件的供应商：

1）保护措施符合法律法规、政策标准以及关键信息基础设施运营者的安全要求；

2）企业运转过程和安全措施相对透明；

3）对下级供应商、关键组件和服务的安全提供了进一步的核查；

4）在合同中声明不使用有恶意代码产品或假冒产品。

5）筛选外包服务开发商和开发人员，人员筛选的准则包括：无过失、可靠或称职的官方证明、良好的背景审查、公民身份和国籍。

c）在签署合同前对供应商进行评估，根据实际情况，包括但不限于：

1）分析供应商对网络产品和服务的设计、开发、实施、验证、交付、支持过程；

2）评价供应商在开发网络产品和服务时接受的安全培训和积累的经验，以判断其安全能力。

d）综合分析各方面的信息，包括执法部门披露的信息、网络安全通报、应急响应机构的风险提示等，以发现来自开发、生产、交付过程以及人员和环境的风险。该分析应尽可能覆盖到各层供应商和候选供应商。

e）发现使用的网络产品、服务存在安全缺陷、漏洞等风险时，及时联系供应商，采取措施消除风险隐患，对存有重大风险的网络产品、服务，按相关规定报告关键信息基础设施安全保护工作部门。

6.9.3 供应链保护措施

关键信息基础设施运营者应：

a）采用措施保护供应链相关信息，包括用户身份、网络产品和服务的用途、供应商身份、安全需求、设计说明书、测评结果、信息系统或组件配置等。

b）采取保护措施，降低攻击者利用供应链造成的危害，包括：

1）优先购买现货产品，避免购买定制设备。

2）在能提供相同产品的多个不同供应商中做选择，以防范供应商锁定风险。

3）选择有声誉的企业，建立合格供应商列表。

4）储备足够的备用组件。

5）缩短采购决定和交付的时间间隔。

6）使用可信或可控的分发、交付和仓储手段。

7）在运输或仓储时使用防篡改包装。

c）定期检查、评审和审核供应商的服务交付。

7 检测评估

7.1 自评估

关键信息基础设施运营者应：

a）参照GB/T DDDDD要求，自行或者委托网络安全服务机构对其安全性和可能存在的风险每年至少进行一次安全评估。

b）从合规检查、技术检测和分析评估三个主要环节进行安全评估。

c）自行或者委托网络安全服务机构开展风险评估。

d）确保检测内容包括但不限于网络安全制度落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、安全防护情况、风险评估情况、应急演练情况、网络安全等级保护工作落实情况等。

e）根据安全评估情况，有针对性地对关键信息基础设施进行安全整改，将风险降低到可接受的水平。

f）参照GB/T DDDDD附录A，编制检测评估报告，报告包括如下基本内容：

1）检查对象基本情况描述，包含关键信息基础设施的定义描述、主要核心资产情况、核心业务情况、面临的主要威胁和系统安全能力的描述情况等。

2）检查评估结果说明，对检查评估中发现的关键信息基础设施存在的主要问题进行分析说明。

g）将检测评估报告及时上报对应的关键基础设施安全保护工作部门。

7.2 安全检测

新建、改建或扩建的关键信息基础设施，所属行业或领域的安全保护工作部门有相关要求的，关键信息基础设施运营者应通过关键信息基础设施安全保护工作部门认可的网络安全服务机构进行检测评估，在对检测评估发现的安全问题进行有效整改后方可上线。

7.3 安全抽查

关键信息基础设施运营者应积极配合关键信息基础设施安全保护工作部门组织开展的关键信息基础设施的安全风险抽查检测工作，提供网络安全管理制度、网络拓扑图、重要资产清单、关键业务介绍等必要的资料和技术支持，针对抽查检测工作中发现的安全问题和风险进行及时整改。

8 监测预警

8.1 安全监测

8.1.1 监测预警制度

关键信息基础设施运营者应：

a）根据国家行业主管或监管部门关键信息基础设施网络安全监测预警制度的要求，按照国家网络安全事件应急预案等规定，建立并完善本组织监测预警制度，提高监测能力，自主监测涉及本组织管理范围内的信息。

b）确定监测对象、监测指标、监测频率，监测对象包括系统运行状态、网络、人员行为、物理环境和策略运行效果等。

c）监测关键信息基础设施运行、操作、故障维护等行为，并留存相关日志，尤其要对远程运维的行为进行严格的管理、控制和审计，相关的系统、网络设备日志留存不少于12个月。日志内容应至少包括：事件的日期和时间、类型、主体、客体、结果等信息。

d）定期对监测情况进行安全评估，向相关人员或角色报告关键信息基础设施安全状态。

8.1.2 信息系统监测

关键信息基础设施运营者应：

a）能够发现攻击行为，使用自动工具对攻击事件进行准实时分析。

b）能够发现非授权的本地、网络和远程连接以及对信息系统的非授权使用；

c）确保信息系统监测活动符合关于隐私保护的相关政策法规。

d）以下迹象发生时，应向相关人员或角色发出警报：

1）受保护的信息系统文件或目录在未得到正常通知的情况下被修改。

2）当发生异常资源消耗时。

3）审计功能被禁止或修改，导致审计可见性降低。

4）审计或日志记录因不明原因被删除或修改。

5）预期之外的用户发起了资源或服务请求。
6）信息系统报告了管理员或关键服务账号的登录失败或口令变更情况。
7）进程或服务的运行方式与系统常规情况不符。
8）在生产系统上保存或安装与业务无关的程序、工具、脚本。

8.1.3 物理访问监测

关键信息基础设施运营者应：
a）对信息系统设施进行物理访问监测，形成物理访问日志。
b）定期或当安全事件发生时，对物理访问日志进行审查。
c）安装物理入侵警报装置，对物理入侵警报装置和监测设备进行监视。
d）对于集中部署了大量信息系统组件的区域（如服务器机房、通讯中心），除了对设施实施访问监测外，对信息系统实施单独的物理访问监测。

8.1.4 信息泄露监测

关键信息基础设施运营者应对公开来源的网站信息（如社交网站信息）进行监测，以确定组织信息是否已被未经授权的方式披露。

8.1.5 恶意代码检测

关键信息基础设施运营者应：
a）采用白名单、黑名单或其他方式，在网络出入口以及系统中的主机、移动计算设备上实施恶意代码防护机制。
b）配置恶意代码防护机制，定期扫描信息系统，以及在终端或网络出入口下载、打开、执行外部文件时对其进行实时扫描。
c）当检测到恶意代码后，阻断或隔离恶意代码、向管理员报警或采取其他举措。
d）及时掌握系统的恶意代码误报率，并分析误报对信息系统可用性的潜在影响。
e）在系统的出入口和网络中的工作站、服务器或移动计算设备上部署垃圾信息检测与防护机制，以检测并应对电子邮件、电子邮件附件、web访问或其他渠道的垃圾信息。
f）确保恶意代码和垃圾信息防护机制得到及时更新，如升级病毒库。

8.2 信息通报

8.2.1 信息通报制度

关键信息基础设施运营者应根据国家行业主管或监管部门关键信息基础设施网络安全信息通报制度的要求，按照国家网络安全事件应急预案等规定，制定并完善本组织信息通报制度，包括：
a）明确负责信息通报工作的主管领导和承担信息通报工作的责任部门、负责人和联络人。
b）及时汇总本组织内部不同部门、不同渠道掌握的网络安全信息。
c）明确本组织信息报送项目。
d）规范报送信息内容和形式，信息包括事件信息和预警信息，其中：
1）事件信息指已经发生的网络安全事件信息，事件信息通报内容主要包括事件统计情况、造成的危害、影响程度、态势分析、典型案例等。
2）预警信息是指存在潜在安全威胁或隐患但尚未造成实际危害和影响的信息，或者对事件信息分析后得出的预防性信息，预警信息通报内容主要包括事件类别、预警级别、可能的受影响系统、可能产生的危害和危害程度、可能影响的范围、建议应采取的应对措施及建议等。

e）明确具体分级标准，将预警信息分为四级，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

8.2.2 预警信息接收

关键信息基础设施运营者应以适当的方式参与本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度，持续接收行业主管或监管部门发布的安全风险、预警信息和应急防范措施建议。

8.2.3 预警研判和通报

关键信息基础设施运营者应：

a）对监测信息进行研判，必要时发出内部的安全预警信息并提出适当的处置建议。

b）根据本组织信息通报制度要求，向相关人员、角色和部门通报安全预警信息和建议。

c）及时响应安全预警信息和建议，如无法响应应说明原因。

8.2.4 信息共享

关键信息基础设施运营者应：

a）按照关键信息基础设施安全保护工作部门要求，建立与有关部门、研究机构、网络安全服务机构的信息共享渠道，接收行业主管或监管部门发布的安全风险、预警信息和应急防范措施建议。

b）建立本组织的信息共享和分析中心，收集网络威胁迹象信息或防护措施并进行分析，必要时与行业网络安全威胁信息共享平台进行对接。

c）对共享或接收网络威胁迹象信息或防护措施进行授权。

e）在监控信息系统、实施防护措施、提供或接收网络威胁迹象信息和防护措施时，应实施安全控制，以保护上述网络威胁迹象信息或防护措施免受未授权访问或获取。

d）在信息共享前，使用技术手段直接删除与网络安全威胁无直接关系的、共享时已知晓是具体人员个人信息或能够用于识别具体人员的信息。

f）限制信息使用目的，对威胁信息的披露、留存与使用仅用于网络安全保护目的。

9 应急处置

9.1 计划

9.1.1 网络安全事件应急预案

关键信息基础设施运营者应：

a）依据本部门、本行业的网络安全事件应急预案，制定组织的网络安全事件应急预案，该应急预案应：

1）说明组织机构与职责。

2）确立组织范围内的预警监测、预警研判和发布、预警响应、预警解除等流程。

3）对事件报告、应急响应、应急结束等程序作出规定。

4）对事件调查、评估等事项作出安排。

5）对预案演练、宣传、培训等工作进行规划。

6）落实技术支撑队伍、专家队伍、社会资源、经费等保障措施。

b）由相关人员或角色对网络安全事件应急预案进行评估。

c）将网络安全事件应急预案向相关人员、角色或部门进行通报。

d）定期评估修订网络安全事件应急预案；当本组织的管理架构、信息系统或运行环境发生变更时，及时更新网络安全事件应急预案。

e）如系统发生变更或在实施、执行或测试中遇到问题，及时修改网络安全事件应急预案并向相关人员、角色或部门及用户进行通报。

f）防止网络安全事件应急预案非授权泄露和更改。

g）在发生安全事件时，确保应急响应计划的实施能够维持信息系统的基本业务功能，并能最终完全恢复信息系统且不减弱原来的安全措施。

h）指定专门的网络安全应急支撑队伍、专家队伍，保障网络安全事件得到及时有效处置。

9.1.2 灾难恢复计划

关键信息基础设施运营者应按照GB/T 20988等标准，制定灾难恢复计划，确保关键信息基础设施能及时从网络安全事件中恢复。

9.2 培训和演练

9.2.1 应急培训

关键信息基础设施运营者应：

a）向相关人员或角色提供应急响应培训。

b）当信息系统变更时，或定期重新开展培训。

9.2.2 应急演练

关键信息基础设施运营者应：

a）至少每年制定或修订应急演练计划。

b）至少每年执行应急演练计划，并且至少在演练开始前通知用户和相关部门。

c）与关键信息基础设施安全保护工作部门和其他有关部门（如应急响应组织）进行沟通协调，为应急演练提供保障条件。

d）记录和核查应急演练结果，并根据需要修正应急响应计划。

e）保存演练记录、演练总结报告等。

f）将信息系统备份能力列入应急演练计划，包括检验备份的可靠性和信息完整性。

g）在替代的处理场所演练应急计划，使应急人员熟悉设施和可用的资源，以评价该场所支持应急运行的能力。

h）将全面恢复和重构信息系统到已知状态作为应急演练计划的一部分。

9.2.3 事件演练

关键信息基础设施运营者应：

a）至少每年制定或修订事件演练计划。

b）定期测试或演练信息系统事件处置的能力，以确定事件响应的有效性并记录测试或演练结果。

9.3 处置

9.3.1 事件管理

关键信息基础设施运营者应：

a）要求使用组织信息系统和服务的员工和合同方注意并报告任何观察到的或可疑的系统或服务中的网络安全弱点。

c）评估网络安全事态，判断其是否属于网络安全事件。

d）确定和应用规程来识别、收集、获取和保存可用作证据的信息。

9.3.2 事件报告

关键信息基础设施运营者应：

a）当发现可疑的安全事件时，及时向本组织的事件处理部门报告。

b）建立事件报告渠道，当发生影响较大的安全事件时，按规定及时将事件信息报送关键信息基础设施安全保护工作部门，内容应至少包括：事件描述、处置措施、当前态势、需要的外部支持等信息。

c）使用自动机制支持事件报告过程。

9.3.3 事件处置

关键信息基础设施运营者应：

a）在事件发生后立即启动应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

b）为事件处置提供必需的资源和管理支持。

c）协调应急响应活动与事件处理活动，并与相关外部组织（如供应链中的外部服务提供商等）进行协调。

d）将当前事件处理活动的经验，纳入事件处理、培训及演练计划，并实施相应的变更。

9.3.4 处置支持

关键信息基础设施运营者应：

a）落实事件处理所需的各类资源，为用户处理、报告安全事件提供咨询和帮助。

b）使用自动机制，为事件处理提供进一步的资源支持。

c）在事件处理部门和外部的网络安全组织之间建立直接合作关系，能够在必要时获得外部组织的协助。

9.3.5 信息系统恢复和重构

关键信息基础设施运营者应：

a）在关键信息基础设施信息系统遭到破坏或发生故障后，及时恢复信息系统业务功能。

b）系统恢复后能够对信息系统进行重构，包括使信息系统回到已知的全面运行状态，还包括停用在恢复操作期间任何可能需要的临时信息系统功能，评估完全恢复的信息系统能力，重新建立连续的监测活动。必要情况下，对信息系统重新授权，以及为防止未来的中断或失败而准备系统。

c）为信息系统中基于事务的系统（如数据库管理系统和事务处理系统等）执行事务恢复，包括事务回滚、事务日志等。

d）在指定的恢复时间内根据受控配置和代表部件安全运行状态的完整性得到保护的磁盘映像重构信息系统部件的功能。

9.4 改进

9.4.1 事件总结

关键信息基础设施运营者应在事件处置完成后3日内向安全保护工作部门书面报告事件情况，内容应至少包括：事件描述、原因和影响分析、处置方式等信息。

9.4.2 事件溯源

关键信息基础设施运营者应具备一定的事件溯源能力，能够为关键信息基础设施安全保护工作部门和执法机构提供可靠的日志，包括网络访问日志、物理访问日志、审计日志等，日志内容应至少包括访问URL、IP地址、操作时间等信息。

9.4.3 事件学习

关键信息基础设施运营者应利用在分析和解决网络安全事件中得到的知识来减少未来事件发生的可能性和影响。

9.4.4 事件配合

关键信息基础设施运营者应积极参与和配合国家网信部门、监管部门和保护工作部门展开的网络安全应急演练、应急处置、信息共享等。

参考文献

[1] NIST Special Publication 800-53 联邦信息系统和组织的安全和隐私控制
[2] NIST 增强关键基础设施网络安全的框架
[3]《国家网络安全事件应急预案》
[4]《关键信息基础设施安全保护条例（征求意见稿）》
[5]《网络关键设备和网络安全专用产品目录（第一批）》