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：2019-4-12)

XXXX - XX - XX 发布　　XXXX - XX - 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。

本标准起草单位：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、公安部第三研究所、公安部第一研究所、国家信息中心、国家工业信息安全发展研究中心、国家互联网应急中心、国家信息技术安全研究中心、中国信息安全测评中心等。

本标准主要起草人：

引　　言

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。

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、事件处置等环节应实施的安全控制措施，以满足关键信息基础设施网络安全保护的基本要求。

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 20984-2007 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 网络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/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

GB/T 32924-2016 信息安全技术 网络安全预警指南

GB/T 36635-2018 信息安全技术 网络安全监测基本要求与实施指南

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 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

为保护关键信息基础设施及其信息的保密性、完整性和可用性等，在管理、运行和技术等方面的防护措施和和对抗措施。

4 概述

4.1 关键信息基础设施保护相关角色和职责

本标准所指的关键信息基础设施包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统、工业控制系统等，其一旦遭到破坏、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。

关键信息基础设施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

本标准参照GB/T AAAAA从风险识别、安全防护、检测评估、监测预警、事件处置五个环节，根据关键信息基础设施的基本要求提出相应的控制措施。关键信息基础设施运营者应在满足网络安全等级保护GB/T 22239相应级别要求的基础上，围绕安全风险管理，根据自身具体情况和识别的安全风险，选择应采取的安全控制措施，确保将安全风险控制在可接受的范围。

——风险识别：围绕关键信息基础设施承载的关键业务，开展风险识别，包括识别资产、威胁、脆弱性、已有安全措施，进行风险分析。风险识别是开展安全防护、检测评估、监测预警、事件处置等工作的基础。

——安全防护：根据已识别的安全风险，实施安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运维管理等方面的安全控制措施，确保关键信息基础设施的运行安全。本环节在认定关键信息基础设施及识别其安全风险的基础上制定安全防护措施。

——检测评估：为检验安全防护措施的有效性，发现网络安全风险隐患，建立健全关键信息基础设施检测评估制度，确定检测评估的流程及内容等要素，分析潜在安全风险并进行整改。

——监测预警：制定并实施网络安全监测预警和信息通报制度，针对即将发生或正在发生的网络安全事件或威胁，提前或及时进行预警通报。

——事件处置：根据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。

5 风险识别

5.1 业务识别

5.1.1 关键业务识别

关键信息基础设施运营者应：

a）识别本组织的关键业务和关键业务所依赖的外部关键业务。

b）当关键业务为外部关键业务提供服务时，识别本组织关键业务对外部关键业务的重要性。

c）建立关键业务链。

5.1.2 关键信息基础设施边界识别

关键信息基础设施运营者应：

a）基于关键业务链，识别关键业务链所需的信息流，主要考虑以下因素：

1）该信息流足以保障关键业务按照预设功能运行。

2）该信息流一旦中断或者发生信息泄露，给关键业务造成严重影响。

b）基于信息流，识别关键信息基础设施的最大可能边界，即涉及的所有网络设施、信息系统。

c）开展关键性评估，调整关键信息基础设施的边界范围，并重新评估至确定边界，评估主要考虑以下因素：

1）网络设施、信息系统等对关键业务的重要程度。

2）网络设施、信息系统等一旦遭到破坏后可能带来的危害程度。

3）对其他组织关键业务的关联性影响。

d）明确本组织的关键信息基础设施分布和运营情况。

5.2 资产识别

5.2.1 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）当关键信息基础设施发生改建、扩建等重大变化时，例如网络拓扑、业务链改变等，重新开展识别工作，并更新资产清单。

c）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。

d）建立数据分类分级制度，对关键信息基础设施承载的数据进行分类分级。

e）参照国家有关要求，识别与国家安全、经济发展以及社会公共利益密切相关的重要数据。

f）基于资产类别、资产本身的重要性以及资产所支撑的业务的重要性，对资产进行优先排序，确定资产防护的优先级。

5.2.2 资产自动管理

关键信息基础设施运营者应能够采用自动化方式进行资产管理，包括：

a）根据关键业务链所依赖资产的实际变化等，自动更新资产清单。

b）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。

c）通过配置管理数据库（CMDB）等方式，实现数据库自动管理。

d）能够使用自动机制识别关键信息基础设施信息系统中新增的非授权软件、硬件或固件组件。

5.3 风险分析

关键信息基础设施运营者应参照 GB/T 20984，围绕关键业务链进行以下活动：

a）识别关键业务链面临的威胁，判断威胁可能性。

b）实施脆弱性扫描，确保所使用的脆弱性扫描工具能对扫描结果生成报告，对发现的漏洞提供修复建议，并及时更新漏洞库，如在实施扫描之前、在新的漏洞信息发布之后。

c）识别组织已有的安全措施，并对已有安全措施的有效性进行确认。

d）根据识别的关键业务链资产、威胁、脆弱性和已有安全措施，进行风险分析。

e）根据业务重要性和风险严重程度，确定关键信息基础设施风险处置的优先级。

5.4 重大变更

当关键信息基础设施发生改建、扩建等重大变更有可能影响认定结果时，关键信息基础设施运营者应当重新开展识别工作，并更新资产清单，及时将相关情况报告保护工作部门，按规定进行重新认定。其中，重大变更的情形包括但不限于：

a）网络拓扑发生重大变化。

b）关键业务链发生变化或关键业务的重要性发生变化。

c）业务服务范围发生重大变化。

6 安全防护

6.1 安全管理制度

关键信息基础设施运营者应：

a）阐明安全保护的总体目标、范围、原则和安全框架等，框架可包括管理机构、管理人员、通信网络、计算环境、建设管理、运维管理等方面。

b）基于已识别的风险和资产以及关键业务链、供应链等安全需求，明确安全防护策略。

c）对安全管理活动中的各类管理内容建立安全管理制度。

d）对管理人员或操作人员执行的日常管理操作建立操作规程。

e）形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

f）指定或授权专门的部门或人员负责安全管理制度的制定。

g）至少每年或发生重大变化时，检查和更新安全策略、安全制度以及相关规程文件。

6.2 安全管理机构

关键信息基础设施运营者应：

a）建立针对关键信息基础设施指导和管理网络安全工作的委员会或领导小组，由本组织的第一责任人担任其最高领导。

b）设置专门的网络安全管理机构，包括：

1）将组织的网络安全职责从信息化职责中剥离出来。

2）配备专职网络安全管理人员，不可兼任。

3）建立健全完善网络安全管理制度，监督落实网络安全防护措施。

c）做好关键岗位的网络安全管理，包括：

1）标识关键岗位，包括与重要系统直接相关的系统管理、网络管理、安全管理等岗位。

2）明确关键岗位的网络安全职责。

3）由专人负责关键岗位，并配备2人以上共同管理。

d）建立并实施网络安全考核及监督问责机制，包括：

1）明确网络安全考核目的、内容、方式等。

2）明确网络安全问责对象、问责对象的责任界定和处罚措施等。

6.3 安全管理人员

6.3.1 人员审查

关键信息基础设施运营者应：

a）在以下情形时对安全管理负责人和关键岗位的人员实施人员安全背景审查，审查通过才可从事相关岗位工作，包括：

1）上岗前。

2）人员的身份、安全背景等发生变化时。

3）岗位发生重大变化或其他必要情况下。

4）至少每年一次。

b）制定关键岗位的人员安全审查准则，如国籍、政治背景、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、调查问卷等方式自行审查，或委托第三方调查机构审查。

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。

6.3.2 人员筛选

关键信息基础设施运营者应：

a）对授权访问关键信息基础设施的人员（包含外部人员）进行筛选，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）与关键岗位的人员签署岗位责任协议。

d）与授权访问关键信息基础设施的人员（包含外部人员）签订保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

e）参照国家或行业相关规定，落实网络安全关键岗位专业技术人员执证上岗的要求。

6.3.3 人员培训

6.3.3.1 培训制度

关键信息基础设施运营者应：

a）建立网络安全教育培训制度，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本安全技能培训，为关键岗位人员提供基于岗位的专业安全技能培训。

b）将安全意识教育和基本安全技能培训作为关键信息基础设施从业人员入职培训的一部分。

c）确保关键岗位人员上岗前参加与岗位相关的安全技能培训。

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8个学时，网络安全关键岗位的人员年度培训时长不少于24个学时。

6.3.3.2 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。

6.3.3.3 培训内容

关键信息基础设施运营者应：

a）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。

b）确保培训内容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、岗位操作规程等。

6.3.3.4 技能考核

关键信息基础设施运营者应至少每年一次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。

6.3.4 人员调动

关键信息基础设施运营者应在人员发生内部岗位调动时：

a）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）及时通知相关人员或角色。

6.3.5 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）及时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）及时通知相关人员或角色。

6.3.6 职责分离

关键信息基础设施运营者应：

a）对关键岗位的职责进行分离，形成相互制约。例如，系统管理员不能同时兼任审计管理员。

b）遵循职责分离原则进行访问授权，以避免未授权或无意的修改或者不当使用组织资产。

6.4 安全通信网络

6.4.1 互联安全

关键信息基础设施运营者应建立或完善不同等级系统、不同业务系统、不同区域之间的安全互联策略，该策略应：

a）确保互联策略包括数据交换、数据获取、数据流向、互联层次、服务请求方向等方面的访问控制、边界防护策略等内容。

b）明确不同等级系统之间的安全互联策略，如从低安全等级向高安全等级的访问控制策略，从高安全等级向低安全等级的数据流控制策略等。

c）明确不同业务系统之间的安全互联策略，如具有相同系统服务安全保护等级系统、不同安全保护等级的业务信息共享型系统、不同安全保护等级的系统服务共享型系统之间的安全互联策略。

d）明确不同区域之间的安全互联策略，如终端区、服务器区、核心交换区、对外服务区等之间的访问控制、边界防护策略等。

e）保持不同系统或区域互联过程中用户身份、安全标记、访问控制策略等的一致性。例如，通过统一身份与授权管理系统对用户身份进行集中管理，实现用户安全标记、应用程序安全标记、业务数据安全标记等应在用户访问关键信息基础设施的全过程中携带，以确保主体对客体访问控制策略的一致性。

f）加强不同局域网之间远程通信时的安全防护，在通信前基于密码技术对通信的双方进行验证或认证，如基于密码机或证书。

6.4.2 边界防护

6.4.2.1 交互控制

关键信息基础设施运营者应采取措施对不同等级系统、不同业务系统、不同区域之间的互操作、数据交换进行严格控制，可包括：

a）确保不同等级系统之间的互联边界达到较高等级系统的安全防护要求。

b）对不同类别、不同级别的数据交换进行限制，如限制从高等级系统向低等级系统的数据输出。

c）通过业务服务层次实现不同等级系统之间的交互，如将低等级系统作为高等级系统的“客户端”。

d）根据区域所处位置、服务特点、功能需求等，明确不同区域之间的访问控制策略。

6.4.2.2 信息流控制

关键信息基础设施运营者应在确保客户隐私权和安全利益的前提下：

a）制定信息流控制策略，控制系统内或互连系统间的信息流动，如限制受控信息流向互联网、限制重要数据流向境外或在境外处理、限制关键信息基础设施信息系统主动对外部网络的访问、限制跨区域数据流动、限制某些数据格式或含关键字的信息流出关键信息基础设施。

b）定义禁止在不同的安全域之间传输的信息类型、特征或关键字，检查跨不同安全域的信息传输中是否存在禁止类信息，并遵循信息流控制策略，禁止传输此类信息。

c）唯一地标识和鉴别以组织、系统、应用、个人为标识的源和目的地址，以实施信息流策略，如禁止信息流向境外目的地址。

d）使用同一设备对多个不同安全域上的计算平台、应用或数据访问时，防止不同安全域之间的任何信息以违背信息流策略的方式流动。

6.4.2.3 软硬件设备管控

关键信息基础设施运营者应采取措施加强对未授权设备的动态检测及管控能力，只允许通过运营者自身授权和安全评估的软硬件运行，措施包括：

a）在设备接入前对其进行安全评估。

b）对设备进行唯一性标识与鉴别，如基于设备的介质访问控制（MAC）地址。

c）对唯一性标识进行集中管理，确保通过唯一性标识可快速查找到设备。

d）对软件进行安全评估，并实施注册管理。

e）对设备接入进行实时监测，能够及时发现和阻止未授权设备接入并报警。

6.4.2.4 移动设备的物理连接

关键信息基础设施运营者应确保只有经其授权的移动设备才能直接连接关键信息基础设施的信息系统，并应：

a）在移动设备连接信息系统前对其进行安全检查，禁止自动执行移动设备上的代码。

b）防止信息系统的信息非授权写入移动设备。

6.4.3 安全审计

关键信息基础设施运营者应：

a）明确审计范围，包括系统运行状态、日常操作、故障维护、远程运维等，并形成审计记录。

b）明确对审计记录进行审查、分析、报告的策略，当信息系统面临的威胁环境发生变化时，及时调整策略。

c）确保审计分析报告至少包括以下内容：

1）对关键信息基础设施网络安全状态的整体描述。

2）审计中发现的异常情况以及处置情况。

3）远程访问的总体情况及其统计分析。

d）使用自动机制对审计记录进行审查和分析，能够发现不当或异常活动，并向相关人员或角色报告。

6.5 安全计算环境

6.5.1 鉴别与授权

关键信息基础设施运营者应：

a）加强对设备、用户、服务或应用、数据的安全管控，包括：

1）在与设备、用户或其他服务或应用建立通信之前，对服务和应用程序进行标识与鉴别。

2）在用户行为出现异常情况时应使用额外的鉴别机制实施身份鉴别。

3）登录用户执行重要操作时应再次进行身份鉴别。

b）针对重要业务数据资源的操作，对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。

6.5.2 入侵防范

关键信息基础设施运营者应：

a）实现或完善对新型网络攻击行为（如APT攻击）的入侵防范，以及因不安全设备组合形成的网络攻击，如工业控制系统、物联网等面临的网络攻击行为。

b）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。

c）对恶意代码防护机制进行自动更新和集中管理。

d）增强系统的主动防护能力，基于主动免疫可信验证机制等技术手段，及时识别并阻断入侵和病毒行为。

6.5.3 数据安全防护

6.5.3.1 数据出境评估

关键信息基础设施运营者应：

a）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）因业务需要，确需向境外提供的，在数据出境前，自行组织或报请关键信息基础设施保护工作部门，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。

c）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保护工作部门。

6.5.3.2 数据安全管理

关键信息基础设施运营者：

a）根据数据分类分级的不同，制定符合其安全需要的保护策略，并在数据全生命周期采取一致的安全保护策略。

b）建立健全数据全生命周期安全管理制度。

c）严格控制重要数据的公开、分析、交换、共享和导出等关键环节。例如，确保重要数据公开前进行经过脱敏、多级审批；导出前应经过多级审批；明确数据分析的程度和范围；限制共享数据的类型、范围以及共享后的使用目的等，对数据进行加密后进行共享；

d）采取措施保护重要数据的完整性、保密性、可用性，防止信息泄露、篡改、损毁、丢失，安全措施可包括加密传输和存储、身份鉴别、访问控制、安全审计和数据备份等。

e）保留对数据的操作记录，增强操作可追溯性。

f）在可能涉及法律责任认定的应用中，能够基于密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

6.5.3.3 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等个人信息保护国家标准要求。

6.5.4 容灾备份

6.5.4.1 容灾备份机制

关键信息基础设施运营者应：

a）确定灾难备份目标，制定容灾备份策略，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，如至少每天完成一次重要系统和数据备份、每天多次利用通信网络将相关数据定时批量传送至备用场地。

b）根据灾难备份策略制定相应的容灾备份系统技术方案，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）对重要系统和数据库实现异地备份。

d）根据业务特点，数据更新快、完整性要求高的重要数据库，实现实时数据传输及完整设备支持。

e）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。

f）对业务连续性要求高的业务，实现异地实时切换。

6.5.4.2 容灾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。

6.5.5 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）业务连续性要求高的实现业务的异地实时切换，确保关键信息基础设施一旦被破坏，可及时进行恢复和补救。

e）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。

6.5.6 自动化管理

6.5.6.1 漏洞自动管理

关键信息基础设施运营者应：

a）使用漏洞管理工具，能够自动发现、记录、处置安全漏洞相关信息，包括漏洞名称、位置、影响、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，确保使用经过测试的漏洞补丁。

c）确保漏洞管理过程对业务连续性的影响在可接受范围内。

6.5.6.2 账户自动管理

关键信息基础设施运营者应：

a）采用自动方式进行账户管理。

b）定义临时账号的有效时间段，超出该时间段后，自动删除或禁用临时和应急账号。

c）定义不活跃时间段，超出该时间段后自动关闭非活跃账号。

d）对账号的建立、更改、禁用和终止行为进行自动审计，并将情况向安全责任部门或相关人员通报。

6.5.6.3 配置自动管理

关键信息基础设施运营者应使用自动机制对配置参数进行集中管理、应用和验证。

6.6 安全建设管理

6.6.1 网络安全与信息化同步要求

6.6.1.1 同步规划

关键信息基础设施运营者在新建或改建、扩建关键信息基础设施时应：

a）在关键信息基础设施建设或改建之初，根据风险识别的结果，从本组织的职能或业务的角度分析关键信息基础设施实施网络安全的需求。

b）基于安全需求，定义关键信息基础设施的网络安全要求。

c）确保安全需求得到网络安全管理机构审核，例如，得到网络安全责任部门签字认可或经过评审并有纪要。

d）同步预算编制，关键信息基础设施的运营者在编制项目投资计划时，将安全措施所需的投资纳入预算。

e）基于网络安全要求，开展详细的安全设计，细化安全机制在关键信息基础设施中的具体实现。

f）确保设计完成后通过评审。

6.6.1.2 同步建设

关键信息基础设施运营者在新建或改建、扩建关键信息基础实施设施时应：

a）实施监理等管控措施。

b）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。

c）确保关键信息基础设施发生重大变化时，按照相关规定进行安全检测评估，并开展安全验收工作，通过验收后方可投入运行。

6.6.1.3 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，确保安全设施保持正常有效状态，与主体工程同时投入使用。

b）关键信息基础设施及其运行环境发生明显变化时，重新评估其风险，根据评估结果及相关要求，及时调整安全设施并实施变更管理，调整后的安全设施原则上不低于原有水平。

c）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。

d）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。

e）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。

6.6.2 供应链保护

关键信息基础设施运营者应采取供应链保护措施，以降低攻击者利用供应链造成的危害。根据实际情况，保护措施可包括但不限于：

a) 优先购买现货产品，避免购买定制设备。

b) 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。

c) 选择有声誉的企业，建立合格供应商列表（含潜在供应商）。

d) 缩短采购决定和交付的时间间隔。

e) 使用可信或可控的分发、交付和仓储手段。

f) 保护供应链相关信息（包括用户身份、产品或服务的用途、供应商身份、供应商处理过程等），如通过向供应商屏蔽关键信息、采取匿名采购或委托采购的方式，以降低因信息汇聚或关联分析而获得供应链关键信息的可能性。

g) 在运输或仓储时使用防篡改包装。例如，采取防伪标签、安全封条、中性化包装，不体现包装物的信息，对包装物的封箱、开箱过程进行监督和记录，对封条使用和货柜安全操作建立指导性规程。

h) 限制从特定供应商或国家采购产品或服务。

i) 使用多个供应商提供的关键组件并储备足够的备用组件。

j) 明确供应商选择和退出的机制，基于供应商协议的履行情况等对供应商服务进行安全评估。按照评估结果对供应商产品进行质量、可靠性、安全进行测试，并将合格的测试结果作为采购的条件。

6.6.3 网络产品和服务采购与使用

关键信息基础设施运营者应：

a）确保采购、使用的网络产品和服务（如网络安全产品、网络专用设备、社会化云服务、安全检测服务），符合法律、行政法规的规定和相关国家标准的要求。

b）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。

c）对于可能影响国家安全的网络产品和服务，采购时确保其按照网络产品和服务安全审查有关法规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。

d）发现使用的网络产品、服务存在安全缺陷、漏洞等风险时，应当及时采取措施消除风险隐患，涉及重大风险的应当按规定向保护工作部门报告。

6.6.4 网络产品和服务供应商管理

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），明确服务水平可满足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、标准以及云服务商的安全要求。

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）提供详细和完整的硬件组件清单和产地清单。

6）提供完整性保护措施，确保提供的产品真实且未被改动，如防伪标签、可核查序列号、防篡改技术等。

7）制定物流管理规程，完整记录入库、转库等物流信息，确保产品的可追溯性；在此基础上，建立标签码追溯数据管理规程和配套系统，确保从物料到产品交付的可追溯性。

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）分析供应商对信息系统、组件和服务的设计、开发、实施、验证、交付、支持过程。

2）评价供应商在开发信息系统、组件或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）当变更供应商时，对供应商变更带来的安全风险进行评估，并采取有关措施对风险进行控制。

6.7 安全运维管理

6.7.1 运维审批和记录

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所控制环境之外进行维护或维修前，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。

6.7.2 运维工具

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）如非必要尽量使用现有运维工具。确需使用由维护人员带入关键信息基础设施内部的维护工具时，在使用前应通过恶意代码检测等方式，确保维护工具未被不当修改。

d）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，例如可通过采取以下措施，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的信息。

2）净化或销毁设备。

6.7.3 远程维护

关键信息基础设施运营者应：

a）采用自动化方式对远程维护活动进行管理、控制和审计。

b）在远程维护完成后及时终止会话。

c）形成远程维护日志，日志留存不少于12个月。

d）定期对远程维护日志进行审查。

e）确保在境内实施远程维护，确需境外维护的，遵照国家有关规定。

6.7.4 运维人员

关键信息基础设施运营者应：

a）建立对运维人员的授权流程，对已获授权的人员建立列表。

b）定期审核更新运维人员授权列表。

c）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。

7 检测评估

7.1 检测评估制度

关键信息基础设施运营者应：

a）根据国家政策、法律法规要求和组织需求，明确检测评估策略（包含网络安全检测和风险评估），阐述检测评估目的、范围、角色、责任及组织内协调等。

b）基于检测评估策略，建立健全关键信息基础设施安全检测评估制度和流程，检测评估应包括合规检查、技术检查、分析评估等方面。

c）建立年度检测评估工作责任制，明确检测中的角色分工和相应职责，建立相应问责机制。

7.2 检测评估方式和内容

关键信息基础设施运营者应：

a）参照GB/T BBBBB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全面的检测评估。选择网络安全服务机构时应考虑其专业资质、评估经验、行业背景等因素。

b）形成常规安全检测评估与全面安全检测评估体系。常规安全检测评估内容包括关键信息基础设施日常运行、相关规程和策略中的安全漏洞、文件和数据的备份及完整性、可用性校验等；全面安全检测评估内容现有安全技术措施的有效性、安全管理制度落地情况、对前次检测评估发现问题的整改情况、漏洞发现、关键信息基础设施的抵御渗透攻击的能力、监测预警能力、关键信息基础设施的安全态势等。

c）在检测评估过程中，明确关键信息基础设施跨系统、跨区域间的信息流动，及其关键业务流动过程中所经资产的安全防护情况。

d）在检测评估过程中，测试工具的接入采取从关键信息基础设施安全防护边界外部到内部网络的逐步逐点接入，如测试工具应从被测系统边界外接入、在被测系统内部与测评对象不同网段及同一网段内接入，包括运维域、办公域、业务域等。

e）参照GB/T BBBBB附录A，编制检测评估报告，并按规定及时上报对应的关键基础设施安全保护工作部门。

f）新建以及改建或扩建的关键信息基础设施发生重大变化时，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行前应自行或委托第三方评估机构按照关键信息基础设施网络安全防护基本要求进行安全检测评估，并开展安全验收工作，通过验收后方可投入运行。

7.3 安全抽查

关键信息基础设施运营者应：

a）参照GB/T BBBBB要求，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。

b）提供可供开展抽查工作的网络和系统接入环境。

7.4 整改

关键信息基础设施运营者应：

a）根据检测评估以及抽查检测情况，针对网络安全状况和存在的风险，提出完善网络安全管理制度和技术防护措施的总体意见。

b）针对检查中发现的具体问题，逐个提出解决措施、整改方案。

c）将上述整改方案提交本组织的网络安全管理机构审核。

d）审核通过后，对关键信息基础设施及时实施整改，将风险降低到可接受的水平。

e）形成整改情况报告。

f）根据检测评估以及抽查检测情况，必要时调整关键信息基础设施安全检测评估制度和程序。

g）如整改导致关键信息基础设施变动较大，对相应的部分重新检测评估。

8 监测预警

8.1 监测预警制度

关键信息基础设施运营者应：

a）根据关键信息基础设施保护工作部门网络安全监测预警和信息通报的要求，制定自身的监测预警和信息通报制度。

b）建立监测预警和信息通报机制，包括：

1）内部沟通合作机制建设，加强管理人员、网络安全管理机构与内部其他部门之间的沟通与合作，定期召开协调会议，共同研判、处置网络安全问题。

2）外部协作处置机制建设，建立和维护外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

c）依据GB/T 36635等标准，制定监测策略，主要包括：

1）明确监测对象，为监测过程提供数据源，包括物理环境、通信环境、区域边界、计算存储环境、安全环境等。

2）明确监测流程，通过数据分析的方法识别与发现网络安全问题与状态，包括接口连接、采集、存储、分析、展示与告警等。

3）明确监测内容，包括运行状态监测、安全事件监测等。

d）依据GB/Z 20986等标准，明确本组织的预警信息分级标准。例如，将预警信息分为四级，分别对应发生或可能发生特别重大事件、重大事件、较大事件和一般事件。

e）参考GB/T 32924，建立预警信息响应处置程序，明确不同级别预警信息的报告、响应和处置流程。

f）综合评估特定时间期限内（如每月）的监测预警情况并向网络安全管理机构以及相关人员或角色报告。

8.2 监测

8.2.1 监测设备

关键信息基础设施运营者应选择和部署监测设备，以满足以下要求：

a）对系统运行状态和安全状态进行监测。

b）支持基于异常流量、行为或状态的监测，能够分析信息系统通信流量模式，建立并定期更新常见系统通信流量或事态的模型。

c）基于监测策略和异常模型等，配置监测系统（包括软硬件工具），以减少误报和漏报。

d）对监测获得的信息采取保护措施，防止其受到未授权的访问、修改和删除。

e）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。

f）将监测分析结果存储至少 12 个月。

8.2.2 监测内容

8.2.2.1 运行状态监测

关键信息基础设施运营者应对关键业务所涉及的信息系统的运行状态进行实时监测，包括：

a）对设备和系统状态进行监测。

b）对网络流量进行监测。

c）对加密通信进行监测。

d）对应用层进行监测。

e）对不同等级系统、不同业务系统、不同区域之间的信息流动进行监测。

f）对远程运维的行为进行监测。

g）对硬设备件的运行参数、人员操作、故障维护进行监测。

8.2.2.2 安全事件监测

关键信息基础设施运营者应对信息系统的安全事件进行监测，包括：

a）能够发现网络攻击行为，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）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监测机制。

d）配置恶意代码监测机制，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。

e）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。

f）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。

g）确保恶意代码监测机制得到及时更新，如升级病毒库。

8.2.2.3 物理访问监测

关键信息基础设施运营者应：

a）对关键信息基础设施进行物理访问监测，例如通过采取门禁、视频监控、电子围栏等措施，形成物理访问日志，物理访问日志留存时间不少于12个月。

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。

8.2.3 监测信息关联分析

关键信息基础设施运营者应：

a）采用自动化机制对关键业务所涉及的信息系统的所有监测信息进行整合分析。

b）对关键业务运行所涉及的各类信息进行关联，包括：

1）分析不同存储库的审计日志并使之关联；

2）系统内多个组件的审计记录进行关联；

3）将取自审计记录的信息与得自物理访问监控的信息进行关联；

4）将来自非技术源的信息（例如供应链活动信息、关键岗位人员信息等）与审计信息进行关联；

5）将监测信息与网络安全信息共享信息进行关联等。

c）整合监测信息和关联信息，及时分析关键信息基础设施的网络安全态势，分析方式可以包括：

1）检查信息系统中近期出现的威胁信息；

2）评估特定类型网络攻击的成功率；

3）分析新技术、新应用产生的脆弱性等。

d）根据安全态势分析结果，确定安全策略和安全控制措施是否合理有效，必要时进行更新。

8.3 预警

8.3.1 信息共享

关键信息基础设施运营者应:

a）建立与关键信息基础设施保护工作部门、研究机构、网络安全服务机构、业界专家及其他有关部门的网络安全信息共享渠道。

b）确定共享信息的范围，包括漏洞信息、威胁信息、最佳实践、前沿技术等。

c）建立本组织的信息共享和分析中心，收集漏洞信息、威胁信息及其防护措施并进行分析，必要时与相关网络安全威胁信息共享平台进行对接，共享时宜采用标准化的网络安全威胁信息格式。

d）对共享或接收网络威胁信息或防护措施的行为进行授权。

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

f）在信息共享前，使用技术手段对共享信息进行脱敏处理，包括但不限于能够可识别具体人员的信息、ICT资产关键信息等。

g）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。

8.3.2 监测报警信息

关键信息基础设施运营者应：

a）建立自动化的报警机制，对监测信息进行研判，必要时能采用自动化的方式向网络安全管理机构及相关人员、角色和部门发出安全报警信息。例如，通过恶意代码防御机制、入侵检测设备或者防火墙等，弹出对话框、发出声音或者向相关人员发出电子邮件等方式进行报警。

b）当发现可能危害关键业务的安全威胁时，及时向相关人员或角色发出相应级别的报警信息，安全威胁包括但不限于：

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）发生异常资源消耗，如缓冲区溢出。

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）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。
6）进程或服务的运行方式与系统常规情况不符。
7）在生产系统上保存或安装与业务无关的程序、工具、脚本。
8）发现使用未知的移动存储介质。
9）未授权读取、修改或删除敏感数据时。

c）能够自动采取对关键业务破坏性最小的行动。

8.3.3 内部预警信息

关键信息基础设施运营者应：

a）对网络安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息。

b）确保内部预警信息的内容包括：基本情况描述、可能产生的危害及程度、可能影响的用户及范围、建议采取的应对措施等。

c）经研判，对于可能造成较大影响的，按照关键信息基础设施保护工作部门网络安全信息通报的要求进行通报。

d）当内部预警信息发出之后，情况出现新的变化，向有关人员和组织及时补发最新内部预警信息。

8.3.4 外部预警信息

关键信息基础设施运营者应：

a）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，持续接收关键信息基础设施安全保护工作部门发布的安全风险、预警信息和应急防范措施建议。

b）分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度。

c）将研判结果向上级或主管部门汇报。

d）经上级或主管部门同意后，采取适当形式发送预警或通告给相关用户。

e）及时响应安全预警信息和建议，必要时启动应急预案，如无法响应需说明原因。

9 事件处置

9.1 事件管理制度

关键信息基础设施运营者应：

a）建立网络安全事件管理制度，该制度应：
1）描述本组织内与事件管理有关的组织架构。
2）参照GB/Z 20986，明确不同网络安全事件的分类分级。
3）明确不同类别、级别事件的报告、处置和响应流程。
4）要求制定应急预案等网络安全事件管理文档。

b）确保网络安全事件管理制度由网络安全管理机构及相关人员或角色审查和批准。

c）具备网络安全事件处置的能力，为网络安全事件处置提供相应资源，指定专门网络安全应急支撑队伍、专家队伍，保障安全事件得到及时有效处置。

d）如系统发生变更或事件管理制度在实施、执行或演练中遇到问题，及时修改并通报相关人员或角色。

9.2 应急预案

9.2.1 预案制定

关键信息基础设施运营者应：

a）依据行业和地方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）明确应急角色、职责和联系信息。

2）明确一旦信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能。

3）明确遭受破坏时恢复关键业务和恢复全部业务的时间。

4）对预案演练、宣传、培训等工作进行规划。

5）落实技术支撑队伍、专家队伍、社会资源、经费等保障措施。

6）不仅包括本组织应急事件的处理，也包括多个组织间的应急事件的处理（若适用）。

b）至少每年一次对网络安全事件应急预案进行评估修订。

c）同所涉及到的组织内部相关计划（例如业务持续性计划、灾难备份计划等）以及外部服务提供者的应急计划进行协调，以确保连续性要求得以满足。

d）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。

e）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。

f）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。

g）防止网络安全事件应急预案非授权泄露和更改。

h）在发生安全事件时，确保应急预案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。

9.2.2 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与其角色或职责相关的应急培训。

b）定期开展应急培训，或当关键信息基础设施发生重大变更时重新开展培训。

c）将模拟事件纳入到应急培训中，以帮助相关人员或角色在紧急情况下做出有效的响应。

d）采用自动化机制支持应急培训环境的建立。

9.2.3 应急演练

关键信息基础设施运营者应：

a）制定应急演练计划并根据演练情况进行持续改进。

b）至少每年组织一次跨组织、跨地域的应急演练，必要时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，完善应急演练计划并根据需要调整应急预案。

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。

i）采用自动化机制来更彻底和有效地演练通过提供更全面的应急问题的应急预案，并选择更现实的演练方案和环境，以便更有效地强调信息系统和支持任务。

9.3 响应和处置

9.3.1 事件报告

关键信息基础设施运营者应：

a）能够采取自动化机制协助生成事件报告。

b）当发生有可能危害关键业务的安全事件时，应组织研判并在规定时间内及时向网络安全管理机构报告，形成事件报告单。

c）及时将可能危害关键业务的安全事件通报到可能受影响的内部部门和人员，并按照规定向关键业务供应链涉及的、与事件相关的其他组织通报安全事件。

d）当发生影响范围或严重程度较大的安全事件时，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。

9.3.2 事件处置

关键信息基础设施运营者应：

a）对监测预警中发现的问题进行评估，判断其是否为安全事件并确定事件级别。

b）按照事件处置流程、应急预案进行事件处置，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大。

c）针对重大或突发的安全事件，及时启动应急预案。

d）协调组织内部多个部门和外部相关组织，以更好的对事件处置。

e）将事件信息和各个事件响应相关联，以便从整个组织的角度知晓事件并予以响应。

f）采用自动化机制支持网络安全事件处置，例如自动隔离有害程序事件、自动阻止网络攻击事件等。

g）在事件发生后尽快收集证据，按要求进行信息安全取证分析，并确保所有涉及的事件处置和应急响应活动被适当记录，便于日后分析。

9.3.3 系统恢复

关键信息基础设施运营者应：

a）在事件发生后，能够恢复关键业务和信息系统到已知的状态。

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。

9.3.4 事件总结

关键信息基础设施运营者应：

a）在事件处置完成后，采用手工或者自动化机制形成完整的事件处理报告。事件处理报告包括：不同部门对事件的处理记录、事件的状态和取证相关的其他必要信息、评估事件细节、趋势和处理。

b）在恢复关键业务和信息系统后，对关键业务和信息系统恢复情况进行评估，查找事件原因，并采取措施防止关键业务和信息系统遭受再次破坏、危害或故障。

c）从事件处置中学到经验教训经验，审核、明确并改进信息安全控制措施的实施，以及事件管理策略。

d）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。

9.3.5 事件通报

关键信息基础设施运营者应：

a）安全事件及其处置情况通报到可能受影响的部门和相关人员。

b）向关键业务供应链涉及的、与事件相关的其他组织提供安全事件信息。

c）按照相关规定通报关键信息基础设施保护工作部门。

9.4 重新评估

关键信息基础设施运营者应：

a）根据检测评估、监测预警中发现的安全隐患和发生的安全事件，以及处置结果开展综合评估。

b）必要时，重新开展风险识别，并更新安全策略和控制措施。

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）》