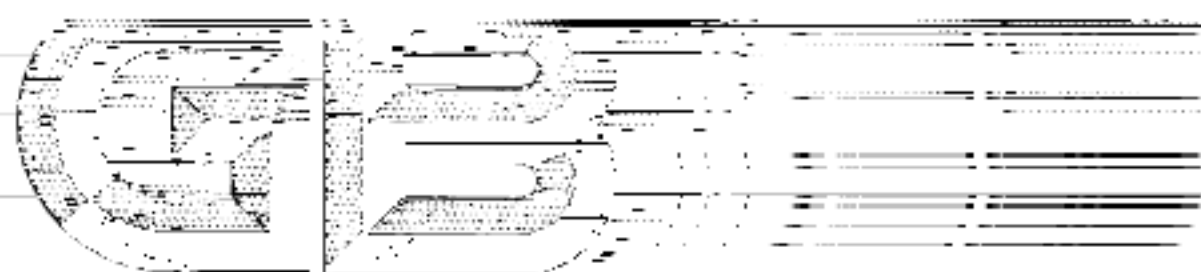


ICS 35.040

L 80



中华人民共和国国家标准

信息安全技术 网络安全等级保护基本要求

代替 GB/T 22080-2008

GB/T 22080-2016/ISO/IEC 27001-2015

信息技术 安全技术

信

网络安全等级保护基本要求

Information technology — Security techniques —

网络安全等级保护基本要求

GB/T 22080-2016/ISO/IEC 27001-2015

2017-02-01 实施

2016-08-29 发布

中华人民共和国国家质量监督检验检疫总局

发布

中华

前

引言

0.1 总则

一是信息组织。二是信息资源建设。三是信息基础设施建设和信息资源开发利用。四是信息安全保障体系建设。五是信息资源开发利用。六是信息资源开发利用。七是信息资源开发利用。八是信息资源开发利用。九是信息资源开发利用。十是信息资源开发利用。十一是信息资源开发利用。十二是信息资源开发利用。十三是信息资源开发利用。十四是信息资源开发利用。十五是信息资源开发利用。十六是信息资源开发利用。十七是信息资源开发利用。十八是信息资源开发利用。十九是信息资源开发利用。二十是信息资源开发利用。二十一、二十二、二十三、二十四、二十五、二十六、二十七、二十八、二十九、三十、三十一、三十二、三十三、三十四、三十五、三十六、三十七、三十八、三十九、四十、四十一、四十二、四十三、四十四、四十五、四十六、四十七、四十八、四十九、五十、五十一、五十二、五十三、五十四、五十五、五十六、五十七、五十八、五十九、六十、六十一、六十二、六十三、六十四、六十五、六十六、六十七、六十八、六十九、七十、七十一、七十二、七十三、七十四、七十五、七十六、七十七、七十八、七十九、八十、八十一、八十二、八十三、八十四、八十五、八十六、八十七、八十八、八十九、九十、九十一、九十二、九十三、九十四、九十五、九十六、九十七、九十八、九十九、一百。

0.2 与其他管理体系标准的兼容性

本标准应用ISO/IEC 合并导则附录SL中定义的高层结构、相同条款标题和核心定义,因此保持了与其他采用附录SL的管理体系的标准具有兼容性。

信息安全管理体系规范

1 范围

2 规范性引用文件

3 术语和定义

4 组织环境

4.1 理解组织及其环境

组织应确定与其范围相关的、且影响其实现信息安全管理体系预期结果能力的外部 and 内部事项。

4.2 理解相关方的需求和期望

组织应确定：

4.3 确定信息安全管理体系范围

组织应确定信息安全管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

a) 4.1 中提到的外部和内部事项；

b) 4.2 中提到的要求；

c) 组织实施的活动之间及其与其他组织实施的活动之间的接口和依赖关系。

该范围应形成文件化信息并可用。

4.4 信息安全管理体

组织应按照本标准的要求，建立、实施、维护和持续改进信息安全管理体系。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实对信息安全管理体系的领导作用和承诺：

- a) 制定信息安全方针；
- b) 制定信息安全管理体系的目标；
- c) 确保信息安全管理体系要求与组织业务目标相一致；
- d) 沟通信息安全管理体系的重要性；
- e) 提供信息安全管理体系所需的资源；
- f) 指定信息安全管理体系的负责人；
- g) 定期向最高管理层报告信息安全管理体系的绩效；
- h) 促进全员参与；
- i) 保持对信息安全管理体系的持续改进；
- j) 与组织外部相关方就信息安全管理体系进行沟通和联系。

5.2 方针

- a) 与组织意图相适宜；
- b) 包括信息安全方针的顶层（见6.2.2）或为顶层提供框架；
- c) 包括对满足适用的信息安全相关要求的承诺；
- d) 包括对持续改进信息安全管理体系的承诺；
- e) 信息安全方针应：
 - a) 形成文件化信息并可用；
 - b) 在组织内得到沟通；
 - c) 适当时，对相关方可用。

的角色、责任和权限

5.3 组织

最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通。

最高管理层

最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通。

最高管理层

- a) 确保信息安全管理体系符合本标准的要求；
- b) 向最高管理者报告信息安全管理体系绩效；

最高管理层的责任和权限

最高管理层的责任和权限

6 规划

6.1 应对风险和机会的措施

6.1.1 总则

组织应确定和实现其信息安全方针和信息安全管理体系的目标，并考虑其风险和机会。

组织应确定和实现其信息安全方针和信息安全管理体系的目标，并考虑其风险和机会。

风险和机会

第一、後時所進德教人利於百萬人皆能生利利則出之無憂國富則

组织应宗旨并应用信息：

2) 信息安全风险评估实施准则。^[1]

© 2004 Blackwell Publishing Ltd *Journal of Internal Medicine* 255: 103–110

2. 识别与除害责任人

1 范围 1.1 本标准适用于任何需要保护其信息的组织。

本标准规定了组织建立、实施、保持和改进信息安全管理体系的要求。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

本标准适用于任何需要保护其信息的组织。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进信息安全管理体系所需的资源。

7.2 能力

组织应：

确定必要能力；

a) 确定在组织控制下从事会影响组织信息安全绩效的工作；

b) 确定从事这些工作的人员应达到的能力要求；

c) 确定从事这些工作的人员应达到的能力要求；

d) 确定从事这些工作的人员应达到的能力要求；

确定必要能力；

确定必要能力；

7.3 意识

在组织控制下工作的人员应了解：

a) 信息安全方针；

b) 其对信息安全管理的要求；

本系统有效性的贡献，包括改进信息安全绩效带来的益处；

本系统有效性的贡献，包括改进信息安全绩效带来的益处；

7.4 沟通

组织应建立、实施、保持和改进信息安全管理体系所需的沟通。

a) 沟通什么；

b) 何时沟通；

- c) 与谁沟通;
- d) 谁来沟通;
- e) 影响沟通的过程。

7.5 文件化信息

7.5.1 总则

二、组织的信息安全管理体系应包括:

- 5) 为信息安全管理系统的有效实施，组织应确定必要的文件化信息，并控制其分发，以确保在需要时，可获得和使用。

7.5.2 创建和更新

加中而雷就寺城其地自明... 如何立路似汗也站

- [illegible]

[illegible]

77-6 土地所有權登記

[illegible]

- 为控制文件化信息, 组织应强调以下活动:

- ② 分发、访问、删除或更改；
- ③ 存储和保护，包括保持可塑性；
- ④ 负责变更控制，如版本控制；
- ⑤ 保留和处理。

型体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。组织确定的为规划和运行信息安全管

8 运行

8.1 运行规划和控制

为了满足信息安全要求以及实现业务连续性保障,项目组

8.2 信息安全风险评估

8.3 信息安全风险处置

9 绩效评价

9.1 监视、测量、分析和评价

9.2 内部审核

5) 与信息安全管理体系相关的外部环境因素的变化。

6) 信息安全事件及应急响应处置。

7) 不符合项纠正措施。

8) 监视、测量、分析和改进。

9) 审核结果。

10) 信息安全目标的达成情况。

11) 相关方反馈。

12) 风险和机遇应对措施的有效性。

13) 管理评审结果。

附录 A（规范性附录）
参考控制目的和控制

控制目的和控制		表 A-1
		信息安全策略
		信息安全管理制度
目的：为信息安全提供管理指导和支持。		目的：依据国家要求制定信息安全策略。
A.5.1.2 信息安全策略的评审	控制	应按计划的时间间隔或当重大变化发生时进行信息安全策略评审，以确保其持续的适宜性、充分性和有效性。
A.6 信息安全组织		
A.6.1 内部组织		
目的：建立一个管理框架，以启动和控制组织内信息安全的实现和运行。		
A.6.1.1 信息安全的角色和责任	控制	所有的信息安全责任应予以定义和分配。
A.6.1.2 职责分离	控制	应予以识别和定义所有信息安全职责，并予以分配。

A.6.1.4	与特定相关方的联系	控制	应维护与特定相关方——其他外部安全过程和去安
管理中的信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管
信息安全	控制	A.6.1.5	项目管

安全区域应由适合的入口控制所保护,以确保只 允许访问。	安全区域应由适合的入口控制所保护,以确保只 有授权的人员才
A.11.1.1.3 办公室、房间和设施的安全控制	控制
A.11.1.1.4 系统和环境数据的安全控制	控制
A.11.1.1.5 在安全区域工作	控制
A.11.1.1.6 交接区	控制
A.11.2 设备	控制
A.11.2.1 设备安置和标记	控制
A.11.2.2 支持性设施	控制
2.3 物理安全	控制
2.3.1 物理访问控制	控制
2.3.2 物理环境安全	控制
2.3.3 物理安全	控制
2.3.4 物理安全	控制
2.3.5 物理安全	控制
2.3.6 物理安全	控制
2.3.7 物理安全	控制
2.3.8 物理安全	控制
2.3.9 物理安全	控制
2.3.10 物理安全	控制
2.3.11 物理安全	控制
2.3.12 物理安全	控制
2.3.13 物理安全	控制
2.3.14 物理安全	控制
2.3.15 物理安全	控制
2.3.16 物理安全	控制
2.3.17 物理安全	控制
2.3.18 物理安全	控制
2.3.19 物理安全	控制
2.3.20 物理安全	控制
2.3.21 物理安全	控制
2.3.22 物理安全	控制
2.3.23 物理安全	控制
2.3.24 物理安全	控制
2.3.25 物理安全	控制
2.3.26 物理安全	控制
2.3.27 物理安全	控制
2.3.28 物理安全	控制
2.3.29 物理安全	控制
2.3.30 物理安全	控制
2.3.31 物理安全	控制
2.3.32 物理安全	控制
2.3.33 物理安全	控制
2.3.34 物理安全	控制
2.3.35 物理安全	控制
2.3.36 物理安全	控制
2.3.37 物理安全	控制
2.3.38 物理安全	控制
2.3.39 物理安全	控制
2.3.40 物理安全	控制
2.3.41 物理安全	控制
2.3.42 物理安全	控制
2.3.43 物理安全	控制
2.3.44 物理安全	控制
2.3.45 物理安全	控制
2.3.46 物理安全	控制
2.3.47 物理安全	控制
2.3.48 物理安全	控制
2.3.49 物理安全	控制
2.3.50 物理安全	控制
2.3.51 物理安全	控制
2.3.52 物理安全	控制
2.3.53 物理安全	控制
2.3.54 物理安全	控制
2.3.55 物理安全	控制
2.3.56 物理安全	控制
2.3.57 物理安全	控制
2.3.58 物理安全	控制
2.3.59 物理安全	控制
2.3.60 物理安全	控制
2.3.61 物理安全	控制
2.3.62 物理安全	控制
2.3.63 物理安全	控制
2.3.64 物理安全	控制
2.3.65 物理安全	控制
2.3.66 物理安全	控制
2.3.67 物理安全	控制
2.3.68 物理安全	控制
2.3.69 物理安全	控制
2.3.70 物理安全	控制
2.3.71 物理安全	控制
2.3.72 物理安全	控制
2.3.73 物理安全	控制
2.3.74 物理安全	控制
2.3.75 物理安全	控制
2.3.76 物理安全	控制
2.3.77 物理安全	控制
2.3.78 物理安全	控制
2.3.79 物理安全	控制
2.3.80 物理安全	控制
2.3.81 物理安全	控制
2.3.82 物理安全	控制
2.3.83 物理安全	控制
2.3.84 物理安全	控制
2.3.85 物理安全	控制
2.3.86 物理安全	控制
2.3.87 物理安全	控制
2.3.88 物理安全	控制
2.3.89 物理安全	控制
2.3.90 物理安全	控制
2.3.91 物理安全	控制
2.3.92 物理安全	控制
2.3.93 物理安全	控制
2.3.94 物理安全	控制
2.3.95 物理安全	控制
2.3.96 物理安全	控制
2.3.97 物理安全	控制
2.3.98 物理安全	控制
2.3.99 物理安全	控制

5.2.3 用户访问控制

用以确保用户访问其用户设备有适当的保护。

A.5.2.3.1 物理访问控制

控制

控制

应控制影响信息安全的变更，包括组织、业务过程、信息处理设施或系统变更。

控制

应对资源的可用性进行持续监测和调整，以保持资源可用性。

5.2.3 运行控制

A.5.2.3.1 运行控制

目的：确保正确、安全的操作信息处理设施。

A.5.2.3.1.1 文件化的操作规程

控制

操作程序文档

A.5.2.3.2 变更管理

A.5.2.3.3 容量管理

[illegible]

A.13.2 信息传输

A.13.2.1 信息传输策略和规程

控制

应有正式传输策略、规程和控制，以保护通过
使用各种类型通信设施进行的信息传输。

A.13.2.2 信息传输协议

控制

A.13.2.4 保密或不泄露协议

控制

A.13.2.3 电子消息发送

A.14 系统安全开发操作

A.15 信息安全要求

其他：所有信息符合其信息系统安全要求，符合其安全策略。

A.16 安全策略

A.17 安全策略

A.18 安全策略

A.19 安全策略

A.20 安全策略

A.21 安全策略

A.22 安全策略

A.23 安全策略

A.24 安全策略

A.25 安全策略

A.26 安全策略

A.27 安全策略

A.28 安全策略

A.29 安全策略

A.30 安全策略

A.31 安全策略

A.32 安全策略

A.33 安全策略

A.34 安全策略

A.35 安全策略

A.36 安全策略

在发生变更时，应确保其符合信息安全要求，并应进行评审和测试，以确保其不会对运行和安全管理产生负面影响。

控制

在变更实施前，应进行风险评估，并应记录变更实施的结果。

A.14.2.3 系统安全工程原则

维护系统安全工程原则，并应在实施工作中

应建立、文档化和

用到任何信息系统

术评审

A.14.2.4 软件包变更的限制

软件包变更应进行风险评估，并应记录变更实施的结果。

且所有变更都应严格审批

控制

应建立、文档化和
用到任何信息系统

的商定级别。

A.15.2 供应商服务交付管理

目的：维护与供应商协议一致的信息安全和服务交付。

A. 17. 1. 1	规划信息安全连续性	<i>控制</i> 组织应确定在不利情况（如危机或灾难）下，对 信息安全及信息安全管理体系持续的要求，并应制定并实施程序，以解决不利情况下的要求。
A. 17. 1. 2	实现信息安全连续性	<i>控制</i> 组织应制定并实施程序，以解决不利情况下的要求，并应制定并实施程序，以解决不利情况下的要求。

			法规。
		A.18.2 信息安全评审	
		目的：确保依据组织策略和规程来实现和运行信息安全。	
安全的独立评审。	控制		A.18.2.1 信息
		应计划的时间间隔或在重大变化发生时，对组	
		织的信息安全管理方法及其实现（如信息安全策	
（过程和规程）进行			控制目的、控制、方针、策略
			独立评审。
		A.18.2.2 符合安全策略和标准	控制
现时的信息安全策略			策略应当定期评审并更新
策略、标准和任何其他安全要求			应定期进行安全策
		符合性。	
	A.18.2.3 技术符合性评审	控制	
		应定期评审信息系统与组织的信息安全策略和标	
标准符合性。			

参 考 文 献

[1] ISO/IEC 27002:2013, 信息技术 安全技术 信息安全控制实用规则

[2] ISO/IEC 27001:2005

[3] GB/T 22080-2016, 信息技术 安全技术 信息安全管理体系

[4] ISO 31000:2009, 风险管理 原则和指南

[5] ISO/IEC 指南, 第一部分, ISO综合补充 ISO具体标准, 2012