



中华人民共和国国家标准

GB/T 25058—2019
代替 GB/T 25058—2010

信息安全技术 网络安全等级保护实施指南

Information security technology—
Implementation guide for classified protection of cybersecurity

2019-08-30 发布

2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 等级保护实施概述	1
4.1 基本原则	1
4.2 角色和职责	2
4.3 实施的基本流程	2
5 等级保护对象定级与备案	4
5.1 定级与备案阶段的工作流程	4
5.2 行业/领域定级工作	4
5.3 等级保护对象分析	5
5.3.1 对象重要性分析	5
5.3.2 定级对象确定	6
5.4 安全保护等级确定	7
5.4.1 定级、审核和批准	7
5.4.2 形成定级报告	8
5.5 定级结果备案	8
6 总体安全规划	8
6.1 总体安全规划阶段的工作流程	8
6.2 安全需求分析	9
6.2.1 基本安全需求的确定	9
6.2.2 特殊安全需求的确定	9
6.2.3 形成安全需求分析报告	10
6.3 总体安全设计	10
6.3.1 总体安全策略设计	10
6.3.2 安全技术体系结构设计	11
6.3.3 整体安全管理体系结构设计	12
6.3.4 设计结果文档化	14
6.4 安全建设项目规划	14
6.4.1 安全建设目标确定	14
6.4.2 安全建设内容规划	14
6.4.3 形成安全建设项目规划	15
7 安全设计与实施	16
7.1 安全设计与实施阶段的工作流程	16
7.2 安全方案详细设计	16

- 7.2.1 技术措施实现内容的设计 16
- 7.2.2 管理措施实现内容的设计 17
- 7.2.3 设计结果的文档化 17
- 7.3 技术措施的实现 18
 - 7.3.1 网络安全产品或服务采购 18
 - 7.3.2 安全控制的开发 18
 - 7.3.3 安全控制集成 19
 - 7.3.4 系统验收 20
- 7.4 管理措施的实现 21
 - 7.4.1 安全管理制度的建设和修订 21
 - 7.4.2 安全管理机构和人员的设置 21
 - 7.4.3 安全实施过程管理 22
- 8 安全运行与维护 22
 - 8.1 安全运行与维护阶段的工作流程 22
 - 8.2 运行管理和控制 23
 - 8.2.1 运行管理职责确定 23
 - 8.2.2 运行管理过程控制 24
 - 8.3 变更管理和控制 24
 - 8.3.1 变更需求和影响分析 24
 - 8.3.2 变更过程控制 25
 - 8.4 安全状态监控 25
 - 8.4.1 监控对象确定 25
 - 8.4.2 监控对象状态信息收集 26
 - 8.4.3 监控状态分析和报告 26
 - 8.5 安全自查和持续改进 26
 - 8.5.1 安全状态自查 26
 - 8.5.2 改进方案制定 27
 - 8.5.3 安全改进实施 27
 - 8.6 服务商管理和监控 28
 - 8.6.1 服务商选择 28
 - 8.6.2 服务商管理 28
 - 8.6.3 服务商监控 29
 - 8.7 等级测评 30
 - 8.8 监督检查 30
 - 8.9 应急响应与保障 30
 - 8.9.1 应急准备 30
 - 8.9.2 应急监测与响应 31
 - 8.9.3 后期评估与改进 32
 - 8.9.4 应急保障 32
- 9 定级对象终止 32
 - 9.1 定级对象终止阶段的工作流程 32
 - 9.2 信息转移、暂存和清除 33

9.3 设备迁移或废弃	33
9.4 存储介质的清除或销毁	34
附录 A (规范性附录) 主要过程及其活动和输入输出	35

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 25058—2010《信息安全技术 信息系统安全等级保护实施指南》，与 GB/T 25058—2010 相比，主要变化如下：

- 标准名称变更为《信息安全技术 网络安全等级保护实施指南》。
- 全文将“信息系统”调整为“等级保护对象”或“定级对象”，将国家标准“信息系统安全等级保护基本要求”调整为“网络安全等级保护基本要求”。
- 考虑到云计算等新技术新应用 in 实施过程中的特殊处理，根据需要，相关章条增加云计算、移动互联网、大数据等相关内容(见 5.3.2、6.3.2、7.2.1、7.3.2)。
- 将各部分已有内容进一步细化，使其能够指导单位针对新建等级保护对象的等级保护工作(见 6.3.2、7.4.3)。
- 在等级保护对象定级阶段，增加了行业/领域主管单位的工作过程(见 5.2)；增加了云计算、移动互联网、物联网、工控、大数据定级的特殊关注点(见 5.3, 2010 年版的 5.2)。
- 在总体安全规划阶段，增加了行业等级保护管理规范和技术标准相关内容，即明确了基本安全需求既包括国家等级保护管理规范和技术标准提出的要求，也包括行业等级保护管理规范和技术标准提出的要求(见 6.2.1, 2010 年版的 6.2.1)。
- 在总体安全规划阶段，增加了“设计等级保护对象的安全技术体系架构”内容，要求根据机构总体安全策略文件、GB/T 22239 和机构安全需求，设计安全技术体系架构，并提供了安全技术体系架构图。此外，增加了云计算、移动互联网等新技术的安全保护技术措施(见 6.3.2, 2010 年版的 6.3.2)。
- 在总体安全规划阶段，增加了“设计等级保护对象的安全管理体系框架”内容，要求根据 GB/T 22239、安全需求分析报告等，设计安全管理体系框架，并提供了安全管理体系框架(见 6.3.3, 2010 年版的 6.3.3)。
- 在安全设计与实施阶段，将“技术措施实现”与“管理措施实现”调换顺序(见 7.3、7.4, 2010 年版的 7.3、7.4)；将“人员安全技能培训”合并到“安全管理机构和人员的设置”中(见 7.4.2, 2010 年版的 7.3.1、7.3.3)；将“安全管理制度的建设和修订”与“安全管理机构和人员的设置”调换顺序(见 7.4.1、7.4.2, 2010 年版的 7.4.1、7.4.2)。
- 在安全设计与实施阶段，在技术措施实现中增加了对于云计算、移动互联网等新技术的风险分析、技术防护措施实现等要求(见 7.2.1, 2010 年版的 7.2.1)；在测试环节中，更侧重安全漏洞扫描、渗透测试等安全测试内容(见 7.3.2, 2010 年版的 7.3.2)。
- 在安全设计与实施阶段，在原有信息安全产品供应商的基础上，增加网络安全服务机构的评价和选择要求(见 7.3.1)；安全控制集成中，增加安全态势感知、监测通报预警、应急处置追踪溯源等安全措施集成(见 7.3.3)；安全管理制度的建设和修订要求中，增加要求总体安全方针、安全管理制度、安全操作规程、安全运维记录和表单四层体系文件的一致性(见 7.4.1)；安全实施过程管理中，增加整体管理过程的活动内容描述(见 7.4.3)。
- 在安全运行与维护阶段，增加“服务商管理和监控”(见 8.6)；删除了“安全事件处置和应急预案”(2010 年版的 8.5)；删除了“系统备案”(2010 年版的 8.8)；修改了“监督检查”的内容(8.8, 2012 年版的 8.9)，增加了“应急响应与保障”(见 8.9)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

GB/T 25058—2019

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所(公安部信息安全等级保护评估中心)、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、北京安信天行科技有限公司。

本标准主要起草人:袁静、任卫红、毕马宁、黎水林、刘健、翟建军、王然、张益、江雷、赵泰、李明、马力、于东升、陈广勇、沙森森、朱建平、曲洁、李升、刘静、罗峥、彭海龙、徐爽亮。

本标准所代替标准的历次版本发布情况为:

——GB/T 25058—2010。

信息安全技术

网络安全等级保护实施指南

1 范围

本标准规定了等级保护对象实施网络安全等级保护工作的过程。

本标准适用于指导网络安全等级保护工作的实施。

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 17859 计算机信息系统 安全保护等级划分准则

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 28448 信息安全技术 网络安全等级保护测评要求

3 术语和定义

GB 17859、GB/T 22239、GB/T 25069 和 GB/T 28448 界定的术语和定义适用于本文件。

4 等级保护实施概述

4.1 基本原则

安全等级保护的核心是将等级保护对象划分等级,按标准进行建设、管理和监督。安全等级保护实施过程中应遵循以下基本原则:

a) 自主保护原则

等级保护对象运营、使用单位及其主管部门按照国家相关法规和标准,自主确定等级保护对象的安全保护等级,自行组织实施安全保护。

b) 重点保护原则

根据等级保护对象的重要程度、业务特点,通过划分不同安全保护等级的等级保护对象,实现不同强度的安全保护,集中资源优先保护涉及核心业务或关键信息资产的等级保护对象。

c) 同步建设原则

等级保护对象在新建、改建、扩建时应同步规划和设计安全方案,投入一定比例的资金建设网络安全设施,保障网络安全与信息化建设相适应。

d) 动态调整原则

应跟踪定级对象的变化情况,调整安全保护措施。由于定级对象的应用类型、范围等条件的变化及