中关村信息安全测评联盟团体标准
T/ISEAA 001-2019

网络安全等级保护测评高风险判定指引

编制说明

（征求意见稿）

《网络安全等级保护测评高风险判定指引》编制组

二〇一九年 7 月

《网络安全等级保护测评高风险判定指引（征求意见稿）》
编制说明

一、工作简况

1、任务来源

等级保护测评是推动和贯彻网络安全等级保护工作的重要环节之一。为了更好地提升全国等级保护测评能力，规范测评机构对系统安全风险严重程度的判定规则，由中关村信息安全测评联盟组织发起，上海市信息安全测评认证中心为标准编制牵头单位，中关村信息安全测评联盟为项目归口管理单位，联合全国多家等保测评机构，共同编写《网络安全等级保护测评高风险判定指引》（简称“判定指引”），旨在推动等保测评工作中风险判断更加标准化，规范化。从而规范等级保护测评过程，提升等级保护测评活动的质量。

2、主要工作过程

起草阶段：

2018 年 6 月，受中关村信息安全测评联盟委托，成立网络安全等级保护测评高风险情况研究讨论组，并在此基础上成立编制组，完成文档基础架构及编制组成员任务分工。

2018 年 7 月-8 月，编制组根据人工分工，进行内容编制，并形成《网络安全等级保护测评高风险判例》合稿。

2018 年 8 月-2018 年 10 月，《网络安全等级保护测评高风险判例》合稿提交讨论组讨论，并根据讨论意见对合稿文本进行了完善，形成《网络安全等级保护测评高风险判例》初稿。

2018 年 11 月 20 日，第八届网络安全等级保护测评体系建设会议上对《网络安全等级保护测评高风险判例》初稿内容进行了专题介绍。

2019 年 1 月-2019 年 3 月，基于《网络安全等级保护测评高风险判例》初稿及体系建设会议上的建议形成《判定指引》第一版征求意见稿，并向全国公安机关、等保测评机构征求意见。

2019 年 3 月-2019 年 4 月，编制组根据反馈的征求意见进一步完善《判定指引》，并在专题研讨会上对完善内容进行了介绍。

2019 年 5 月-2019 年 7 月，参编单位根据专题研讨会上专家的意见以及《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》、《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》的要求，对文档结构及内容进行再次完善，形成了《判定指引》第二版征求意见稿，并于 7 月中旬向标委会秘书处提交征求意见稿以及编制说明。

3、标准起草单位及其分工

本标准起草单位：上海市信息安全测评认证中心，杭州安信检测技术有限公司、江苏金盾检测技术有限公司、深圳市网安计算机安全检测技术有限公司、合肥天帷信息安全技术有限公司、山东新潮信息技术有限公司、成都安美勤信息技术股份有限公司、甘肃安信信息安全技术有限公司、江苏骏安信息测评认证有限公司、安徽祥盾信息科技有限公司。

本标准主要起草单位分工

（1）上海市信息安全测评认证中心负责组织《判定指引》标准文本的起草，按照团体标准报批要求，分阶段完成征求意见稿、送审稿、报批稿和其它相关资料。负责编制“安全物理环境”、“安全管理中心”、“管理制度”等部分高风险判例的编写以及全文统稿工作。

（2）杭州安信检测技术有限公司负责编制“安全边界区域”部分高风险判例的编写工作。

（3）江苏骏安信息测评认证有限公司、成都安美勤信息技术股份有限公司、甘肃安信信息安全技术有限公司负责“安全计算环境-设备部分”部分高风险判例的编写工作。

（4）江苏金盾检测技术有限公司、深圳市网安计算机安全检测技术有限公司负责“安全计算环境-应用和数据安全”部分高风险判例的编写工作。

（5）合肥天帷信息安全技术有限公司、山东新潮信息技术有限公司、安徽祥盾信息科技有限公司负责“管理制度”部分高风险判例的编写工作。

二、标准编制原则、确定标准主要内容的依据

1、标准编制原则

（1）本标准依据 GB/T 1.1-2016 要求进行编制。

（2）集全国各家机构经验，提出一些可判高风险的场景，给测评人员一个参考尺度，使等保测评工作更加标准化，规范化。

（3)与等保标准各等级中的核心要求相对应，强化各等级要求中必须实现的安全控制措施要求，从而提高被测系统的防护能力。

2、标准编制主要内容及其依据

（1）第一章　范围

本标准规定了适用于网络安全等级保护测评活动、安全检查等工作。信息系统建设单位亦可参考本指引描述的案例编制系统安全需求。

（2）第二章　规范性引用文件

本标准中引用了最新版国标、行标，以保证本标准条款的可依性和可行性。根据工作组会议讨论决定，规范性引用文件严格按照《标准化工作导则　第 1 部分： 标准结构和编写》GB/T 1.1-2009 要求进行逐条核对，并将本标准引用的标准全部列入。

（3）第三章　术语和定义

本章对后文中会使用的术语进行了定义，对后续章节内容描述提供了术语支持。

（4）第四章　安全物理环境

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全物理环境”的相关要求，提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、适用范围、满足条件、补偿措施、整改建议等信息。

（5）第五章　安全通信网络

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全通信网络”的相关要求，提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、

适用范围、满足条件、补偿措施、整改建议等信息。

（6）第六章　安全区域边界

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全区域边界”的相关要求，提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、适用范围、满足条件、补偿措施、整改建议等信息。

（7）第七章　安全计算环境

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全计算环境”的相关要求，针对设备、应用系统的差异，分别提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、适用范围、满足条件、补偿措施、整改建议等信息。

（8）第八章　安全管理中心

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全管理中心”的相关要求，提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、适用范围、满足条件、补偿措施、整改建议等信息。

（9）第九章　安全管理制度

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全管理制度”的相关要求，提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、适用范围、满足条件、补偿措施、整改建议等信息。

（10）第十章　安全管理机构

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全管理机构”的相关要求，提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、适用范围、满足条件、补偿措施、整改建议等信息。

（11）第十一章　安全建设管理

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全建设管理”的相关要求，提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、适用范围、满足条件、补偿措施、整改建议等信息。

（12）第十二章　安全运维管理

本章对应《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》中“安全运维管理”的相关要求，提出了可判高风险的场景，并针对于每条高风险判例并给出了判例内容、对应要求、适用范围、满足条件、补偿措施、整改建议等信息。

（13）附录 A(资料性附录) 基本要求与判例对应表

本章给出《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》与高风险判例的对应表。

三、标准中涉及专利的情况

本标准不涉及专利问题。

四、与国际、国外对比情况

无。

五、在标准体系中的位置，与现行相关法律、法规、规章及相关标准， 特别是强制性标准的协调性。

本标准属于等级保护测评活动的拓展标准。本标准与现行相关法律、法规、规章及相关标准无冲突。

六、重大分歧意见的处理经过和依据

无。

七、标准性质的建议说明

建议本标准的性质为推荐性团体标准。

八、贯彻标准的要求和措施建议

建议本标准实施与《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》实施时间保持一致。

九、废止现行相关标准的建议

无。

十、其他应予说明的事项

无。