团体标准《信息安全技术 网络安全等级保护应用软件开发安全管理测评要求》（草案）编制说明

一、工作简况

1、任务来源

本项目为2022年的中关村信息安全测评联盟团体标准制定项目，标准名称为《信息安全技术 网络安全等级保护应用软件开发安全管理测评要求》，中关村信息安全测评联盟的团体标准立项公告文件号为：信安联〔2022〕50号。

2、标准编制的主要成员单位

本项目由公安部信息安全等级保护评估中心牵头，参与起草单位包括昆仑数智科技有限责任公司、深圳开源互联网安全技术有限公司、杭州默安科技有限公司、上海计算机软件技术开发中心、北京神州绿盟科技有限公司等。

3、主要工作过程

1、2021年8月至2021年11月，标准牵头单位及协作单位调动相关技术人员对标准的内容进行预研，分析了国内外相关形势及发展趋势，研究了国内外的相关政策法规及标准，草拟了标准草案的大纲。

2、2021年11月至2022年3月，标准牵头单位及协作单位根据草案大纲完成了编制草案初稿的编制。

3、2022年4月-9月，开展标准编制组内针对标准草案进行多轮讨论和修订。

4、2022年10月，提交了团体标准制修订的立项申请书。

5、2022年10月13日，中关村信息安全测评联盟下发了《关于<信息安全技术 网络安全等级保护应用软件开发安全管理测评要求>团体标准立项的公告》（信安联[2022]50号）。

6、2022年10月-12月，标准编制组对标准草案核心内容进一步完善修改。

7、2023年3月，标准编制组将标准草案稿提交给中关村信息安全测评联盟，召开标准草案专家评审会。

8、2023年4月-5月，标准编制组根据专家意见修行完善修改。

二、标准编制原则和确定主要内容的论据及解决的主要问题

随着信息技术在社会各领域、生活各方面的不断应用，人们对于软件的依赖越来越明显，但软件自身的安全问题导致各类安全漏洞伴随着软件开发过程而产生。如果在软件设计和开发过程注重安全，将会使很多安全问题得到解决。

同时等级保护系列标准之：GB/T 22239-2019和GB/T 28448-2019仅在安全管理要求中对两类开发方式：自行开发和外包开发做出了简明要求，未对应用软件开发整体上做出更加系统化的要求。为进一步明确软件开发过程中的主要安全管理活动，同时将22239-2019中通用安全管理要求中关于软件开发的相关安全管理要求进一步细化和扩展，确保安全因素在开发过程中得以考虑和实施，本标准正是基于以上目的而编制。

1、编制原则

本标准在编制过程中遵循以下原则：

a) 实用性原则

本标准在编制过程中，综合考虑我国目前网络安全工作需要，各类等级保护对象安全开发现状，在充分全面的调研基础上开展，使得标准更贴近实际需要，保证可操作性。

b) 通用性原则

本文件规定了网络安全等级保护第一级至第四级等级保护对象在应用软件开发过程中应遵循的安全要求，适用于各类开发单位、软件采购、使用单位、第三方评估单位等对应用软件开发过程进行监督管理和安全评估。

c) 符合性原则

符合国家有关法律法规和已有标准规范的相关要求。

2、确定主要内容的依据

标准制定的依据为：

a）标准格式按照 GB/T 1.1—2020 标准要求编写。

b）本标准制定参考以下国家标准：

1）GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

2）GB/T 28448-2019 信息安全技术　网络安全等级保护测评要求

3）GB/T 38674-2020 信息安全技术 应用软件安全编程指南

3、标准主要内容

本标准共分为 9 章，其中：

第1、2、3章，为标准的常规性描述，包括范围、规范性引用文件、术语和定义。

第 4 章为概述，描述软件开发周期安全管理框架。该框架主要是由管理对象安全和管理过程安全两大方面构成。其中，管理对象安全主要包括安全管理制度、人员安全管理、环境安全管理、开发工具安全管理等内容；管理过程安全主要遵循应用软件开发周期各个环节(即，需求、设计、开发、测试、发布和交付等环节)提出的安全管理要求。另外，规范了软件安全测评的等级划分。测评等级分为基本级（LB）和增强级(LI)。安全保护等级为第二级及以下的安全保护对象，其应用软件开发过程的安全管理要求参考基本级（LB）管理要求；安全保护等级为第三级及以上的安全保护对象，其应用软件开发过程安全管理要求除基本级管理要求外，还需参考增强级管理要求(LI)。

第 5 章为安全管理要求。从软件开发过程中需遵循的管理要求角度，分别从安全管理制度、安全管理人员、环境安全管理、工具安全管理和开发过程安全控制管理等方面提出要求。其中安全管理制度描述在软件开发过程中需建立、发布并维护各类管理制度、操作规范和表单，确保各项开发管理行为“有法可依、有据可查”。安全管理制度描述开发涉及各类岗位设置、职责明确，任职过程中培训、考核以及离职管理等要求。环境安全管理描述开发环境、测试环境和交付环境等建设过程和日常运维管理。工具安全管理描述工具准入机制建立、工具使用过程管理以及工具终止机制等收回管理。开发过程安全控制管理描述安全需求、安全设计、安全开发、安全测试、安全发布、安全交付等软件开发生命周期各个活动所需考虑的安全要求。

第 6 章为安全测评要求。分别从测评、评估的角度针对第 5 章的安全要求提出各个测评单元实施过程。每个测评单元分别包括：测评指标、测评对象、测评实施和测评结果构成。

三、采用国际标准的程度及水平的简要说明

组织编制组成员学习国际 NIST800 系列关于安全软件开发框架、ISO/IEC27034 等系列标准的核心内容，并力求在本标准中加以考虑，确保相

关内容与现有标准保持一致性。

四、重大分歧意见的处理过程和依据

无

五、其他应予说明的事项

无

《信息安全技术 网络安全等级保护应用软件开发安全管理测评要求》

编制工作组

2023-05-30