ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 29240—2012

# 信息安全技术　终端计算机通用安全技术要求与测试评价方法

**Information security technology—General security technique requirements and testing evaluation method for terminal computer**

2012-12-31 发布　　2013-06-01 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 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/TC 260)提出并归口。

本标准起草单位:公安部计算机信息系统安全产品质量监督检验中心、联想控股有限公司。

本标准主要起草人:邱梓华、韦卫、宋好好、王京旭、张艳、顾健、吴秋新、顾玮、赵婷、宁晓魁、邹春明、张笑笑、俞优、冯荣峰。

# 引　言

本标准包含两部分内容，一部分是终端计算机的通用安全技术要求，用以指导设计者如何设计和实现终端计算机，使其达到信息系统所需安全等级，主要从信息系统安全保护等级划分的角度来说明对终端计算机的通用安全技术要求和测试评价方法，即主要说明终端计算机为实现 GB 17859—1999 中每一个保护等级的安全要求应采取的安全技术措施。本标准将终端计算机划分为五个安全等级，与信息系统的五个等级一一对应。考虑到可信计算是当今终端计算机安全技术主流发展方向，所以在整个终端计算机安全体系设计中凸显可信计算技术理念，特别是在高安全等级（指 3 至 5 级）的安全技术措施设置方面，强调采用基于自主可信计算技术标准的可信计算功能特性，而且我国主流终端计算机厂商已建立起相关产业环境，因此，本标准的技术路线选择能够适应我国终端计算机安全技术产业发展水平；另一部分是依据技术要求，提出了具体的测试评价方法，用以指导评估者对各安全等级的终端计算机评估，同时也对终端计算机的开发者提供指导作用。

本标准部分条款引用了其他标准的内容，有些是直接引用的，有些是间接引用的，对于直接引用的，请参考被引用标准的具体条款。对于间接引用的，以本标准文本的描述为准。

为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，在第 4 章的描述中，每一级的新增部分用**“宋体加粗”**表示。

# 信息安全技术　终端计算机<br>通用安全技术要求与测试评价方法

## 1　范围

本标准按照国家信息安全等级保护的要求，规定了终端计算机的安全技术要求和测试评价方法。

本标准适用于指导终端计算机的设计生产企业、使用单位和信息安全服务机构实施终端计算机等级保护安全技术的设计、实现和评估工作。

## 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—1999　计算机信息系统　安全保护等级划分准则

GB/T 17901.1—1999　信息技术　安全技术　密钥管理　第1部分：框架

GB/T 20271—2006　信息安全技术　信息系统通用安全技术要求

GB/T 20272—2006　信息安全技术　操作系统安全技术要求

## 3　术语和定义、缩略语

### 3.1　术语和定义

GB 17859—1999、GB/T 20271—2006 和 GB/T 20272—2006 界定的以及下列术语和定义适用于本文件。

3.1.1

**终端计算机　terminal computer**

供个人使用的、能独立进行数据处理及提供网络服务访问的计算机系统。

注：终端计算机一般为台式微型计算机系统和便携微型计算机系统两种形态，终端计算机通常由硬件系统、操作系统和应用系统(包括为用户访问网络服务器提供支持的工具软件和其他应用软件)等部分组成。

3.1.2

**完整性度量　integrity measurement**

使用杂凑算法对被度量对象计算其杂凑值的过程。

3.1.3

**完整性度量值　integrity measurement value**

部件被杂凑算法计算后得到的杂凑值。

3.1.4

**完整性基准值　predefined integrity value**

部件在发布时或在可信状态下被度量得到的杂凑值，作为完整性校验的参考基准。

3.1.5

**可信度量根　root of trust for measurement**

一个能够可靠进行完整性度量的计算引擎，是信任传递链的起始点。