ICS 35.030
CCS L 09

DB23

黑 龙 江 省 地 方 标 准

DB23/T XXX—XXXX

平台用户信息保护指南

Guidelines for platform user information protection

(点击此处添加与国际标准一致性程度的标识)

（（征求意见稿））

联系单位：黑龙江省运通科技有限公司

联系人：吕翔宇

联系电话：13936673292

邮箱：sean.lv@foxmail.com

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

黑龙江省市场监督管理　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

平台用户信息保护指南

1 范围

本文件给出了平台用户信息保护的术语和定义、基本原则、管理能力、信息处理过程、相关利益方权益、服务监督、评价与改进相关利益方权益。

本文件适用于指导平台用户信息的保护工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 2887 计算机场地通用规范

GB/T 9361 计算机场地安全要求

GB/T 20985.2 信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

GB/T 20985.1 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理

GB/T 24363 信息安全技术 信息安全应急响应计划规范

GB/T 25069-2010 信息安全技术 术语

GB/T 31167 信息安全技术 云计算服务安全指南

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 31722 信息技术 安全技术 信息安全风险管理

GB/T 34942 信息安全技术 云计算服务安全能力评估方法

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 40652 信息安全技术 恶意软件事件预防和处理指南

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

平台 platform

充分运用互联网和移动技术，构建由数据驱动、平台支撑、网络协同的活动单元，在本质上是市场的具化，是一种虚拟或真实的交易场所。

3.2

用户信息 customer information

基于平台提供的服务，收集用户喜好、用户细分、用户需求、用户联系方式等基本资料信息，主要分为描述类信息、行为类信息和关联类信息。

3.3

最小元素集合 minimum collection

以明确、合理的目的收集与用户直接相关的信息，并确定对用户权益影响最小的要素范围。

注：直接关联是指没有该信息的参与，无法实现功能。

3.4

用户信息主体 subject of personal information

用户信息所标识的自然人、法人和非法人组织。

3.5

用户信息管理者 administrator of personal information

决定用户信息处理的目的和方式，实际控制用户信息并利用信息系统处理用户信息的组织和机构。

3.6

用户信息获得者 receiver of personal information

从信息系统获取用户信息的个人、组织和机构，依据用户信息主体的意愿对获得的用户信息进行处理。

3.7

敏感信息 sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人或组织身心健康、名誉受损或受到歧视性待遇等的信息。

注 1：个人、法人和非法人组织身份证件号码个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 周岁以下(含)儿童的个人信息等。

注 2：法人和非法人组织的商业秘密等。

3.8

用户一般信息 customer general information

除用户敏感信息以外的用户信息。

3.9

用户信息处理 personal information handing

处置用户信息的行为，包括收集、存储、使用、加工、传输、提供、公开、删除等。

3.10

去标识化 de-identification

通过对用户信息的技术处理，使其在不借助额外信息的情况下，无法识别用户信息主体的过程。

3.11

匿名化 anonymization

通过对用户信息的技术处理，使得用户信息主体无法被识别，且处理后的信息不能被复原的过程。

4 基本原则

4.1 总体原则

遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

4.2 目的原则

为实现关联处理目的，以用户信息处理为核心，采取最小元素集合限度的手段。

4.3 公开透明原则

明示用户信息的处理目的、方式和范围，强化用户的主体地位，保障用户的知情权和决定权。

4.4 质量原则

保证用户信息质量的准确性、完整性、时效性，避免因用户信息不准确、不完整对用户权益造成不利影响。

4.5 责任原则

处理者对用户信息处理活动负责，将用户信息安全作为工作重点，并采取必要的保障措施。

5 管理能力

5.1 组织的管理能力

5.1.1 明确用户信息保护管理目标，规划内容和范围，制定信息处理过程管理制度，并对过程管理进行记录。

5.1.2 建立组织结构框架图，规定用户信息管理人员职务或职位，明确各岗位责任。

注 1：公开用户信息保护负责人，包括姓名、联系方式等，并报送履行用户信息保护职责的部门。

注 2：规定的中华人民共和国境外的用户信息处理者，需在中华人民共和国境内设立专门机构或者指定代表，负责处理用户信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行用户信息保护职责的部门。

5.1.3 制定并组织实施用户信息安全事件应急预案。

5.1.4 建立定期评估管理制度，对处理用户信息遵守的法律、行政法规的情况，进行合规审计。

5.1.5 制定岗位培训计划，进行岗前、在岗和离岗管理，定期对从业人员进行安全教育和岗位培训。

注 1：调查和了解从业人员背景，签署保密协议或在劳动合同中设置相应的条款。

注 2：按照管理制度，及时终止离职人员对用户信息的访问权限。

5.1.6 建立用户投诉渠道，用户行使权利方式宜便捷，拒绝用户行使权利请求时，应当说明理由。

5.2 人员的职业能力

5.2.1 能够掌握用户信息安全相关法律、法规、标准、管理制度、岗位职责及保密条款。

5.2.2 能够落实和宣传用户信息保护策略，开展用户信息保护日常管理。

5.2.3 能够执行用户信息保护制度，在授权范围内进行用户信息的处理。

5.2.4 能够分析处理用户信息保护存在的问题，提出风险控制建议和技术改进指导方案。

5.2.5 能够按照国家网信部门要求，监督检查用户信息处理活动全过程。

注：设置专职用户信息保护负责人管理岗位。

5.3 环境的保护条件

5.3.1 建立安全环境保护制度，包括但不限于：物理环境、网络环境、计管机环境和应用环境，宜参考附录 A 的相关标准。

5.3.2 建立用户信息存储相关设备和各类介质安全管理制度，对设备移入或移出保护区域，进行严格的申请和审批管理。

注：介质包括但不限于：磁介质、半导体介质和光介质。

5.3.3 建立机房分区管理制度，设置不同区域，区域之间设置物理隔离装置或隔离标识，在重要区域前设置交付或安装等过渡区。

5.3.4 机房环境安全宜分类保护、多级保护，包括但不限于：增加防盗技术、安装报警设备、布设监控设施、安装空调系统与报警系统联动控制设施、防电磁泄露装置，严格控制静电源、安全可靠及时消除机房的静电、定期对防静电设施进行检测和维护。

5.3.5 建立物理线路安全、物理访问控制、电力供应安全保障制度。

5.3.6 计算机场地基础建设符合 GB/T 2887，计算机场地安全保障符合 GB/T 9361 的相关规定。

5.3.7 制定应用环境运行管理制度，包括但不限于：测评机构、设备供应商、电信运营商、外来参观人员。

6 信息处理过程

6.1 收集

6.1.1 概述

履行用户信息收集管理制度，明确用户信息收集目的、范围、方法手段、处理方式等内容，保障用户信息的质量和准确性。宜采取显著标注的方式、清晰易懂的语言，真实、准确、完整地告知用户，并在充分知情的前提下使用户自愿、明确地作出单独同意。

6.1.2 收集目的

基于为用户提供服务、与用户建立联系、改善服务质量等目的收集和使用用户信息。

注：提示用户提供用户信息后可能存在的风险，以及不提供用户信息可能出现的后果。

6.1.3 收集范围

收集范围包括用户信息和用户敏感信息，用户信息包括以电子或者其他方式记录的已识别或者可识别的个人、法人和非法人组织有关的各种信息，不包括匿名化处理的信息。用户敏感信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息。

注 1：用户敏感信息一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。

注 2：收集未成年人用户信息前，需征得未成年人或其监护人的明示同意，未满 14 周岁的，需征得其监护人的明示同意。

6.1.4 方法手段

信息收集前，确认数据来源的合法性，保存期限以实现处理目的所必要的最短时间。采取最小元素集合确定收集内容，仅采用已告知的技术手段收集用户信息，不采取隐藏的技术手段收集用户信息。在公共环境下，收集用户信息的客户端采用隐蔽去标识化处理的输入方式。

注：如果是通过交易得来的数据，明确交易对象和过程的合法性。

6.1.5 处理方式

宜按照收集目的，立即对收集的用户信息进行去标识化处理，不对用户信息进行其他不相关的处理。未经用户信息处理者同意，受托人不得转委托他人处理用户信息。对用户信息的处理采取相应技术管理措施，保障用户信息的安全。

6.2 存储

6.2.1 概述

履行用户信息存储管理制度，对信息系统用户进行分类管理，建立用户分类清单，明确用户信息存储的信息存储时限、原始信息存储、敏感信息存储、境内存储、停止运营存储、存储安全等内容，保障用户信息的存储安全。

6.2.2 信息存储时限

基于实现用户信息授权使用的目的，明确用户信息存储期限所必需的最短时间，超出约定存储期限后,采取删除或匿名化处理。

注：法律法规另有规定或者用户另行授权同意的除外。

6.2.3 原始信息存储

单独存储用户的原始信息，加强访问和使用的权限管理，保证收集的用户信息不被其他设备或程序非授权获取或篡改。

注：个人生物识别信息要与个人身份信息分开存储，宜通过存储个人性别信息的摘要信息，在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；在使用面部识别特征、 指纹、掌纹、虹膜等实现识别身份、认证等功能后，删除可提取个人生物识别信息的原始图像。

6.2.4 敏感信息存储

明确访问权限，对非存储区域暂存的敏感信息，进行加密处理，使用后立即清除。信息系统或云计算系统中存储敏感信息，必要时采用加密的方式存储，并通过有效的技术措施保证存储过程中敏感信息不被非授权获取。

6.2.5 境内存储

关键信息基础设施运营者和处理用户信息达到国家网信部门规定数量的用户信息处理者,需将在中华人民共和国境内收集和产生的用户信息存储在境内。

6.2.6 停止运营存储

当用户信息处理者停止运营其产品或服务时,停止收集用户更新的信息，对其所持有的用户信息进行删除或匿名化处理，并将停止运营的通知进行公告或逐一送达用户。

6.2.7 存储安全

将用户信息保护管理纳入安全风险管理制度，定期对采集、处理、存储用户信息的主机和终端进行安全防护系统更新升级、安全漏洞扫描和安全配置检查,并建立用户信息保护检查评估机制和工作流程，及时发现、修补和评估用户信息保护工作中存在的问题、漏洞及风险。

6.3 使用

6.3.1 概述

履行用户信息使用管理制度，明确用户信息使用的密码管理、访问设置、账号管理、登录控制、主动推送等内容，保障用户登录安全。宜采取的验证手段，包括但不限于密码、令牌（如证书等）、生物特征。

6.3.2 密码管理

建立符合国家密码管理规定的密码技术使用制度，对密码进行加密保护，密码明文不得以任何形式出现，用户密码宜由数字或字符共同组成，长度不少于 6 位。重置用户密码前必须对用户身份进行核实。宜引导用户定期更改登录密码，修改周期不宜超过 90 天。

6.3.3 访问设置

建立用户口令保护制度，对主机、计算机终端、网络安全设备和应用系统用户口令的长度、复杂度、修改周期进行规定，不易采取空口令、弱口令登录。

6.3.4 账号管理

实施审批手续，严格管理用户账户添加、修改或删除操作的权限，对连续 90 天未使用的账号予以权限冻结，冻结后 30 天仍未使用的，予以注销。

6.3.5 登录控制

设定用户登录服务器连续失败次数（宜为 3 次-5 次），在用户账号冻结后，宜经系统管理员对用户身份进行验证，通过后予以恢复。宜设置无操作登录时间上限，超时后需重新登录并验证其身份。

6.3.6 主动推介

通过自动化决策方式向用户进行信息推送、商业营销，不宜针对其用户特征设置选项，同时提供便捷的拒绝方式。

6.4 加工

6.4.1 概述

履行用户信息加工管理制度，明确加工用户信息的自动化决策分析、敏感信息处理、监督加工记录等内容，保障用户信息处理预期目标的完成。

6.4.2 自动化决策分析

用户信息处理者利用用户信息进行自动化决策分析，保证决策的透明度和结果的公平、公正性。

6.4.3 敏感信息处理

处理敏感用户信息前需告知处理敏感用户信息的必要性，并取得用户的单独授权，在符合有关法律法规的要求、相关政府主管部门的要求、满足社会公众利益的需求、维护用户合法权益的前提下，采取严格的保护措施，处理用户的敏感信息。

注：在法律、行政法规规定处理敏感用户信息时，取得书面同意的除外。

6.4.4 监督加工记录

采取有效监督措施，进行监控、跟踪和审计，建立相关的日志、记录档案，及时发现问题并进行处理。

6.4.5 委托加工处理

参考 GB/T 35273 的要求。

6.4.6 安全事件处理

参考 GB/T 35273 的要求。

6.5 传输

6.5.1 概述

履行用户信息传输管理制度，明确传输用户信息前征得用户同意、请求转移用户信息、评估安全风险、信息传输完整、平台主体变更等内容，保障用户信息的质量和准确性。宜采取显著标注的方式、清晰易懂的语言，真实、准确、完整地告知用户，并在充分知情的前提下使用户自愿、明确地作出单独同意。

6.5.2 征得用户同意

采用明确、合法的手段，告知并征得用户同意，在用户信息收集目的范围内传输用户信息，保证用户信息的安全。

6.5.3 请求转移用户信息

用户请求将用户信息转移至其指定的用户信息处理者，符合国家网信部门规定条件的，用户信息处理者应当提供转移的途径。

6.5.4 评估安全与风险

制定安全风险评估制度，明确传输过程中可能存在的风险及相关责任，保证用户信息在转移过程中的保密性、完整性和准确性，采取加密算法，实现数据加密或协议加密，防止用户信息在传输过程中被非授权获取。

注：用户敏感信息中的个人身份信息在发送至客户端之前，采用匿名处理的方式，可采用屏蔽个人身份信息中不可猜测的部分，并使用统一的符号替代。

6.5.5 信息传输的完整

对传输中的用户信息数据进行完整性保护，包括但不限于，完整性检测、必要的完整性恢复等。

6.5.6 平台主体变更

用户信息处理者因合并、分立、解散、被宣告破产等原因需要转移用户信息的，需向用户告知接收方的名称或者姓名和联系方式。接收方应当继续履行用户信息处理者的义务。接收方变更原先的处理目的、处理方式的，需重新取得用户同意。

6.6 提供

6.6.1 概述

建立用户信息提供管理制度，明确自动化决策推送、向境内外用户信提供信息等内容，确保用户的权益。

6.6.2 自动化决策推送

通过自动化决策方式向用户进行信息推送、商业营销，同时提供不针对其用户特征的选项，或者向用户提供便捷的拒绝方式。

6.6.3 向境外提供信息

用户信息处理者向中华人民共和国境外提供用户信息的，需通过国家网信部门组织的安全评估。告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、用户信息的种类以及用户向境外接收方行使权利的方式和程序等事项，并取得用户的单独同意。

6.7 公开

6.7.1 概述

履行用户信息公开管理制度，明确安全评估、记录与存储、法律风险、禁止公开等内容，确保告知用户公开目的、公开类型、是否涉及敏感信息，并事先征得用户明示同意。

6.7.2 安全评估

开展用户信息安全影响评估是公开用户信息的前提，依据安全影响评估结果采取有效的保护措施。

6.7.3 记录与存储

准确记录用户信息的公开披露情况，包括但不限于：公开披露的日期、规模、目的、公开范周等。

6.7.4 法律风险

承担因公开披露用户信息对用户合法权益造成损害的相应责任。

6.7.5 禁止公开

禁止公开披露个人生物识别信息，禁止公开披露公民的种族、民族、政治观点、宗教信仰等用户敏感数据的分析结果。

6.8 删除

6.8.1 概述

履行用户信息删除或销毁管理制度，明确监督销毁记录、用户信息返还、部分信息保留、违法违约转让、代位权行使等内容，确保使用完毕或保存到期的用户信息得到及时、有效、完全的清除或删除，保证用户信息不可恢复。

注：信息载体包括但不限于：报废设备、纸介质、磁介质、半导体介质和光介质。

6.8.2 监督销毁记录

采取有效监督措施，宜分类销毁用户信息，销毁前确保获得相应的授权，建立销毁登记记录，记录内容包括但不限于：使用人、用途、销毁方式与时问、销毁人签字、监督人签字。

6.8.3 用户信息返还

基于用户同意处理的用户信息，用户有权撤回其同意。用户信息处理者需提供便捷的撤回同意方式。当委托合同不生效、无效、被撤销或者终止的，受托人应当将用户信息返还用户信息处理者或者予以删除，不得保留。

6.8.4 部分信息保留

用户信息使用目的后完成后或留存期限到期时，宜立即删除或销毁相关信息，如留存使用，需去标识化，涉及用户敏感信息留存的用户信息处理者，需获得用户信息主体的明示同意。

6.8.5 违法违约转让

用户信息主体对违反法律法规规定或违反与用户信息主体的约定向第三方共享、转让其用户信息的，可要求用户信息控制者停止共享、转让、删除用户信息。

6.8.6 代位权行使

自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关用户信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

7 相关利益方权益

7.1 注册用户

保障用户对其用户信息的处理享有知情权、决定权，包括但不限于：

——用户有权要求用户信息处理者对其用户信息处理规则进行解释说明；

——用户有权向用户信息处理者访问、查阅、复制其用户信息；

——用户发现其用户信息不准确或者不完整的，有权请求用户信息处理者更正、补充；

——用户有权限制或者拒绝平台对其用户信息进行处理；

——用户有权请求将用户信息转移至其指定的用户信息处理者；

——用户在用户信息处理者向第三方传递或变更其用户信息时，有表决权、撤销权；

——用户有权请求删除用户信息，享有撤回同意权；

——用户信息主体权益受到侵害时追究法律责任的权力。

7.2 用户合同委托

通过合同等方式规定受委托者的责任和义务，包括但不限于：

——对受委托者进行审计；

——准确记录和存储委托处理用户信息的情况；

——发现受委托者未按照委托要求处理个人信息，或未能有效履行，宜立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施控制或消除用户信息面临的安全风险，必要时可终止与受委托者的业务关系，并要求受委托者及时删除从用户信息控制者获得的用户信息。

7.3 用户信息处理者

用户信息处理者公布的事项，包括但不限于：

——用户信息处理者的名称或者姓名和联系方式；

——用户信息的处理目的、处理方式，公开，并且便于查阅和保存；

——处理的用户信息种类、保存期限；
——用户行使本法规定权利的方式和程序；
——用户信息主体的投诉渠道和应急机制；
——用户信息侵害可能导致的实质损害及解决办法。

7.4 第三方用户信息处理者

由两个以上的用户信息处理者共同处理用户信息，应明确用户信息处理的目的和处理方式的，约定各自的权利和义务，包括但不限于：
——建立第三方产品或服务接人管理机制和工作流程；
——与第三方产品或服务提供者通过合同等形式明确双方的安全责任；
——收集、改变用户信息前，征得用户的授权同意，做好管理记录，确保可供相关方查阅；
——其他事项按照用户信息处理者的要求履行。

7.5 采用云计算部署处理信息者

采用云计算部署信息系统的，包括但不限于：
——宜采用 GB / T 31168 和 GB / T 31167 的内容，保证不对信息系统的用户信息进行转存、读取、分析和外泄；
——定期对信息系统进行安全检查和风险评估，宜采用 GB/T 34942 提供的方法；
——建立用户信息保护安全事件报告和通报机制，宜采用 GB/T 24363、GB/T 31722 的内容；
——提高组织用户信息保护的安全预防和预警能力，宜采用 GB/T 20985.1、GB/T 20985.2、GB/T 40652 的内容。

8 服务监督、评价与改进

8.1 服务监督

建立用户信息处理者信息公开制定,做到公示信息及时更新,维护服务用户的知情权和监督权,依法保护服务对象的隐私权，向用户公示的事项，包括但不限于：
——用户信息处理者的名称或者姓名和联系方式；
——用户信息的处理目的、处理方式；
——处理的用户信息种类、保存期限；
——用户行使自身权利的方式和程序；
——用户信息主体的投诉渠道和应急机制；
——用户信息侵害可能导致的实质损害及解决办法。

8.2 服务评价

采取内部评价和外部评价相结合,开展满意度测评，包括但不限于：
——基于用户体验，评价用户信息的处理目的、处理方式等是否合法、正当、必要；
——基于管理能力，评价管理组织、人员、环境是否存在制定缺失、管理不到位、合规风险的问题；
——基于流程管理，评价各流程中可能对用户权益的影响及安全风险；
——基于技术保障，评价现有技术是否满足用户保护需求。

8.3 服务改进

注重服务质量的持续改进，包括但不限于：

——建立平台用户信息管理制度，明确用户信息收集、存储、使用、加工、传输、提供、公开、删除的管理流程；

——建立审计制定，定期开展内部或外部审计，并根据审计结果持续改善流程，完善相关制度；

——建立应急响应机制，形成应急预案，并定期演练，以有效应对用户信息保护安全事件。

附 录 A
（资料性）
安全环境相关标准

A.1 安全环境相关标准

表 1 给出了安全环境的相关标准，在使用的过程中，宜考虑标准的修订和废止，及在体系中的增加。

标准号	标准名称	ICS	CCS
GB 4943.23-2012	信息技术设备安全 第 23 部分：大型数据存储设备	35.020	L 09
GB/T 17903.2-2021	信息技术 安全技术 抗抵赖 第 2 部分：采用对称技术的机制	35.040	L 80
GB/T 17903.3-2008	信息技术 安全技术 抗抵赖 第 3 部分: 采用非对称技术的机制	35.040	L 80
GB/T 20009-2019	信息安全技术 数据库管理系统安全评估准则	35.020	L 09
GB/T 20261-2020	信息安全技术 系统安全工程 能力成熟度模型	35.040	L 80
GB/T 20273-2019	信息安全技术 数据库管理系统安全技术要求	35.040	L 80
GB/T 20275-2021	信息安全技术 网络入侵检测系统技术要求和测试评价方法	35.030	L 80
GB/T 20277-2015	信息安全技术 网络和终端隔离产品测试评价方法	35.040	L 80
GB/T 20278-2022	信息安全技术 网络脆弱性扫描产品安全技术要求和测试评价方法	35.040	L 80
GB/T 20281-2020	信息安全技术 防火墙安全技术要求和测试评价方法	35.030	L 80
GB/T 21050-2019	信息安全技术 网络交换机安全技术要求	35.040	L 80
GB/T 21052-2007	信息安全技术 信息系统物理安全技术要求	35.040	L 80
GB/T 22239-2019	信息安全技术 网络安全等级保护基本要求	35.040	L 80
GB/T 28450-2020	信息技术 安全技术 信息安全管理体系审核指南	35.040	L 80
GB/T 28454-2020	信息技术 安全技术 信息安全管理体系审核指南	35.040	L 80
GB/T 28458-2020	信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作	35.040	L 80
GB/T 30276-2020	信息安全技术 网络安全漏洞标识与描述规范	35.040	L 80
GB/Z 32906-2016	信息安全技术 网络安全漏洞管理规范	35.040	L 80
GB/T 34978-2017	信息安全技术 中小电子商务企业信息安全建设指南	35.040	L 80
GB/T 34990-2017	信息安全技术 移动智能终端个人信息保护技术要求	35.040	L 80
GB/T 36618-2018	信息安全技术 信息系统安全管理平台技术要求和测试评价方法	35.040	L 80
GB/T 37939-2019	信息安全技术 网络存储安全技术要求	35.040	L 80
GB/T 37988-2019	信息安全技术 数据安全能力成熟度模型	35.040	L 80
GB/T 37964-2019	信息安全技术 个人信息去标识化指南	35.040	L 80
GB/T 40653-2021	信息安全技术 安全处理器技术要求	35.030	L 80
GB/T 40660-2021	信息安全技术 生物特征识别信息保护基本要求	35.030	L 80

参 考 文 献

[1] GB 4943.23-2012 信息技术设备 安全 第23部分：大型数据存储设备
[2] GB/T 17903.2-2021 信息技术 安全技术 抗抵赖 第2部分：采用对称技术的机制
[3] GB/T 17903.3-2008 信息技术 安全技术 抗抵赖 第3部分：采用非对称技术的机制
[4] GB/T 20009-2019 信息安全技术 数据库管理系统安全评估准则
[5] GB/T 20261-2020 信息安全技术 系统安全工程 能力成熟度模型
[6] GB/T 20273-2019 信息安全技术 数据库管理系统安全技术要求
[7] GB/T 20275-2021 信息安全技术 网络入侵检测系统技术要求和测试评价方法
[8] GB/T 20277-2015 信息安全技术 网络和终端隔离产品测试评价方法
[9] GB/T 20278-2022 信息安全技术 网络脆弱性扫描产品安全技术要求和测试评价方法
[10] GB/T 20281-2020 信息安全技术 防火墙安全技术要求和测试评价方法
[11] GB/T 21050-2019 信息安全技术 网络交换机安全技术要求
[12] GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求
[13] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[14] GB/T 28450-2020 信息技术 安全技术 信息安全管理体系审核指南
[15] GB/T 28454-2020 信息技术 安全技术 信息安全管理体系审核指南
[16] GB/T 28458-2020 信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作
[17] GB/T 30276-2020 信息安全技术 网络安全漏洞标识与描述规范
[18] GB/Z 32906-2016 信息安全技术 网络安全漏洞管理规范
[19] GB/T 34978-2017 信息安全技术 中小电子商务企业信息安全建设指南
[20] GB/T 34990-2017 信息安全技术 移动智能终端个人信息保护技术要求
[21] GB/T 36618-2018 信息安全技术 信息系统安全管理平台技术要求和测试评价方法
[22] GB/T 37939-2019 信息安全技术 网络存储安全技术要求
[23] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[24] GB/T 37964-2019 信息安全技术 个人信息去标识化指南
[25] GB/T 40653-2021 信息安全技术 安全处理器技术要求
[26] GB/T 40660-2021 信息安全技术 生物特征识别信息保护基本要求
[27] 《中华人民共和国刑法修正案（九）》，2015
[28] 《中华人民共和国网络安全法》，2016
[29] 《中华人民共和国电子商务法》，2019
[30] 《全国人民代表大会常务委员会关于加强网络信息保护的决定》，2012
[31] 《国务院关于大力推进信息化发展和切实保障信息安全的若干意见（国发（2012）23号）》，2012
[32] 《电信和互联网用户个人信息保护规定（工业和信息化部令第24号）》，2013
[33] 《最高人民法院关于审理网络消费纠纷案件适用法律若干问题的规定（一）》，2022
[34] 《中华人民共和国计算机信息系统安全保护条例（国务院令第147号）》，1994
[35] 《中华人民共和国计算机信息网络国际联网管理暂行规定（国务院令第195号）》，1996
[36] 《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法（国信（1998）003号）》，1998