03.100
A 02

团 体 标 准

T/ISC 0023—2023

信息通信及互联网行业企业合规管理体系 指南

Guidelines for Compliance Management System of Information and Communicational and Internet Enterprises

（发布稿）

2023-03-02 发布　　2023-03-02 实施

中 国 互 联 网 协 会　　发 布

目　录

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》给出的规则起草。

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这些专利的责任。

本文件中使用的任何商品名称均为方便用户而提供的信息，不构成背书。

本文件由中国互联网协会提出并归口。

本文件主要起草单位：中国信息通信研究院、小米科技有限责任公司、华为技术有限公司、北京百度网讯科技有限公司、OPPO广东移动通信有限公司、北京抖音信息服务有限公司、蚂蚁科技集团股份有限公司、阿里巴巴集团控股有限公司、北京新浪互联信息服务有限公司、中国搜索信息科技股份有限公司、奇安信科技集团股份有限公司、恒生电子股份有限公司、科大讯飞股份有限公司、宜信惠民投资管理(北京)有限公司、北京快手科技有限公司、紫光展锐（上海）科技有限公司、北京京东叁佰陆拾度电子商务有限公司、维沃移动通信有限公司、厦门市美亚柏科信息股份有限公司、北京蜜莱坞网络科技有限公司、竞技世界（北京）网络技术有限公司、北京来也网络科技有限公司、北京小桔科技有限公司、广东移动通信有限公司。

本文件主要起草人：李文宇、张夕夜、林中天、陈慧、赵湘旻、曾令国、张朗、吴昊、游朋、孔宇杰、包达、杜剑波、何煜炜、冯雨柔、史金城、江松燊、李昳婧、王洁、吴斌、杨妮、顾伟、鲁艳、胡海娜、白雅喜、崔倩倩、朱希琳、马兰、安锦程、章燕燕、何永春、刘颖、陈彦文、赵洋、李硕、仇寿霞、游涛、李梦雪、邱福恩、田喜清、陈一夫、刘文园、赵帅、马可、何佳、徐迪、黄原娇、高俊林、宋基星、范思睿、谷元坤、吴少卿、王玺龙、许如清、王圣宇、周开辰、李美欣、张贝贝、曹苓、杨扬、王志强、张向拓、黄河清、刘艳霞、赵永飞、吴彬、王子坤、魏妍妍、任媛媛、陈滢滢、楚赟、刘宇、董雪、沈晓东、李瑛、华爽、汪海伦、秦思思、王瑛、欧阳邓亚、王娇妮、潘景燕、范艳伟、李倩、丁雪萍、黄翀、李晓红、卢敏聪、宋大鹏、李媛、郝敏、关昊昕、范琦。

引　言

合规不仅是成功和可持续企业的基础，也是企业发展的机遇。企业的长期成功发展需要建立并维护合规文化，同时考虑相关方的需求和期望。

有效的企业合规管理体系，能够表明企业在经营管理过程中遵守相关法律法规、政府监管要求、行业守则、良好的治理标准、社会一般道德和对期望的承诺。

企业合规，是由领导运用核心价值观以及被普遍认可的优秀治理方法、道德和相关标准共同构建的。将合规融入企业工作人员的行为，依赖于各层级的领导力和企业清晰的价值观，以及承认和实施促进合规的措施。如果不能保证企业各级都符合上述标准，则可能存在合规风险和违规行为的风险。

当前，我国已进入高质量发展阶段，企业是新时代构建新发展新格局的生力军。合规管理，是企业积极应对不断变化的内、外部环境，传统与非传统风险的有效途径，也是主动适应并推进国家经济发展方式、结构转型优化的重要举措。

为响应党和国家的政策要求，加快提升互联网行业企业依法合规经营管理水平，助力互联网行业企业高质量全面发展，根据《中央企业合规管理办法》、《企业境外经营合规管理指引》、ISO 37301：2021《合规管理体系 要求及使用指南》及相关法律法规、标准要求，结合互联网行业企业的实际情况，特制定本文件。

本文件中的要求和指南均可调整。根据企业合规管理体系的规模、成熟度，以及企业的活动和目标的背景、性质和复杂性，实施方式可以有所不同。

信息通信及互联网行业企业合规管理体系 指南

1 范围

本文件规定了信息通信及互联网企业建立、实施、评估、维护及改进合规管理体系的总体指南。本文件适用于开展合规管理相关工作的信息通信及互联网企业。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

合规 compliance

企业及其员工的经营管理行为符合法律法规、政府监管规定、行业准则和企业章程、规章制度以及国际条约、规则、商业道德规范和社会责任等要求。

3.2

合规风险 compliance risk

企业及其员工因不合规行为，引发法律责任、受到相关处罚、造成经济或声誉损失及其他负面影响的可能性。

3.3

合规管理 compliance management

以有效防控合规风险为目的，开展包括体系构建、制度制定、风险识别、合规审查、风险应对、责任追究、考核评价、合规培训等有组织、有计划的管理活动。

4 合规原则

4.1 全面性原则

企业合规管理活动应覆盖企业的所有业务领域、各业务部门、各级子企业和各分支机构、全体员工，贯穿决策、执行、监督、反馈等各个环节，体现于决策机制、内部控制、业务流程等各个方面。

4.2 有效性原则

合规管理制度应有效嵌入到经营业务的重点领域和关键环节当中，与法务、审计监察、内控等工作相统筹，建立相应责任制，有效化解合规风险，监督并确保合规管理体系有效运行。

4.3 独立性原则

企业合规管理应从组织机构设置、制度设计、汇报路径等方面保证独立性，不受其他部门和人员的干涉。

4.4 动态性原则

企业合规管理需与企业经营范围、组织结构和业务规模相适应；根据企业内外部环境的变化适时进行调整和完善；企业经营管理中存在的合规风险问题，能够得到及时反馈、纠正和改进。

4.5 可查证原则

企业合规遵循明确的流程规范，以合适的形式对合规管理进行记录留存，确保企业合规管理有迹可循、有证可查。

5 合规管理组织体系

5.1 组织体系设立原则

5.1.1 设计科学，权责对等

合规管理组织体系的设计，应做到科学合理、权责一致。力求做到机构不重叠、职能不缺位，避免职责不明、义务履行推诿缺位及运行效率低下等情况发生。

5.1.2 合理高效，运转协调

合规管理组织体系设计，宜综合考虑企业发展战略、管理定位、运营特点、业务范围、员工情况等因素，结合企业全面风险管理及合规管理现状，构建合理高效、运转协调的组织体系。

5.2 组织体系与职责

5.2.1 组织体系

合规管理组织体系由企业决策层、管理层与执行层共同组成：

决策层以保障企业合规经营为目的，进行顶层设计，优化企业合规管理中的权力资源配置问题；

管理层确保分配充足的资源，建立、制定、实施、评价、维护和改进企业的合规管理体系；

执行层遵守合规管理要求，改进合规管理措施，执行合规管理制度和程序，落实相关合规管理工作。

企业可以根据业务规模、合规风险等因素组建合规管理队伍，设置由合规管理委员会、合规管理负责人和合规管理牵头部门组成的合规管理组织体系。

5.2.2 董事会

董事会的合规管理主要职责包括：

a）批准企业合规管理的整体规划、基本制度和年度报告；

b）推动完善合规管理体系；

c）决定合规管理负责人的任免；

d）决定合规管理牵头部门的设置和职能；

e）研究决定合规管理的有关重大事项；

f）按照权限决定有关违规人员的处理事项。

5.2.3 监事会

监事会的合规管理主要职责包括：

a）监督董事会的工作决策与流程是否合规；
b）监督董事和高级管理人员合规管理职责履行情况；
c）对引发重大合规风险负有主要责任的董事、高级管理人员提出罢免建议；
d）向董事会提出撤换合规管理责任人的建议。

5.2.4 经理层

经理层的合规管理主要职责包括：
a）根据董事会决定，建立健全合规管理组织架构；
b）批准合规管理具体制度规定；
c）批准合规管理计划，采取措施确保合规制度得到有效执行；
d）明确合规管理流程，确保合规要求融入业务领域；
e）及时制止并纠正不合规的经营行为，按照权限对违规人员进行责任追究或提出处理意见；
f）经董事会授权的其他事项。

5.2.5 合规管理委员会

设立合规管理委员会，负责合规管理的组织领导和统筹协调工作，主要职责包括：
a）规划合规管理体系建设工作；
b）听取合规管理工作汇报；
c）研究合规管理重大事项并提出指导意见；
d）指导、监督及评价合规管理工作；
e）统筹协调重大合规风险事件的处理；
f）其他重大事项。

合规管理委员会，可与企业法治建设领导小组等相关机构合署。

5.2.6 合规管理负责人

合规管理负责人，可以由企业相关负责人、总法律顾问或者首席合规官担任。其主要职责包括：
a）贯彻执行合规管理委员会、决策层对合规管理工作要求，全面负责企业合规管理工作；
b）组织制订合规管理战略规划，参与企业重大决策并提出合规意见；
c）协调合规管理与各业务部门之间关系，监督合规管理工作建设执行情况，解决合规管理工作推进过程中的重大问题；
d）领导合规管理牵头部门开展合规管理工作，加强合规管理队伍建设；
e）组织起草合规管理年度报告；
f）向合规管理委员会、决策层汇报合规管理重大事项。

5.2.7 合规管理牵头部门

企业结合自身情况设置合规管理牵头部门，组织、协调和监督合规管理工作，为其他部门提供合规支持。其主要职责包括：
a）负责企业合规管理体系建设，制定企业合规管理建设规划和实施方案；
b）组织制定、修订企业合规管理基本制度和具体制度，总结梳理合规管理相关工作标准程序；
c）制订年度合规管理工作计划，并推动合规管理工作贯彻落实，组织编报合规管理年度报告；
d）持续关注重大法律法规等变化，组织协调重点领域合规风险评估工作；
e）组织协调开展专项合规工作，参与重大事项决策、重要规章制度、重大合同的法律合规审查；

f）设定合规培训计划指标，组织或协助业务单位、人力资源部门、培训部门开展合规培训；
g）组织开展合规检查工作，督促违规整改和持续改进，参与违规事件处置；
h）组织或参与企业合规管理考核、评价工作；
i）指导所属企业开展合规管理工作；
j）参与合规管理工作经费预算审核与统筹。

5.2.8 业务部门

业务部门负责本领域的日常合规管理工作。其主要合规管理职责包括：
a）主动开展并配合合规管理牵头部门开展合规工作，按照合规要求完善业务管理制度和流程；
b）组织或配合合规管理牵头部门进行合规风险识别和隐患排查，及时向合规管理牵头部门通报风险事项，妥善应对合规风险事件；
c）做好本领域合规培训和商业伙伴合规尽职调查工作；
d）组织或配合违规调查及整改工作。

5.3 合规管理沟通与协作

建立紧密结合、协同联动的合规管理机制，发挥合规防护、监督作用，降低合规风险。有效的企业合规管理沟通与协作包括：
a）各职能管理部门与各业务部门，对其职责范围内的合规管理工作负直接责任；
b）合规管理牵头部门，主要履行组织、协调和监督合规管理工作等职责；
c）审计、内控、纪检监察等部门，主要履行合规管理监督职责。

6 合规风险评估与应对

6.1 合规风险评估目的

合规风险评估是识别企业内部合规风险，制定企业行为守则和构建企业合规管理体系的前提与基础。信息通信及互联网企业应在进行合规管理活动过程中开展企业内部的合规风险评估活动。

6.2 合规风险评估团队组建

合规风险评估活动由合规管理牵头部门负责统筹，合规风险评估团队成员宜涵盖牵头部门和协同部门等专业人员，从企业经营管理活动的各个领域和各个环节展开合规风险评估活动。

为增强评估的客观性、独立性，不具备条件和能力的企业可以聘请中立、专业的合规风险评估团队进行合规风险评估。

6.3 风险识别

针对企业合规管理重点，建立具体的合规风险评估流程。

统筹组织合规风险评估团队识别企业合规义务，进行企业合规风险评估，并详细记录合规风险评估的过程和结果。

6.4 合规风险应对

针对发现的风险，制定预案，采取有效措施，及时应对处置。对于重大合规风险事件，由合规管理负责人或合规管理职能部门及时向合规管理委员会、决策层逐级汇报。合规管理委员会统筹领导，合规管理负责人履行职能，相关部门协调配合，共同提出风险管理改进措施，最大限度化解风险，降低损失。

6.5 合规风险评估周期

企业应定期进行有效的合规风险评估活动。

在企业进入新市场、重大资产重组、合并和收购等重大事件发生时，应在企业内部开展合规风险评估活动。

7 信息通信及互联网企业合规管理重点

7.1 合规管理重点领域

7.1.1 合规管理重点领域整体要求

企业在开展重点领域合规管理活动时，应遵守我国相关法律法规及监管规定；涉及境外经营活动的，应遵守项目所在国相关法律法规、监管规定及国际规则。

7.1.2 采购管理

7.1.2.1 采购合规概述

7.1.2.1.1 相关术语概念及其定义

a) 采购：指企业作为需求方，在一定条件下从第三方处有偿取得货物、工程和服务的行为（货物、工程和服务，下文统称为“产品”）。
b) 采购合规：指在企业内部，执行相关法律法规，制定相关采购制度、流程，加强成本管理、供应商管理、合同管理，以防控采购中的各类风险。

7.1.2.1.2 相关主要依据

a) 《中华人民共和国民法典》
b) 《中华人民共和国政府采购法》
c) 《中华人民共和国招标投标法》
d) 《中华人民共和国招标投标法实施条例》
e) 《中华人民共和国政府采购法实施条例》

7.1.2.2 主要合规风险点

a) 供应商选择不当，可能导致采购物资质次价高，不能供货，或者出现舞弊行为。
b) 本方人员未经授权对外订立采购合同；合同对方的主体资格、履约能力等未达要求；以及合同内容存在重大疏漏或欺诈等情况，导致企业合法权益受到损害。
c) 采购定价机制不科学，采购定价方式选择不当，造成企业资金损失。
d) 缺乏对采购合同履行情况的有效跟踪，运输方式选择不合理以及忽视运输过程风险等问题。
e) 验收标准不明确，验收程序不规范或者对验收中存在的异常情况不作处理，造成提供的货物或服务不能满足采购要求等问题。
f) 付款审核不严格，付款方式不恰当，付款金额管控不严，导致企业资金损失。

7.1.2.3 具体实施措施

7.1.2.3.1 企业采购合规基本原则

采购合规宜遵循依法办事、预防为主、层层把关、跟踪监督、及时调处等原则，以维护企业的合法权益。

7.1.2.3.2 企业采购合规管理部门

企业可设立采购合规管理部门（或岗位），负责依据国家采购、招投标相关政策法规、企业内部相关管理制度要求，组织开展采购相关的规范化管理提升、合法合规监督检查及问题整改工作，以及采购相关的合规管理内控制度、流程的完善与修订。

7.1.2.3.3 企业采购合规管理具体实施措施

a）国家要求必须招投标项目的合规要求

根据《中华人民共和国招标投标法》第三条的规定，国家要求必须招投标的项目（例如，全部或者部分使用国有资金投资或者国家融资的项目），应当采用符合国家要求的招投标方式进行采购。

b）企业自主采购项目的合规建议

- 加强供应商资质审查，建设供应商管理平台、建立统一供应商库、设立供应商入库标准。在与新供应商开展合作时，除对供应商经营资质进行审查、对履约能力及信誉情况进行调查外，可在供应商管理平台对其进行利益冲突报备、关联关系报备、重大纠纷诉讼仲裁或行政处罚报备。关联关系报备包括但不限于董监高及亲属，公司之间、公司员工及亲属持股（直接或者间接持股）等情况。
- 建立供应商黑名单：根据供应商的历史合作情况以及是否存在违法违规、被列为被执行人、重大违约等情况设立供应商黑名单。供应商入库时与库内设置的黑名单库实现自动比对，以触发相关提示，审批流程。
- 建立重大采购项目供应商询价、打分制度：由企业内部的专职采购员统一进行重大采购项目“货比三家”程序，对相关供应商进行统一的类似招标的询价流程，根据供应商提供的报价单等相关文件综合判断供应商的履约能力、匹配度、价格优势，从而选中最优质供应商。为了防止供应商的“串标行为”，可从股权穿透角度判断供应商是否为“关联方”，杜绝“关联方”参加同一个采购项目。

c）合同审查合规重点

- 首先，要审查对方主体是否具备合同签订资格，比如营业执照是否合法存续，经营范围是否与合同交易内容相符合，是否应当取得行政许可资质（包括相关资质是否在有效期内）；其次，要对对方的履约能力、信用情况进行必要评估，以保证签约后能够顺利履行合同。
- 合同中交易标的的名称宜准确、规范；对所购产品或服务的质量标准在合同中宜明确约定；对可明确约定的产品名称、品牌、规格、型号、等级、生产厂家、数量等各项标示，尽量写入合同，以免所交货物不符合采购需求而引发纠纷。
- 为了避免所采购的产品因过期等原因失去原有的使用价值，在采购合同中宜明确约定货物到交货地点后采购人的收货时间，并写明具体、明确的交货地点，以保证货物能够及时签收，避免丢失。
- 合同中宜明确产品单价、计量标准、数量、产品附件等。对于涉外合同，还宜明确货币种类及外汇结算标准，防止出现分歧。
- 合同中须保障采购方在使用采购产品或其任何一部分时不受到第三方关于侵犯专利权、商标权或工业设计权等知识产权的指控。
- 采购合同中的违约责任作为双方无法履行合同时的赔偿方案，核心是违约责任约定清晰、可操作性强。采购合同中如约定定金、违约金以及赔偿金的计算方法等，宜有针对性地设置；对未按期付款或迟延供货，宜约定需承担迟延履行的违约责任，例如，每逾期一日，违约方应当按合同金额支付一定比例的违约金；若未遵守保密条款，宜约定违约方应当支付的违约金金额等。
- 纠纷处理，可首先审查管辖条款是否有效：如果是约定仲裁解决，可仔细核对仲裁机构的名称是否准确；如果是约定法院诉讼解决，可审查管辖地是否与合同有连接点，是否违反级别管辖和专属管辖的规定。其次，需审查管辖条款对采购方是否有利：在采购方比较强势的情况下，可以直接把管辖约定

在采购方所在地；如果采购方相对弱势，可以将管辖条款折中约定，例如，设置为原告所在地法院。

- 审核售后服务承诺，可审查供方在合同中承诺接受问题的响应速度和处理问题的最长等待时间。例如，接到客户投诉后两小时之内予以回复；如需现场维修，可在几天之内安排工作人员上门解决问题等。
- 在审查招投标方式进行的采购合同时，需注意，投标人提交的投标文件，如投标书、开标一览表、分项报价表、供货清单等文件，均对其具有约束力，采购方在与其签订正式采购合同时，可将投标人的投标文件作为合同附件。

7.1.3 网络安全合规

7.1.3.1 网络安全保护概述

7.1.3.1.1 相关术语概念及其定义

网络安全：是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

7.1.3.1.2 相关主要依据

a) 《中华人民共和国网络安全法》
b) 《中华人民共和国个人信息保护法》
c) 《中华人民共和国数据安全法》
d) 《关键信息基础设施安全保护条例》
e) 《网络安全等级保护条例（征求意见稿）》
f) 《网络安全审查办法》
g) 《国家网络安全事件应急预案》
h) 《网络安全威胁信息发布管理办法（征求意见稿）》
i) 《网络安全国家标准应用指南》

7.1.3.2 主要合规风险点

a) 未按照网络安全等级保护制度的要求，履行相关安全保护义务，导致保障网络遭受干扰、破坏或者未经授权的访问，以及网络数据遭到泄露或者被窃取、篡改；
b) 未采取监测、记录网络运行状态、网络安全事件的技术措施，未按照规定留存相关的网络日志不少于六个月；
c) 未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；
d) 网络产品提供者、网络运营者和网络产品安全漏洞收集平台未建立健全网络产品安全漏洞信息接收渠道；
e) 关键信息基础设施运营者未设置专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，或者安全管理机构未履行下列职责：

- 建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；
- 组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；
- 按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；
- 认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；
- 组织网络安全教育、培训；

- 履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；
- 对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；
- 按照规定报告网络安全事件和重要事项。

7.1.3.3 网络安全等级保护

7.1.3.3.1 安全通信网络

a）网络架构

- 保证网络设备的业务处理能力满足业务高峰期需要；
- 保证网络各个部分的带宽满足业务高峰期需要；
- 划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
- 避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
- 提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

b）通信传输

- 可采用密码技术保证通信过程中数据的保密性。
- 可采用校验技术或密码技术保证通信过程中数据的完整性；

7.1.3.3.2 安全区域边界

a）边界防护

- 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
- 应能够对非授权设备私自联到内部网络的行为进行检查或限制；
- 应能够对内部用户非授权联到外部网络的行为进行检查或限制；
- 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

b）访问控制

- 在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
- 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
- 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
- 应能根据会话状态信息为进行数据流提供明确的允许/拒绝访问控制的能力；
- 应对进出网络的数据流实现基于应用协议和应用内容的访问控制；

e）入侵防范

- 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
- 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
- 应采取技术措施对网络行为进行分析、实现对网络攻击特别是新型网络攻击行为的分析；
- 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警；

7.1.3.3.3 安全计算环境

安全计算环境从身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护方面进行安全计算环境防护设计。

a) 身份鉴别

- 可对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
- 可具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
- 当进行远程管理时，可采取必要措施防止鉴别信息在网络传输过程中被窃听；
- 可采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中 一种鉴别技术至少应使用密码技术来实现。

b) 访问控制

- 宜对登录的用户分配账户和权限；
- 宜重命名或删除默认账户，修改默认账户的默认口令；
- 宜及时删除或停用多余的、过期的账户，避免共享账户的存在；
- 宜授予管理用户所需的最小权限，实现管理用户的权限分离；
- 宜由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
- 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
- 宜对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

c) 恶意代码防范

- 在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

d) 安全审计

- 宜启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- 宜对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- 宜对审计进程进行保护，防止未经授权的中断。

e) 入侵防范

- 应遵循最小安装的原则，仅安装需要的组件和应用程序；
- 应关闭不需要的系统服务、默认共享和高危端口；
- 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
- 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
- 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
- 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

f) 恶意代码防范

- 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

g）可信验证

- 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

h）数据完整性

- 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
- 应采用校验技术或密码技术保证重要数据在传送过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

i）数据备份恢复

- 应提供重要数据的本地数据备份与恢复功能；
- 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
- 应提供重要数据处理系统的热冗余，保证系统的高可用性。

j）剩余信息保护

- 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
- 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

7.1.3.4 关键信息基础设施运行安全保护

7.1.3.4.1 网络安全等级保护制度

应落实符合国家网络安全等级保护制度相关要求，开展定级、备案、相应等级的安全建设整改和等级测评工作，相关技术合规要求参见7.1.3.1网络安全等级保护。

7.1.3.4.2 安全管理制度

- 建立适合本组织的网络安全保护计划，结合关键业务链的安全风险报告，明确关键信息基础设施安全保护工作的目标、安全策略、组织架构、管理制度、技术措施等内容，加强机构、编制、人员、经费、装备、工程等资源保障，支撑关键信息基础设施安全保护工作。网络安全保护计划应形成文档并经审批后发布至相关人员。网络安全保护计划应至少每年修订一次，或发生重大变化时进行修订。
- 基于关键业务链、供应链等安全需求建立或完善安全策略和制度，并根据关键信息基础设施面临的安全风险和威胁的变化相应调整。

7.1.3.4.3 安全管理机构

- 运营者应成立指导和管理网络安全工作的委员会或领导小组，由组织主要负责人担任其领导职务，设置专门的网络安全管理机构（以下简称“安全管理机构”），明确机构负责人及岗位，建立并实施网络安全考核及监督问责机制。
- 安全管理机构相关人员应参加国家、行业或业界网络安全相关活动，及时获取网络安全动态，并传达到相关部门及人员。

7.1.3.4.4 安全管理人员

- 对安全管理机构的负责人和关键岗位的人员进行安全背景审查和安全技能考核，符合要求的人员方能上岗，关键岗位包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位。关键岗位应专人负责，并配备 2 人以上共同管理。
- 在上岗前对人员进行安全背景审查，当必要时或人员的身份、安全背景等发生变化时（例如取得非中国国籍）应根据情况重新进行安全背景审查。应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份鉴别相关的软硬件设备，进行离职面谈并通知相关人员或角色。
- 明确从业人员安全保密职责和义务，包括安全职责、奖惩机制、离岗后的脱密期限等。必要时，签订安全保密协议。定期开展基于岗位的网络安全教育培训和技能考核。

7.1.3.4.5 网络安全与信息化同步要求

- 在新建或改建、扩建关键信息基础设施时，充分考虑网络安全因素，在规划、建设和投入使用阶段保证安全措施的有效性，并采取测试、评审、攻防演练等多种形式验证。必要时，可建设关键业务的仿真验证环境。
- 在关键信息基础设施退役废弃时，按照数据安全管理策略对存储的数据进行处理。

7.1.3.4.6 安全运维管理

- 保证关键信息基础设施的运维地点位于中国境内，如确需境外运维，应当符合我国相关规定。
- 应要求维护人员签订安全保密协议。
- 确保优先使用已登记备案的运维工具，如确需使用由维护人员带入关键信息基础设施内部的维护工具，应在使用前通过恶意代码检测等测试。

7.1.3.4.7 检测评估

a) 检测评估制度

- 运营者应建立健全关键信息基础设施安全检测评估制度，包括但不限于检测评估流程、方式方法、周期、人员组织、资金保障等。

b) 检测评估方式和内容

- 自行或者委托网络安全服务机构对关键信息基础设施安全性和可能存在的风险每年至少进行一次检测评估，并及时整改发现的问题。
- 在涉及多个运营者时，定期组织跨运营者的关键信息基础设施安全检测评估，并及时整改发现的问题。
- 在检测评估时，内容包括但不限于网络安全制度（国家和行业相关法律法规政策文件及运营者制定的制度）落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、网络安全等级保护工作落实情况、密码应用安全性评估情况、技术防护情况、云服务安全评估情况、风险评估情况、应急演练情况、攻防演练情况等，尤其关注关键信息基础设施跨系统、跨区域间的信息流动，及其在关键业务流动过程中所经资产的安全防护情况。
- 在新建关键信息基础设施，或关键信息基础设施在改建、扩建中发生重大变化时，自行或者委托网络安全服务机构进行检测评估，分析关键业务链以及关键资产等方面的变更，评估上述变更给关键信息基础设施带来的风险变化情况，并依据风险变化以及发现的安全问题进行有效整改后方可上线。
- 针对特定的业务系统或系统资产，采取不正式告知的、模拟的网络攻击方式检测关键信息基础设施在面对实际网络攻击时的防护和响应能力。

- 在安全风险抽查检测工作中，提供网络安全管理制度、网络拓扑图、重要资产清单、关键业务介绍、网络日志等必要的资料和技术支持，针对抽查检测工作中发现的安全问题和风险进行及时整改。

7.1.3.5 网络安全事件应急预案制度

7.1.3.5.1 网络安全事件处置原则

a) 快速恢复原则。发生需要跨部门协调处置的网络安全事件时，各部门应按照“解决问题优先，程序次之”的原则共同协作，力争快速恢复系统，使损失最小化。

b) 责任制原则。按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的要求，信息系统的业务主管部门、使用部门和运行部门是信息系统协调和处置的直接责任部门，其他直属部门负责人是第一责任人。各部门在处置中做好协调和沟通联系，在分工合作的基础上落实处置工作责任制，确保责任落实。

7.1.3.5.2 网络安全事件分类

a) 有害程序事件（MI）

- 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件。以下为对相关事件的解释说明：
- 计算机病毒事件（CVI）是指蓄意制造、传播计算机病毒，或是因受到计算机病毒影响而导致的信息安全事件。计算机病毒是指编制或者在计算机程序中插入的一组计算机指令或者程序代码，它可以破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制；
- 蠕虫事件（WI）是指蓄意制造、传播蠕虫，或是因受到蠕虫影响而导致的信息安全事件。蠕虫是指除计算机病毒以外，利用信息系统缺陷，通过网络自动复制并传播的有害程序；
- 特洛伊木马事件（THI）是指蓄意制造、传播特洛伊木马程序，或是因受到特洛伊木马程序影响而导致的信息安全事件。特洛伊木马程序是指伪装在信息系统中的一种有害程序，具有控制该信息系统或进行信息窃取等对该信息系统有害的功能；
- 僵尸网络事件（BI）是指利用僵尸工具软件，形成僵尸网络而导致的信息安全事件。僵尸网络是指网络上受到黑客集中控制的一群计算机，它可以被用于伺机发起网络攻击，进行信息窃取或传播木马、蠕虫等其他有害程序；
- 混合攻击程序事件（BAI）是指蓄意制造、传播混合攻击程序，或是因受到混合攻击程序影响而导致的信息安全事件。混合攻击程序是指利用多种方法传播和感染其它系统的有害程序，可能兼有计算机病毒、蠕虫、木马或僵尸网络等多种特征。混合攻击程序事件也可以是一系列有害程序综合作用的结果，例如一个计算机病毒或蠕虫在侵入系统后安装木马程序等；
- 网页内嵌恶意代码事件（WBPI）是指蓄意制造、传播网页内嵌恶意代码，或是因受到网页内嵌恶意代码影响而导致的信息安全事件。网页内嵌恶意代码是指内嵌在网页中，未经允许由浏览器执行，影响信息系统正常运行的有害程序；
- 其它有害程序事件（OMI）是指不能包含在以上 6 个子类之中的有害程序事件。

b) 网络攻击事件（NAI）

- 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。以下为对相关事件的解释说明：
- 拒绝服务攻击事件（DOSAI）是指利用信息系统缺陷、或通过暴力攻击的手段，以大量消耗信息系统的 CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行为目的的信息安全事件；
- 后门攻击事件（BDAI）是指利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门

而对信息系统实施的攻击的信息安全事件；

- 漏洞攻击事件（VAI）是指除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件；
- 网络扫描窃听事件（NSEI）是指利用网络扫描或窃听软件，获取信息系统网络配置、端口、服务、存在的脆弱性等特征而导致的信息安全事件；
- 网络钓鱼事件（PI）是指利用欺骗性的计算机网络技术，使用户泄漏重要信息而导致的信息安全事件。例如，利用欺骗性电子邮件获取用户银行帐号密码等；
- 干扰事件（II）是指通过技术手段对网络进行干扰，或对广播电视有线或无线传输网络进行插播，对卫星广播电视信号非法攻击等导致的信息安全事件；
- 其他网络攻击事件（ONAI）是指不能被包含在以上 6 个子类之中的网络攻击事件。

c) 信息破坏事件（IDI）

- 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件。以下为对相关事件的解释说明：
- 信息篡改事件（IAI）是指未经授权将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件，例如网页篡改等导致的信息安全事件；
- 信息假冒事件（IMI）是指通过假冒他人信息系统收发信息而导致的信息安全事件，例如网页假冒等导致的信息安全事件；
- 信息泄漏事件（ILEI）是指因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者而导致的信息安全事件；
- 信息窃取事件（III）是指未经授权用户利用可能的技术手段恶意主动获取信息系统中信息而导致的信息安全事件；
- 信息丢失事件（ILOI）是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件；
- 其它信息破坏事件（OIDI）是指不能被包含在以上 5 个子类之中的信息破坏事件。

d) 信息内容安全事件（ICSI）

- 信息内容安全事件是指公司对外发布的消息或内容中，包含以下内容的事件：
- 违反宪法和法律、行政法规的内容；
- 针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的内容；
- 组织串连、煽动集会游行的内容；
- 其他造成公司不良影响的内容。

e) 设备设施故障（FF）

- 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障，以下为对相关故障的解释说明：
- 软硬件自身故障（SHF）是指因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的信息安全事件；
- 外围保障设施故障（PSFF）是指由于保障信息系统正常运行所必须的外部设施出现故障而导致的信息安全事件，例如电力故障、外围网络故障等导致的信息安全事件；
- 人为破坏事故（MDA）是指人为蓄意的对保障信息系统正常运行的硬件、软件等实施窃取、破坏造成

的信息安全事件；或由于人为的遗失、误操作以及其他无意行为造成信息系统硬件、软件等遭到破坏，影响信息系统正常运行的信息安全事件；

- 其它设备设施故障（IF-OT）是指不能被包含在以上 3 个子类之中的设备设施故障而导致的信息安全事件。

f）灾害性事件（DI）

- 灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

g）其他事件（OI）

- 其他事件类别是指不能归为以上 6 个基本分类的信息安全事件。

7.1.3.5.3 网络安全事件分级处置流程

a）网络安全事件处理原则

- 网络安全事件的处置以降低或消除事件影响为目标，应避免引发其他事件。如相关处置过程存在可预知风险，需提交网络安全委员会评估。
- 对重大网络安全事件（P2 及以上级别）原因明确，处置措施步骤已事先通过网络安全委员会审核或先行处置可减少公司损失的，网络安全部可先组织开展应急处置，并在事后进行报告。
- 在紧急的信息安全事件处置过程中，如不便召集网络安全委员会成员时，可由网络安全委员会主任进行决策。

b）网络安全事件分类分级

处置等级	事件描述
P1 级	1.公司 50%以上业务和服务因安全原因中断或不可用，或面向客户的业务预计中断 4 小时以上； 2.单次网络安全事件造成公民个人信息泄露超过 5000 条以上； 3.网络安全事件预计会引发集团或集团客户遭受财务或名誉损失超过 500 万或网络安全委员会认定造成非常严重影响； 4.其他网络安全部评估确认并报网络安全委员会核准的事件。
P2 级	1.公司 2 个（含）以上业务和服务因安全原因中断或不可用且影响超过 1000 人，或面向客户的业务预计中断 1 小时以上； 2.单次网络安全事件造成公民个人信息泄露超过 500 条以上； 4.网络安全事件预计会引发集团或集团客户遭受财务或名誉损失超过 50 万或网络安全委员会认定造成较为严重影响； 5.其他网络安全部评估确认并报网络安全委员会核准的事件。
P3 级	1.公司任意业务和服务因安全原因中断或不可用且影响人数超过

	500 人，或 2 个（含）以上业务和服务存在不可用风险； 2.涉及到公司敏感数据的泄露、篡改、伪造、丢失； 3.网络安全事件预计会引发集团或集团客户遭受财务或名誉损失超过 10 万或网络安全委员会认定造成严重影响； 4.其他网络安全部评估确认并报网络安全委员会核准的事件。
P4 级	1.公司任意业务和服务存在因安全原因中断或不可用风险； 2.涉及到公司非敏感数据的泄露、篡改、伪造、丢失； 3.网络安全事件预计会引发集团或集团客户遭受财务或名誉损失； 4.其他网络安全部评估确认的事件。
P5 级	1.公司信息系统发生安全事件但不影响数据、业务、服务； 2.公司面临未被及时阻止的网络安全威胁，但该威胁经评估不足以对正常业务产生影响； 3.公司面临被及时阻止的网络安全威胁，但威胁可能会对公司正常业务造成影响的风险； 4.其他网络安全部评估确认的事件。

c) 事件分级原则

- 事件分级以量化指标为优先原则，在主观量化损失时应按较高的量化损失或更严重的影响作为评估依据；
- 如判断进行准确量化存在较大困难或量化所消耗成本较高时可基于主观判断进行；
- 在事件持续过程应根据事件进展动态更新事件级别。

7.1.3.6 网络安全监测预警和信息报送制度

7.1.3.6.1 监测预警

a) 日常活动预警要求

- 根据国家行业主管或监管部门关键信息基础设施网络安全信息通报制度的要求，按照国家网络安全事件应急预案等规定，制定并完善本组织信息通报制度，明确负责信息通报工作的主管领导和承担信息通报工作的责任部门、负责人和联络人。
- 应制定不同级别不同分类预警的处置防范措施建议。
- 应具备威胁预警、漏洞预警和攻击预警等多种预警能力。
- 应建立预警快速发布与响应、预警升降级和解除等预警程序，不同级别预警可采用不同流程，并应产生记录。
- 预警机制应采用自动化方式，在发现可能危害关键业务的迹象时，应能采用自动化的方式及时报警，并自动化地采取对关键业务破坏性最小的行动。例如：恶意代码防御机制、入侵检测设备或者防火墙等弹出对话框、发出声音或者向相关人员发出电子邮件等方式进行报警。

- 预警方式应区分为内部预警和外部预警，对网络安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息。对于可能造成较大影响的，应按照相关部门要求进行通报等外部预警。内部预警信息的内容应包括：基本情况描述、可能产生的危害及程度、可能影响的用户及范围、建议采取的应对措施等。
- 当内部预警信息发出之后，情况出现新的变化，运营者应向有关人员和组织及时补发最新内部预警信息。
- 能持续获取预警发布机构的安全预警信息，分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度，必要时启动应急预案。获取的安全预警信息应按照规定通报给相关人员和相关部门。
- 采取相关措施对预警进行响应，当安全隐患得以控制或消除时，应执行预警解除流程

b) 重大活动预警要求

- 建立重大活动的预警保障方案，纳入本单位的应急预案，定期组织演练。
- 重大预警事件应采取自动、半自动、人工等两种以上的预警通道，最终可达责任人。
- 重大活动期间按预警分类明确响应处置时限，保障及时响应处置。

c) 突发事件预警要求

- 应建立突发预警流程，组建应急专项小组，制定涵盖病毒、网络等各方面专业人才联络清单。应急专项小组，由运营企业负责人担任组长，承担应急过程中的指挥协调、资金保障等工作。
- 设立无法分类的事件预警通道，设立响应时限，充分联合保护工作部门、研究机构、网络安全服务机构、业界专家及其他有关部门进行共同处置，并形成记录。
- 第一时间分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度，根据情况启动与预警等级和事件类型相应的应急预案，并向上级汇报处置计划，根据上级指示随时调整。
- 积极配合上级领导机构的应急指挥工作，主动提供有助于应急处置的设备、技术、财产等人物力应急资源，保障应急措施快速落实。
- 事后主动开展预警响应工作复盘分析，总结经验收获向保护工作部门、公安机关报告。

7.1.3.6.2 信息通报

a) 信息报送方案

b) 信息报送类型

- 报送方报送的信息类型包括脆弱性信息、网络安全威胁信息、网络安全事态信息、网络安全事件信息、网络安全态势信息、网络安全资讯、其他信息等。
- 其中，网络安全事件信息是对影响网络安全情况的确定性事件的描述信息，网络安全威胁信息是对网络安全事件的潜在原由的描述信息，脆弱性信息是对可被网络安全威胁利用的网络自身属性的描述信息，网络安全事态信息是对可能由网络安全事件导致的可识别影响的描述信息，网络安全态势信息是从宏观角度对一定范围网络安全情况的整体描述信息，网络安全资讯是对网络安全情况的外部描述信息，其他信息是可对网络安全态势研判起支撑作用的其他情况的描述信息。

c) 信息格式

接收方宜制定信息报送格式规范，并与报送方取得共识。如果某个报送方不能按照格式要求报送信息，宜向接收方提供明确的信息报送格式说明。报送的信息宜使用可机读形式，可附加非机读内容。接收方宜设计并实现信息格式转换方法，将相应报送方报送的信息转换为符合信息报送格式要求的信息格式后，再进行信息汇总和后续处理。

d）报送方式

信息报送方式的要求宜包括以下方面：

- 信息报送发起方式，可包括报送方主动报送信息、根据接收方的要求报送特定信息；
- 信息报送接口，可包括系统接口、界面填报、其他方式等；
- 信息报送通道，可包括互联网、专线、其他方式等；
- 信息报送流程宜支持双向的数据和指令传输。

e）实效性

- 接收方宜制定信息报送的时效性规范，并与报送方取得共识。

f）安全性

- 接收方宜制定信息报送的安全性规范，如高等级或高敏感信息的知悉范围、信息保护措施、特定报送流程等内容，并与报送方取得共识。

7.1.3.7 关键信息基础设施个人信息和重要数据境内存留制度

- 将在我国境内运营中收集和产生的个人信息和重要数据存储在境内，因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估，法律、行政法规另有规定的，依照其规定。
- 严格控制重要数据的公开、分析、交换、共享和导出等关键环节，并采取加密、脱敏、去标识化等技术手段保护敏感数据安全。
- 建立业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份。
- 业务数据安全性要求高的实现数据的异地实时备份。
- 业务连续性要求高的实现业务的异地实时切换，确保关键信息基础设施一旦被破坏，可及时进行恢复和补救。

7.1.4 数据安全与管理

7.1.4.1 数据安全合规概述

7.1.4.1.1 相关术语概念及其定义

a）数据：任何以电子或者其他方式对信息的记录。

b）数据安全：通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

c）数据处理者：在中华人民共和国境内开展数据处理活动的主体。

7.1.4.1.2 主要相关依据

a）《中华人民共和国数据安全法》

b）《中华人民共和国网络安全法》

c）《中华人民共和国个人信息保护法》

7.1.4.2 合规职能部门及职责

数据处理者应当按照法律法规要求，制定内部安全管理制度和操作规程，宜确定数据安全负责人，落实数据安全保护责任。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

7.1.4.3 合规主要风险点

7.1.4.3.1 数据处理者的合规风险

a) 数据处理者未依照法律、法规的规定，没有确定数据安全管理的主要负责人、责任部门和关键岗位人员，未建立数据生命周期全流程数据安全管理制度和数据分级分类制度；
b) 数据处理者未针对不同类型、级别数据，采取相应的权限管理、安全技术措施和其他必要措施，保障数据安全；
c) 数据处理者未定期对从业人员开展数据安全教育和培训，未制定数据安全风险应急预案，未定期进行演练。

7.1.4.3.2 重要数据处理者的合规风险

a) 重要数据的处理者未建立覆盖本单位相关部门的数据安全工作体系，未明确数据安全负责人和管理机构，未落实数据安全保护责任；
b) 重要数据的处理者未按照规定对其数据处理活动定期开展风险评估，未向有关主管部门报送风险评估报告；
c) 重要数据处理者未按照有关要求进行备案，备案内容发生变化的，未在三个月内报备变更情况。

7.1.4.4 合规管理措施

7.1.4.4.1 数据安全合规管理原则

数据处理者应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

7.1.4.4.2 数据安全合规管理目标

数据处理者应当建立数据安全合规管理体系，保障数据的收集、存储、使用、加工、传输、提供、公开等数据处理活动的安全，有效应对数据安全事件，防范数据安全风险，维护数据的完整性、保密性和可用性。

7.1.4.4.3 数据安全合规管理具体实施步骤

a) 数据处理者应当建立数据全生命周期安全管理制度，建立健全数据分类分级管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、公开等环节的具体分级防护要求和操作规程；
b) 数据处理者应当严格落实网络安全等级保护制度；
c) 数据处理者应当根据数据的类型、数量、安全级别、处理方式以及对国家安全、公共利益或者个人、组织合法权益带来的影响和安全风险等，采取相应的技术措施和其他必要措施，保障数据安全；
d) 重要数据处理者应当按照有关要求进行备案，备案内容发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新；
e) 数据处理者应当定期对从业人员开展数据安全教育和培训；
f) 重要数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，应当明确数据安全管理的主要负责人和责任部门，落实数据安全保护责任；
g) 数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动；
h) 数据处理者收集数据应当遵循合法、正当、必要的原则；

i) 数据处理者在数据收集、处理的过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集、处理人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录；

j) 数据处理者通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任；

k) 数据处理者应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据的，应当采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理；

l) 数据处理者应当合理确定数据处理活动的操作权限，严格实施人员权限管理；

m) 数据处理者在数据全生命周期处理过程中，应当记录数据处理、权限管理、人员操作等日志，日志留存时间不少于六个月；

n) 数据处理者应当制定数据安全事件应急预案，并定期进行演练；

o) 数据处理者使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动，应当取得个人、单位等的同意；

p) 数据处理者利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据的，应当加强访问控制，建立登记、审批机制并留存记录；

q) 数据处理者应当依据行业数据分类分级管理要求，明确数据提供的范围、数量、条件、程序等。提供重要数据的，应当采取数据脱敏等措施，建立审批机制；

r) 数据处理者应当事先对数据接收方的数据安全保护能力进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实；

s) 数据处理者委托他人开展数据处理活动的，应当对被委托方的数据安全保护能力、资质进行核实，确保符合国家、行业主管部门的相关要求，并通过合同约束、现场核查等方式对被委托方落实数据安全保护措施的情况进行监督管理；

t) 数据处理者公开数据应当真实、准确，在公开前应当开展安全评估；

u) 数据处理者应当建立数据销毁策略和管理制度，明确销毁对象、流程和技术等要求，对销毁活动进行记录和留存；

v) 符合以下情况的，数据处理者应当销毁相应数据：i)因业务约定，需要销毁的；ii)个人依据其合法权益请求销毁的；iii)组织基于保护国家安全、社会公共利益目的，且有公证机构提供证明，请求销毁的；

w) 数据处理者因兼并、重组、破产等原因需要转移数据的，应当明确数据承接方案，并通过电话、短信、邮件、公告等方式通知受影响用户；涉及重要数据的，应当及时向所在地工业和信息化主管部门或通信管理局备案；

x) 数据处理者在中华人民共和国境内收集和产生的重要数据，应当依照法律、行政法规要求在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估，在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握；

y) 数据处理者应当定期进行安全审计，并形成审计报告，涉及重要数据的，应当至少每年进行一次。

7.1.5 个人信息保护

7.1.5.1 个人信息保护领域概述

7.1.5.1.1 术语与定义

a) 个人信息：以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

b) 处理：包括收集、存储、使用、加工、传输、提供、公开、删除等动作在内的针对个人信息的处置动作。
c) 个人信息处理者：指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。
d) 敏感个人信息：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，以及不满14周岁未成年人的信息。
e) 自动化决策：通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并作出决定的活动。

7.1.5.1.2 主要相关依据

a)《中华人民共和国个人信息保护法》
b)《中华人民共和国网络安全法》
c)《中华人民共和国民法典》

7.1.5.2 合规职能部门及职责

个人信息处理者宜建立个人信息保护责任部门或指定负责人，专门负责个人信息保护合规管理工作。

7.1.5.3 主要合规风险点

a) 个人信息处理者在个人信息处理活动中，未遵守合法、正当等处理个人信息的基本原则，通过误导、欺诈、胁迫用户等方式侵害用户个人信息权益，或非法收集、使用、加工、传输个人信息等，造成恶劣的社会影响；
b) 个人信息处理者在不满足《个人信息保护法》第十三条规定的处理个人信息的合法情形的前提下，违规收集、使用用户个人信息；
c) 个人信息处理者未在实现处理目的的最小范围内处理个人信息，存在超范围、过度收集使用用户个人信息的行为，造成个人信息滥用的风险；
d) 在基于用户个人同意进行个人处理的情形下，个人信息处理者未确保用户个人充分知情并自愿而明确地作出对其个人信息处理的同意，即未获得有效同意或超出用户同意范围进行处理，损害用户个人信息权益；
e) 个人信息处理者未能针对敏感个人信息提供特殊的处理保护机制，违规处理敏感个人信息，造成个人信息泄露或非法使用，导致用户人格遵守受到侵害，人身、财产安全受到危害；
f) 个人信息处理者利用个人信息进行自动化决策，未能保证决策透明度和结果公平公正，对个人在交易条件上设置不合理的差别待遇，侵犯用户合法权益；
g) 个人信息处理者在开展业务过程中如涉及向境外提供个人信息，未按照跨境规则履行出境配套义务，从事违规跨境行为，造成境内用户个人信息权益损害且风险显著扩张；
h) 个人信息处理者无正当理由而未能及时响应个人信息主体对其个人信息享有的知情权、决定权、查阅、复制、删除等依法行使的权利、主张，造成个人的信息权益无法得到有效保障。

7.1.5.4 合规管理措施

7.1.5.4.1 个人信息保护基本原则

个人信息处理者应当遵守合法、正当、必要、诚信、公开、透明等原则，进行个人信息处理活动。个人信息处理者不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。不得通过误导、欺诈、胁迫等方式处理个人信息。不得过度收集个人信息。

7.1.5.4.2 个人信息保护合规管理目标

个人信息处理者进行个人信息处理活动应当遵守相关法律法规规定，在合理利用个人信息、为用户提供便捷高效的网络服务同时，充分保障个人信息权益。

7.1.5.4.3 个人信息保护关键措施

个人信息处理者宜建立健全企业个人信息保护合规管理体系，加强个人信息保护合规制度及配套管理措施建设。遵守国（境）内个人信息保护法律法规监管规定，建立完善的个人信息保护制度，确保个人信息的合理利用和安全存储。包括但不限于：

a) 加强个人信息的全生命周期保护机制，对法律法规明确规定开展事前个人信息保护影响评估的处理行为开展个人信息安全影响评估，并对处理情况进行记录,定期对处理个人信息遵守法律、行政法规的情况进行合规审计；
b) 建立内部个人信息保护体系，并依据企业情况定期更新完善；
c) 培育个人信息的基础数据安全能力；
d) 建立个人信息风险应急处置机制，制定并组织实施个人信息安全事件应急预案;
e) 建立并加强对敏感个人信息的特殊处理机制；
f) 依法制定和运行利用个人信息的自动化决策机制；
g) 建立个人信息合作第三方合规管理机制；
h) 建立健全个人信息数据出境管理制度及对应合规管理措施；
i) 完善个人信息主体权利保障机制，并确保其有效性；
j) 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训。

7.1.6 出口管制

7.1.6.1 出口管制概述

7.1.6.1.1 术语和定义

a) 出口管制：出口管制是指为了维护国家安全和利益，履行防扩散等国际义务，国家对从本国境内向境外转移管制物项，以及本国公民、法人和非法人组织向外国组织和个人提供管制物项，采取禁止或者限制性措施。物项：受出口管制法所管辖的货物、技术、服务及其相关的技术资料等数据。
b) 出口管制合规管理委员会：企业董事会（5.2.2）领导下的出口管制合规委员会是按照5.2.5履行出口管制合规管理职责的企业内设机构。
c) 出口管制合规管理负责人：企业中，按照5.2.6的规定承担出口管制合规管理负责人职能的人。
d) 出口管制合规管理牵头部门：出口管制合规管理部门是按照5.2.7的规定制定、实施和监督出口管制合规管理工作，为其他业务部门提供出口管制合规支持的部门。

7.1.6.1.2 规范性引用文件

a) 《中华人民共和国出口管制法》、《中华人民共和国对外贸易法》、《中华人民共和国反外国制裁法》。
b) 《中华人民共和国货物进出口管理条例》、《中华人民共和国技术进出口管理条例》、《中华人民共和国核材料管制条例》、《中华人民共和国核两用物品及相关技术出口管制条例》、《中华人民共和国生物两用品及相关设备和技术出口管制条例》。
c) 《阻断外国法律与措施不当域外适用办法》、《不可靠实体清单规定》、《两用物项和技术进出口许可证管理办法》、《两用物项和技术进出口许可证管理目录》、《禁止出口限制出口技术管理办法》、《商务部关于两用物项出口经营者建立出口管制内部合规机制的指导意见》、《两用物

项出口管制内部合规指南》、《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》。

7.1.6.2 主要合规风险点

a) 产品受出口管制法律法规管控且应当申请办理许可，而未办理许可违规出口的风险。
b) 产品出口的目的地为适用出口管制法律法规限制国家或者地区的风险。
c) 交易主体（包括进口商与最终用户）为适用出口管制法律法规所限制主体的风险。
d) 产品被用于适用出口管制法律法规所限制用途的风险。
e) 无视风险信号进行出口的风险。
f) 合规管理体系存在漏洞，未能有效筛查出风险交易的风险。

7.1.6.3 具体实施措施

7.1.6.3.1 合规原则、目标、方针

企业出口管制合规管理工作应当遵循合规管理的原则，全面性（4.1）、有效性（4.2）、独立性原则（4.3）、动态性原则（4.4）和可查证原则（4.5）。

出口管制合规的目标应当为通过制定合规管理架构、合规政策和流程设计等方式保证在相关业务领域的各个业务环节符合出口管制法律。

出口管制合规管理的方针应当是建立健全出口管制合规管理体系，通过多种手段确保体系运行的实时有效性，并且有纠错和应急机制。

企业可以根据自身企业文化、风险偏好，结合企业经营类型和业务开展的自身特点制定本企业的出口管制目标和方针。

7.1.6.3.2 核心合规内容

出口管制合规的内容包括，充分发挥合规管理组织作用，建立有效的出口管制合规体系、通过多重手段建立企业合规文化。建立、制定和实施出口管制合规体系，并且对该体系进行有效维护、定期和/或不定期评估，以促使该体系不断优化，充分保障实现出口管制的合规目标的实现。

7.1.6.3.3 合规职能部门及职责

企业可根据自身实际及“全面评估”的结果，建立由决策层支持，出口管制合规管理部门牵头负责、各业务部门具体落实合规工作相结合的，全方位、多层次合规管理组织构架。企业应确定组织架构各层级，明确出口管制合规人员选拔标准、岗位职责、权限与联系方式，并将合规工作表现纳入绩效考核。企业可参考以下组织体系，或将出口管制合规组织机构嵌入现有合规管理体系，根据出口管制业务规模、全面风险评估结果等酌情调整。

出口管制合规管理委员会：企业董事会（5.2.2）领导下的出口管制合规委员会按照5.2.5的规定履行出口管制合规管理职责，企业可以根据实际情况，将该机构职能由合规管理委员会（5.2.5）一并行使。尚不具备条件的企业可结合实际，只任命合规管理负责人或者首席合规官（5.2.6）履行该管理职责。

出口管制合规管理负责人：按照5.2.6的规定承担出口管制合规管理负责人的职能，如果企业不设立出口管制合规管理委员会，仅设立出口管制合规管理负责人，则出口管制合规管理负责人还需要按照5.2.5的规定承担合规管理委员会的职责。

出口管制合规管理部门：出口管制合规管理部门是出口管制合规管理牵头部门，负责推动出口管制合规

政策在相关业务领域的落实，并按照5.2.7的规定进行组织、协调和监督合规管理工作，为其他部门提供合规支持。尚不具备条件的企业可根据本企业出口管制业务规模、风险评估结果等仅设置出口管制合规岗位承担相关职责。

各业务部门：各业务部门依据5.2.8规定的职责，在出口管制合规部门指导下，严格执行本企业出口管制合规管理制度。

7.1.6.3.4 具体实施措施

a）拟定合规政策声明

企业主要负责人签署政策声明，并通过公开讲话宣贯、向全体员工发送邮件、网站发布声明、组织录制相关视频等多种方式公开承诺支持合规政策，遵守合规制度，保证出口管制合规的资源投入。企业的中高层管理人员应带头践行合规政策。声明面向全体员工，如有必要，也可以面向合作伙伴分发，表明本企业的出口管制合规立场。该声明应当根据法律法规变动、企业自身合规需求进行更新。

合规政策声明的内容包括但不限于：

- 阐明出口管制合规的基本目的和重要意义；
- 承诺遵守适用的出口管制法律法规；
- 承诺任何情况下都不会从事违反出口管制相关法律法规的商业活动；
- 明确表示对出口管制合规的支持；
- 承诺在商业活动前，对出口管制风险进行评估审查；
- 强调员工熟悉出口管制相关规定并认真遵守的重要性，并要求员工遵守出口管制相关法律法规，任何情况下不得违规出口；
- 列明违反出口管制相关法律法规的风险和可能受到的处罚；
- 提供企业出口管制合规联系人及联系方式。

b）进行全面风险评估

全面的风险评估是出口管制内部合规制度的基础。企业定期对自身可能存在的出口管制风险进行全面评估，并根据风险评估的结果有针对性地建立健全适合自身特点的出口管制内部合规制度和合规管理组织架构，梳理分析可采取的风险防范措施。风险评估包括如下几个方面：

i)经营物项情况：

- 经营物项是否被列入出口管制清单（包括临时管制）。
- 对经营物项进行梳理和科学分类，判断是否属于中国、进口国或第三国（过境、转运、通运、再出口等）相关进出口管制法律法规管辖的范围。
- 梳理物项可能的主要用途，物项是否存在：（1）危害国家安全和利益的风险；（2）被用于设计、开发、生产或者使用大规模杀伤性武器及其运载工具的风险；（3）被用于恐怖主义目的的风险。

ii)合作伙伴情况：

- 合作伙伴是否被列入我国管控名单等禁止或限制交易名单，或被列入联合国的制裁清单。
- 合作伙伴所在国家或地区风险等级。
- 合作伙伴类型，是供应商、经销商、最终用户还是合作开发伙伴。
- 合作伙伴的主要业务范围，是否涉及军事等敏感业务。

iii)研发情况：

- 排查日常经营是否涉及属于管制物项的技术。
- 摸排日常经营中的技术交流、传输是否有构成技术出口的风险和隐患。使用电子邮件、电话和传真以及国内外社交软件等电子形式传输技术信息都有可能构成技术的出口和转让，使用“云”等在线存储模式对软件和技术进行存储或传输也可能存在出口管制合规风险。
- 梳理从事受控技术相关工作的员工情况，摸排是否可能存在未申请许可证向外国组织和个人提供受控技术的风险和隐患，如有雇用外籍员工从事受控技术相关工作、在贸易展上发布受控技术相关信息等情况，需按照法律法规要求申请许可证。
- 及时跟踪本企业的设计和研发计划，并就可能的出口管制合规风险提供早期建议。如有必要，可以咨询国家出口管制管理部门。

iv)内部运作情况

- 梳理本企业涉及出口管制的供应链各重要部门可能存在风险的环节，包括但不限于研发、采购、销售、财务、物流、报关等。
- 是否设有专门组织机构/人员负责出口管制合规相关工作，资源配备是否充足。
- 是否有 IT 筛查工具，以及 IT 筛查工具的有效性。

c）履行合规审查

企业科学设计审查程序，并根据出口管制相关法律法规、出口管制清单等，针对每一笔交易做好全流程风险审查工作。根据公司业务开展情况和合规体系建设情况，鼓励采取信息化自动筛查手段。

在交易洽谈之初，企业需对物项、交易类型、最终用户、最终用途、运输路径等进行综合评估。审查人员应在能力范围内尽可能获取上述信息，并综合分析以上审查结果，审慎提出“批准交易”、“取消交易”或“暂停交易”的意见。如交易情况过于复杂，可逐级上报至出口管制合规部门或出口管制合规委员会做出相关决定。

合同中设置出口管制合规相关条款，约束交易方遵守出口管制相关法律法规，以防范出口管制相关风险。

如交易需要申请许可证的，需要按法律法规相关规定向国家出口管制管理部门提交相应材料，并申请出口许可证；依法需要取得相关管制物项出口经营资格的，应当取得相应资格，否则不得履行合同相关义务。

e）组织合规培训

企业应当对全体员工进行出口管制合规培训，可根据员工的岗位职责设计不同的培训内容。企业可采取不同形培训式，如网络授课等，确保全员接受培训。

企业可以编制合规手册，通过多种途径向全体员工发放，使得员工能够随时获得出口管制合规方面的帮助。

f）保留资料档案

各部门应当完整、准确保留与出口管制合规相关的文件，定期归档，并不定期抽查存档情况。档案一般保留五年以上。企业可以根据工作实际选择最适当的存档方式，可以是原始文件，也可以是复制件或电子文件，但需确保复制件和电子文件真实、准确、清晰，并保留原始文件的所有标记、信息和其他特征。

存档文件如需向境外提供，应当按照《中华人民共和国出口管制法》第三十二条要求进行。

归档文件一般包括出口产品规格、商业交易相关文件（如询盘相关记录、订货表格、合同、发票、提单、货运单、转账记录等）；与相关政府部门沟通情况；客户筛查记录及往来记录；最终用户和最终用途证明文件；许可申请文件；许可审批文件；出口项目执行情况；涉及出口管制的规章制度，会议纪要、会议决议、管理文件；曾发现的违规问题及处理措施；培训记录和材料；审计报告书；国外分包商、客户等来访的记录；其它需要归档的文件。

7.1.6.3.5 出口管制合规的有效性

企业可以通过整体审计和专项审计来对企业出口管制内部制度及其执行情况进行评估。企业可以根据具体情况，安排定期审计或不定期审计。审计可以由企业内部人员进行，也可以聘请外部专业机构进行。

企业应当根据审计结果进行持续改进，对提出的整改措施狠抓落实，保障出口管制内部合规制度的有效运行，提高内部合规管理水平。

7.1.6.3.6 纠错与持续改进机制

业务部门应时刻警惕，发现风险后及时主动向出口管制合规部门、管理层报告。企业也可以接收其他途径的举报。

企业应当向员工、客户、第三方等举报人提供安全的、不受限制的举报途径，以接受对违规行为的举报，允许举报人匿名举报，并对举报人的身份和举报事项严格保密，不得擅自对外泄露。

根据举报或者其他信息，由合规部门确定是否启动企业内部调查、确定调查范围；明确调查程序；起草调查报告；视情向举报人通报调查结果；向管理层汇报。

通过调查、发现确实存在违规行为时，应当采取纠错或补救措施，必要时，还应当向国家出口管制管理部门报告。

设立奖惩制度，对积极参与合规管理工作的员工给予奖励。同时建立违规约束机制，对违反合规规定和管理政策的员工按照公司员工守则等内部规定给予严厉惩戒，必要时可辞退。

7.1.6.4 特别说明

7.1.6.4.1 平台义务

从事平台业务的互联网企业，应特别注意平台的合规审查义务。除了对合作的商家进行合规审核，还应结合平台的明知义务采取适当措施，对平台上销售的商品/服务、收货地址、收货人进行审核，确保不违反相关法律规定。

7.1.6.4.2 技术进出口

在整合全球研发资源的通信和互联网行业，跨境技术交互频繁，企业应当注重识别技术跨境的各种场景，识别企业技术研发的管控水平，并且注意识别外籍员工在研发工作中的职能是否会触发出口管制相关规定。

7.1.6.4.3 数据跨境传输

企业在日常经营中，如果存在跨境数据传输的场景，可以根据企业自身需要，将出口管制合规制度的相应环节用于数据出口管制的预警和处置。

7.1.6.4.4 境外经营

企业在境外设立主体进行经营时，需要注意对业务运营进行评估，识别多主体之间的物项交互场景，确

认需要遵守的出口管制法律，此时，有可能需要遵守多国的相关规定。

7.1.7 移动互联网应用程序（APP）

7.1.7.1 移动互联网应用程序（APP）概述

7.1.7.1.1 术语与定义

a) 移动互联网应用程序：通过预装、下载等方式获取并运行在移动智能终端上、向用户提供信息服务的应用软件。
b) 移动互联网应用程序提供者：提供信息服务的移动互联网应用程序所有者或运营者
c) 互联网信息服务：通过互联网向上网用户提供信息的服务活动。

7.1.7.1.2 主要依据

a) 《中华人民共和国个人信息保护法》
b) 《中华人民共和国网络安全法》
c) 《中华人民共和国数据安全法》
d) 《中华人民共和国消费者权益保护法》
e) 《互联网信息服务管理办法》
f) 《移动互联网应用程序信息服务管理规定》

7.1.7.2 合规职能部门及职责

企业合规职能部门及职责参见第5章合规管理组织体系。在此基础上，企业应根据自身规模、业务情况、监管要求、实际提供的服务等情况，设立专职合规人员或相关的合规管理组织有效建立、制定、实施、执行合规管理要求和相关工作。

7.1.7.3 合规主要风险点

7.1.7.3.1 资质准入

通过移动互联网应用程序（APP）提供互联网信息服务，应当依法取得法律法规规定的相关资质，属于经营《电信业务分类目录（2015年版）》规定的电信业务的，应依法申请相应电信业务经营业务许可。从事新闻、出版、教育、金融、医疗保健、药品和医疗器械等互联网信息服务的，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。如根据《教育移动互联网应用程序备案管理办法》，教育移动应用提供者还应按照教育部的要求进行提供者备案，并配合注册地省级教育行政部门做好备案审核工作。

7.1.7.3.2 数据安全

参见7.1.4数据安全与管理。

7.1.7.3.3 个人信息保护

参见7.1.5个人信息保护。

7.1.7.3.4 应用安全正常运行

移动互联网应用程序提供者应为用户提供安全可靠的使用环境和基本、正常完整的功能，不得含有试图

滥用或不当使用任何网络、设备以及干扰其他应用的安全隐患和不合理限制。

a) 应用不得含有病毒、木马等侵害用户的功能或行为；
b) 应用不得在未告知用户的情况下，超出业务需要，频繁自动联网，消耗用户流量；
c) 应用不得未经用户授权强制启动系统服务；
d) 应用不得含有第三方加载可执行代码的应用或SDK；
e) 应用不得出现任何窃取数据、暗中监控用户、或其他损害用户利益的恶意行为，以及不得出现对其他应用的恶意干扰和屏蔽行为；
f) 应用不得带有修改其他应用数据、存档等内容的功能；
g) 应用应具备良好的兼容性，需能够正常安装、启动、卸载，不得出现运行时频繁崩溃，不得出现需借助第三方软件才可卸载的情况，法律法规另有规定的除外；
h) 应用功能需确保已实现和使用正常，不得存在不合理的使用限制；
i) 应用不得强制要求用户下载其他非必要的移动应用；
j) 应用描述和实际功能应保持一致，不得欺骗用户下载使用。

7.1.7.3.5 互联网信息内容管理

参见7.1.15内容合规。

7.1.7.3.6 消费者权益保护

移动互联网应用程序提供者在面向用户提供服务时应遵循自愿、平等、公平、诚实信用的原则，切实保障用户的知情权、自主选择权、人身财产安全权、公平交易权等权利，保障用户使用和体验，保护消费者的合法权益。

a) 依法保障用户在安装或使用应用程序过程中的知情权和选择权，未向用户明示并经用户同意，不得开启收集地理位置、读取通讯录、使用摄像头、启用录音等功能，不得开启与服务无关的功能，不得捆绑安装无关应用程序；
b) 利用互联网发布、发送广告时，不得影响用户正常使用网络。在互联网页面以弹出等形式发布的广告，应当显著标明关闭标志，确保一键关闭；
c) 提供自动展期、自动续费等服务的，应当在用户接受服务前和自动展期、自动续费等日期前五日，以显著方式提请用户注意，由用户自主选择；在服务期间内，应当为用户提供显著、简便的随时取消或者变更的选项，并不得收取不合理费用；
d) 应用内某功能涉及需要付费才能使用的，应合理定价，不得出现定价过高或价格欺诈的行为。
e) 尊重和保护知识产权，不得制作、发布侵犯用户或他人知识产权的应用程序；
f) 用户在购买、使用服务时，移动互联网应用程序提供者应确认产品符合保障人身、财产安全的要求。

7.1.8 反洗钱/反恐怖融资

7.1.8.1 反洗钱及反恐怖融资概述

7.1.8.1.1 术语定义

a) 反洗钱：反洗钱是指为了预防通过各种方式掩饰、隐瞒犯罪所得及其收益的来源和性质的洗钱活动，遏制相关违法犯罪活动，依法采取相关措施的行为。
b) 恐怖融资：恐怖融资是指恐怖组织、恐怖分子募集、占有、使用资金或者其他形式财产；以资金或者

其他形式财产协助恐怖组织、恐怖分子以及恐怖主义、恐怖活动犯罪；为恐怖主义和实施恐怖活动犯罪占有、使用以及募集资金或者其他形式财产；为恐怖组织、恐怖分子占有、使用以及募集资金或者其他形式财产。

c) 互联网企业义务主体：互联网企业义务主体是指是指根据《反洗钱法》等相关法律法规的规定，属于金融机构及特定非金融机构，应当履行反洗钱义务的互联网企业。注：本章节合规标准宜适用于《中华人民共和国反洗钱法》所规定的义务主体。对于上述法定义务主体以外的互联网企业，可根据自身实际情况酌情参考适用本章节合规标准。

d) 风险识别与评估：风险识别与评估是指通过一定的程序和方法，对已存在或可能发生的风险进行认识、辨别和发现，并评判和预估其可能带来的法律责任、监管处罚、经济损失和声誉损失等不利后果的风险和严重性，目的是针对不同类型和等级的风险采取相应的应对措施。

e) 了解你的客户/员工/第三方服务供应商：了解你的客户/员工/第三方服务供应商是指通过尽职调查和身份识别等措施，了解相关主体的身份信息、信用程度、经营状况、交易或合作背景、资金来源和用途及风险状况等。

7.1.8.2.2 制度建设

互联网企业宜将反洗钱和反恐怖融资相关内容纳入互联网企业的合规管理建设，通过企业合规政策制度将对互联网企业反洗钱/反恐怖融资的要求予以明确。

一般而言，反洗钱和反恐怖融资政策制度可包含以下主要内容：

a) 负责人员和职责

b) 风险管理

c) 合规审计

d) 报告和记录

e) 违规后果

f) 配合调查/执法

g) 培训

7.1.8.2.3 人员职能

根据互联网企业的组织架构和合规现状，可设置专岗负责反洗钱/反恐怖融资，也可由合规/法务/风控人员兼任。

7.1.8.2 反洗钱及反恐怖融资风险管理

7.1.8.2.1 制定风险管理计划

为有效遏制和防控洗钱风险，各互联网企业义务主体应当以风险为本的方法，制定洗钱风险管理计划，识别、评估和了解本公司洗钱与恐怖融资风险，并采取相应管控措施。洗钱风险管理应纳入企业全面风险管理，包括但不限于以下要素：风险管理架构；风险管理策略；风险管理政策和程序；信息系统、数据治理；内部检查、审计、绩效考核和奖惩机制。

7.1.8.2.2 风险识别与评估

a) 主体风险识别与评估：互联网企业应结合自身的业务特性、地域、客户、产品（服务）、渠道等因素评估自身的洗钱与恐怖融资风险。对风险识别与评估可采取定量和定性相结合的方法，评估其固有风险、管控措施有效性及剩余风险。互联网企业应定期或不定期开展风险评估，并充分运用风险评估的结果，确保资源配置、洗钱风险管理策略、政策和程序与评估所识别的风险相适应。

b) 客户风险识别与评估：互联网企业应对客户开展风险评估，关注客户带来的洗钱风险。客户的风险评

估包括初次评估、持续评估及动态调整。对客户的评估至少分为三个风险等级，对于风险较高的客户，应采取包括强化身份识别，限制交易额度、频次与渠道，提高审批层级等管控措施。

c) 员工风险识别与评估：互联网企业应将员工的洗钱风险纳入风险监测，评估员工参与洗钱风险的可能性。

d) 第三方服务供应商风险识别与评估：互联网企业与第三方服务供应商合作时，应对第三方进行充分的尽职调查，确保第三方机构受到监督、管理或监测，评估第三方的洗钱及恐怖融资风险。当第三方服务供应商无法开展尽职调查或评估风险过高时，应终止与其的合作。

7.1.8.2.3 风险因素

a) 国家/地域风险：在高风险国家（地区）设立境外分支机构情况；交易对手或对方金融机构涉及高风险国家（地区）情况；境外分支机构数量及地域分布情况；高风险国家（地区）经营收入占比等。

b) 客户风险：非居民客户数量占比；离岸客户数量占比；政治公众人物客户数量占比；使用不可核查证件开户客户数量占比；职业不明确客户数量占比；高风险职业（行业）客户数量占比；由第三方代理建立业务关系客户数量占比；来自高风险国家（地区）的客户情况；被国家机关调查的客户情况等。

c) 产品业务风险：现金交易情况；非面对面交易情况；跨境交易情况；代理交易情况；公转私交易情况；私人银行业务情况；特约商户业务情况；一次性交易情况；通道类资产管理业务情况；场外交易情况；大宗交易情况；新三板协议转让业务；场外衍生品业务；保单贷款业务等。

d) 渠道风险：渠道覆盖范围（线下网点数量与分布区域，线上可及地域范围）及相应地区（包括境外国家和地区）的风险程度；该渠道建立业务关系的客户数量和风险水平分布；该渠道办理业务的客户数量、交易笔数与金额，办理业务的主要类型和风险水平。

7.1.8.2.4 了解你的客户/员工/第三方服务供应商

7.1.8.2.4.1 客户身份识别

客户身份识别是指通过采集及核查客户身份信息资料，了解客户及其交易目的和交易性质，核查客户真实资金来源和资金用途，了解并识别实际控制客户的自然人和交易的受益所有人。

7.1.8.2.4.2 客户尽职调查

客户尽职调查是客户身份识别的措施，客户尽职调查的目的是为实现客户身份识别。互联网企业可结合自身的业务模式和风险类别，制定相应的客户尽职调查标准和程序，并在下列情况下进行客户尽职调查：建立业务关系；在特定情况下开展一次性资金交易；怀疑存在洗钱或恐怖融资活动；对先前获得的客户身份识别信息的真实性或充分性存疑。

7.1.8.2.4.2.1 标准尽职调查

互联网企业可根据自身评估情况，决定是否采用如下全部或部分客户身份识别手段：

a) 客户身份识别和验证——可通过系统比对客户身份证件的真实性、有效性，采用人脸识别、活体识别、照片比对等技术手段完成身份验证；

b) 制裁名单筛查——可参考各项制裁制度规定和公布的已知或疑似恐怖分子、毒品走私贩等犯罪分子的名单进行对客户进行比对、筛查。

c) 政治公众人物筛查——可通过公开渠道信息或采购外部系统识别政治公众人物及相关人员。若确定客户为政治公众人物及相关人员，宜对其采取增强尽职调查措施。

d) 负面新闻筛查——可主动采取措施以筛查负面新闻中的高风险实体，以更好地划分客户风险等级。

7.1.8.2.4.2.2 简化尽职调查

对于低风险客户，信息通信及互联网企业可酌情采取简化尽职调查措施。

7.1.8.2.4.2.3 增强尽职调查

信息通信及互联网企业对高风险客户宜采取增强客户尽职调查措施，包括但不限于：在开立账户前或建立服务关系前密切审核高风险客户；要求客户提供相关信息（如资金和财富来源、职务或业务类型、账户控制人身份信息、对账户活动变动的解释等；在账户关系存续期间更频繁地审核其交易。

7.1.8.2.4.3 员工尽职调查

信息通信及互联网企业可制定适当的人员聘用背景调查制度、员工录用标准、考核标准和其他内控措施等，对潜在员工、现有员工和外部顾问等人员（统称“企业人员”）进行尽职调查，了解企业人员的背景、利益冲突情况、犯罪记录，并评估其涉足洗钱/恐怖融资活动的可能性，防止企业因聘用高风险人员面临诉讼或监管处罚。

7.1.8.2.4.4 第三方服务供应商尽职调查

若信息通信及互联网企业的业务运营依靠第三方服务供应商（包含分销商、中介机构、合作伙伴及交易对手等），企业可制定适当的服务采购尽职调查及准入审批制度，重点关注第三方服务供应商的业务性质、风险特性和风险类别，确保可即时或持续进行筛选、核查与监控，防止企业因选用高风险的服务供应商而面临诉讼或监管处罚。

7.1.8.2.5 风险分析与应对

a) 可疑活动分析与监控

基于风险为本的方法，互联网企业在设计洗钱/恐怖融资可疑活动监控规则时考虑企业的规模、客户群、地域范围、产品及产品特点，同时清楚界定触发调查的参数和阈值。

b) 可疑活动调查

互联网企业可根据自身情况制定相应的制度和程序，通过设置内部热线、员工举报、跟踪负面新闻等方式完善可疑活动监控手段。若企业收到反洗钱行政主管部门或其他监管机构的反洗钱调查通知，企业应依法配合反洗钱调查，不得为洗钱等违法犯罪活动提供便利。

c) 可疑活动报告

互联网企业发现未履行反洗钱/反恐怖融资义务的情况，可向反洗钱行政主管部门、有关主管部门举报；发现洗钱/恐怖融资可疑活动，可向反洗钱行政主管部门、有关主管部门以及公安机关举报。

d) 风险应对措施

根据国家反洗钱法的规定，企业可对高风险客户采取反洗钱特别预防措施，包括但不限于禁止与名单中列名对象、其代理人、其拥有或者控制的实体进行任何交易；对列名对象所拥有或者控制的资金、资产采取冻结或者相应措施以限制被列名对象获得资金、资产。

7.1.8.2.6 风险控制与监督

a) 审计

互联网企业可根据自身风险情况每年一次地对反洗钱/反恐怖融资工作进行审计：a)低、中风险企业的审计工作可由企业内部的内审/风控/法务/合规等部门中具有反洗钱知识的人员负责；b)高风险企业的审计工作宜由外部机构指定具备反洗钱知识、资质和经验的审计人员独立进行。

b) 定期评估

互联网企业可定期（例如每年一次，或因企业业务、产品、服务、客户群、服务地域变更等引起企业的反洗钱/反恐怖融资风险评级发生变动时）对反洗钱/反恐怖融资开展工作内部评估，以确保其有效性并及时发现新的风险因素。企业可参考《中国人民银行反洗钱局关于印发<法人金融机构洗钱和恐怖融资风险自评估指引>的通知》的评估模版内容，结合自身情况予以酌情采纳。

7.1.8.3 档案管理

7.1.8.3.1 身份资料保存及交易记录保存

互联网企业应建立客户、员工、第三方服务供应商身份资料和客户、供应商交易记录保存制度。

- 互联网企业应当保存的客户、员工、第三方服务供应商身份资料包括：记载客户、员工、第三方服务供应商身份信息、资料以及反映互联网企业开展客户、员工、第三方服务供应商等身份识别工作情况的各种记录和资料。
- 互联网企业应当保存的交易记录包括：关于客户与企业、客户与第三方服务供应商、第三方服务供应商与企业每笔交易/业务合作的数据信息（包括交易对手信息、网上交易 IP 地址、交易对象等）、业务凭证、账簿/电子凭证以及可以反映交易真实情况的合同、业务凭证、单据、业务函件或其他资料。

客户、员工、第三方服务供应商身份资料自业务关系或雇佣关系结束当年或者一次性交易记账当年计起至少保存五年。相关交易记录，自交易记账当年计起至少保存五年。

7.1.8.3.2 反洗钱及反恐怖融资工作档案保存

a) 互联网企业应建立健全反洗钱/反恐怖融资工作档案管理制度，保证档案资料收集齐全，归档及时，整齐有序，查阅方便，严防丢失和泄密。（注：反洗钱/反恐怖融资工作档案是指互联网企业反洗钱/反恐怖融资工作部门在开展交易监测分析、大额交易报告和可疑交易报告等反洗钱/反恐怖融资工作中收集、形成的具有保存价值的文字、材料、图表、音像、计算机磁盘、云存储、实物等形式的历史记录）
b) 反洗钱/反恐怖融资工作档案的保管期限分为永久保存、长期保存和短期保存。永久保存的档案包括已判决案件的相关资料等；长期保存的档案包括可疑案件线索及相关资料、反洗钱/反恐怖融资现场检查工作相关记录等；其他档案资料短期保存。

7.1.8.3.3 数据安全及个人信息保护要求

互联网企业应建立健全反洗钱/反恐怖融资数据及个人信息保护管理制度，不能以履行反洗钱/反恐怖融资义务为理由，肆意处理客户、员工个人数据和第三方服务供应商数据。互联网企业出于反洗钱/反恐怖融资需要，采集、存储、使用客户、员工个人信息的，应满足《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等规定要求。

7.1.8.3.4 保密

互联网企业宜建立健全反洗钱/反恐怖融资信息保密管理制度，明确因反洗钱/反恐怖融资义务获得的客户、员工、第三方服务供应商身份资料和交易信息，应当予以保密；非依法律规定，不得向任何组织和个人提供。

7.1.8.4 反洗钱/反恐怖融资合规文化建设

a) 互联网企业应积极开展反洗钱/反恐怖融资宣传语培训工作，为反洗钱/反恐怖融资工作营造良好环境。以多样化的形式和手段，明确反洗钱/反恐怖融资工作部门及其他各业务条线、各层级、各岗位的合

规职责和履职标准，让员工了解本企业的反洗钱/反恐怖融资的特点。

b) 互联网企业应将反洗钱/反恐怖融资的合规文化建设要求纳入企业文化、企业内控管理体系，每年应对管理层、相关工作人员进行至少一次反洗钱/反恐怖融资培训。培训应重点结合企业存在的反洗钱/反恐怖融资问题、历史案件、各岗位履职要求等针对性内容展开，确保反洗钱/反恐怖融资工作部门的工作人员及管理层能够接受反洗钱/反恐怖融资知识培训。

c) 互联网企业应组织人员编写具有企业特色的反洗钱/反恐怖融资宣传材料，发送至每位员工，及时掌握反洗钱基础知识，随时了解反洗钱/反恐怖融资动态及形势，提高企业员工反洗钱/反恐怖融资意识及职业敏感度，促进反洗钱/反恐怖融资工作的有效开展。

7.1.9 第三方/供应链管理

7.1.9.1 第三方/供应链合规概述

7.1.9.1.1 相关术语概念及其定义

第三方/供应链管理：指在满足一定的客户服务水平的条件下，为了使整个供应链系统成本达到最低而把第三方供应商、制造商、仓库、配送中心和渠道商等有效地组织在一起来进行的产品制造、转运、分销及销售的管理方法。第三方/供应链管理通常涵盖了采购、开发、外包、集成、交付、使用和服务等环节。

7.1.9.1.2 主要相关依据

a) 中华人民共和国《中央企业合规管理指引》

b) 中华人民共和国《信息安全技术 ICT供应链安全风险管理指南》

7.1.9.2 主要合规风险点

a) 供应链产品全生命周期：

- 产品全生命周期包括产品的设计、开发、采购、生产、仓储、物流、销售、维护、召回等，在供应链的某一环节，都有可能对产品或上游组件进行恶意篡改、植入、替换等，以嵌入包含恶意逻辑的软件或硬件，从而对企业造成不可估量的损失。

b) 基于全球供应链管理中企业的社会责任治理：

- 全球供应链中，企业社会责任治理的动力在欧美等发达国家日益兴起，诸如劳工、环保、健康安全、道德、应对气候变化以及节能减排等问题。

c) 供应商选择与管理

- 在供应链企业之间和工作合作过程中，存在各种不确定性的因素，如果企业供应链合作伙伴选择不当，将会导致供应链运行中存在较大的风险。

7.1.9.3 具体实施措施

7.1.9.3.1 企业第三方/供应链管理合规基本原则

第三方/供应链管理条按照“源头管控、安全可靠、持续监管、风险可控”原则，选择合规合格的供应商，保障其为企业提供符合合规要求的产品与服务，加强风险控制，消除供应链不安全隐患。

7.1.9.3.2 企业第三方/供应链管理合规管理部门

企业可设立供应链合规管理岗位，负责依据国家《中央企业合规管理指引》等相关政策法规、集团管理

要求和制度框架，组织开展供应链管理相关的规范化管理提升、合法合规监督检查及问题整改工作，以及供应链相关的合规管理内控制度、流程的完善与修订。

7.1.9.3.3 企业第三方/供应链合规管理具体实施措施

a) 针对供应链关键产品开展尽职调查，管控供应链安全风险：建议对进入企业关键软硬件产品进行尽职调查，将产品研发、测试、交付和技术支持过程中的供应链合规风险作为审查重点，提高供应链的透明度。

b) 督促第三方供应商营造合规供应环境，强化对供应链合规威胁的源头管控

- 要求供应商建立健全产品开发生命周期合规管理制度，强化产品需求分析、功能设计、开发实施、测试验证和上线发布等环节的质量和合规把控。

c) 利用合同约束，设立合规防火墙

- 企业与第三方/供应链签订购买或服务订单或合同之前，宜向对方明确相关合规要求，可要求第三方/供应链签署合规承诺函，从供应商和生产商处取得合规承诺。并定期核验合规承诺函所含信息的准确性。

d) 实现有害物质的合规管理

- 大力推动供应链开展物质成分信息披露，变革产品有害物质合规模式，提高环境合规验证效率，为产品废弃拆解、逆向供应链、材料再利用等提供依据，实现有害物质的合规管理。

e) 制定供应商合规准则

- 制定和实施《供应商行为操守准则》，详细记录对供应商的合规环境表现和期望，进行供应商绿色管理、评估和监督。

7.1.10 反腐败

7.1.10.1 反腐败概述

7.1.10.1.1 术语与定义

a) 腐败：本行业所述腐败，是指企业或其员工为其特殊利益而滥用职权行为，具体表现包括但不限于：

- 利用职务便利，侵吞、窃取、骗取或者以其他手段非法占有财务；
- 利用职务便利，索取他人财物的，或者非法收受他人财物，为他人谋取利益；
- 为谋取不正当利益，给予他人以财物；
- 国有企业从事公务人员的财产、支出明显超过合法收入，差额巨大，不能说明来源。

b) 商业伙伴：与企业已经或计划建立某种业务关系的外部方。

c) 利益冲突：员工履职时可能会影响其判断的商业、金钱、家庭、政治或个人利益的情形。企业员工在履行企业职务时，其所代表的企业利益与自身或其关联方利益存在冲突。

d) 尽职调查:进一步评价腐败风险的性质和程度的过程，以帮助企业对特定交易、项目、活动、商业伙伴和员工作出决策。

e) 第三方:独立于企业的个人或机构。

f）公职人员：包括任命或选举产生的拥有立法、司法、执法权力的人员；履行公共职能（包括为政府机关、事业单位、人民团体、国有企业服务）的人员；国内或国际组织的官员或代理人，或公职部门的候选人。

g）有影响力的人：包括公职人员的近亲属或者其他与公职人员关系密切的人；离职的公职人员或者其近亲属以及其他与其关系密切的人。

7.1.10.1.2 相关主要依据

a）《联合国反腐败公约》
b）《经济合作与发展组织反腐败公约》
c）《中华人民共和国刑法》
d）《中华人民共和国反不正当竞争法》
e）《中华人民共和国公司法》
f）《中华人民共和国监察法》
g）《最高人民法院、最高人民检察院关于办理贪污贿赂刑事案件适用法律若干问题的解释》

7.1.10.2 主要合规风险点

依据3.1、3.2规定，合规风险包含企业与员工两个维度，企业与员工的经营管理行为均应合规。

7.1.10.2.1 费用管控

a）现金和现金等价物、礼品、款待与外部差旅

- 企业或其员工向外部方提供现金、现金等价物、礼品、款待或差旅，从而为企业获取或保留业务、争取有利的交易条件或其他商业利益。
- 员工以对外部方提供现金、现金等价物、礼品、款待或差旅为名向企业报销或对外付款，但实际上相关商品或服务并未向外部方提供，而是用于满足员工的私人利益。
- 员工接受外部方提供的现金、现金等价物、礼品、款待或差旅，并为其谋取不正当利益。

b）报销和采购管理

- 企业或其员工向外部方提供现金、现金等价物、礼品、款待或差旅，从而为企业获取或保留业务、争取有利的交易条件或其他商业利益，并进行报销。
- 员工通过舞弊手段向企业申请虚假报销，侵占企业资金。

7.1.10.2.2 与外部各方交往

a）与客户的交往

- 企业或其员工向客户提供不正当利益，从而为企业获取或保留业务、争取有利的交易条件或其他商业利益。客户通过明示或默示的方式，要求企业或其员工向其提供不正当利益。
- 员工利用职务便利，截留销售回款或伪造退款，侵占企业资金；员工利用职务便利，为亲友谋取不正当利益。员工接受客户提供的好处，并为其谋取不正当利益。

b）与供应商的交往

- 企业或其员工向供应商提供不正当利益，以换取对方向企业提供某项关键资源或服务，例如获取垄断材料、设备、信息系统的购买权，获取优惠的采购价格与折扣等。
- 员工与供应商勾结串通，通过不恰当地对外付款侵占企业资金。员工接受供应商提供的好处，并为其谋取不正当利益。

c）与公职人员及有影响力的人的交往

- 企业或其员工向公职人员及有影响力的人提供不正当利益，从而影响某项政府决策。

d）公益性捐赠

- 企业或其员工对外提供不恰当的公益性捐赠，以达到行贿的目的。

e）商业赞助

- 企业或其员工对外提供不恰当的商业赞助，以达到行贿的目的。

f）其他

- 为黑灰产人员提供信息或便利，以谋取不当利益。

7.1.10.2.3 资产管理

a）资金管理

员工通过舞弊手段侵占企业资金，如挪用企业资金用于私人目的。

b）实物资产管理

- 企业或其员工不当处分或使用企业实物资产，以达到行贿的目的，如向公职人员提供企业商品或服务的免费（或低价）使用权。
- 员工通过舞弊手段侵占企业实物资产，如盗窃企业商品、样机、设备等。
- 员工通过舞弊手段挪用企业实物资产，为自己和亲友谋取不正当利益。

c）无形资产管理

- 企业或其员工不当处分或使用企业无形资产，以达到行贿的目的，如通过低价售卖出租企业资产。
- 员工通过舞弊手段侵占或使用企业无形资产，如泄露或出卖企业商业秘密，倒卖产品或广告流量。
- 员工通过舞弊手段不正当使用客户个人信息，如违规出售客户身份证号、手机号码、家庭住址、联络邮箱等个人信息。
- 员工通过舞弊手段非法侵入或破坏公司计算机信息系统，为自己或他人谋取不正当利益。

7.1.10.2.4 人事管理

a）招聘管理

- 员工帮助密切关系人获取企业或企业商业伙伴的工作机会。

b）薪酬与待遇管理

- 员工帮助密切关系人获取高于其实际工作表现的薪酬待遇，如任人唯亲、偏袒特定人员。
- 员工通过舞弊手段虚构业绩，套取公司奖励。

c) 影子员工及考勤管理

- 员工利用职务便利，实施“吃空饷”行为，如虚构人员编制，为不存在的员工支付工资。

d) 内部利益冲突

- 员工及其关联方均在企业任职，且属于不相容职责岗位。

e) 外部利益冲突

- 员工或其关联方与企业存在外部利益冲突，如与企业存在直接交易的利益冲突。

7.1.10.2.5 其他

a) 刑事法律风险

企业或其员工违规行为情节严重的，可能触犯刑法，涉及的相关罪名：

- 企业构成的单位犯罪：单位行贿罪、对单位行贿罪、对非国家工作人员行贿罪、对外国公职人员/国际公共组织官员行贿罪、单位受贿罪。
- 员工构成的个人犯罪：贪污罪、巨额财产来源不明罪、职务侵占罪、受贿罪、非国家工作人员受贿罪、挪用公款罪、挪用资金罪、行贿罪、对非国家工作人员行贿罪、对外国公职人员/国际公共组织官员行贿罪、对有影响力的人行贿罪、对单位行贿罪、介绍贿赂罪、盗窃罪、内幕交易罪、泄露内幕信息罪、侵犯商业秘密罪、侵犯公民个人信息罪、非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪、非法控制计算机信息系统罪、破坏计算机信息系统罪、诈骗罪。

7.1.10.3 具体实施措施

7.1.10.3.1 反腐败原则、目标、方针

a) 反腐败原则:零容忍、全覆盖、无禁区。
b) 反腐败目标：构建不敢腐、不能腐、不想腐的体制机制，最大限度根除腐败违规问题。
c) 反腐败方针：反腐败工作的方针是坚持“标本兼治、综合治理、惩防并举、注重预防”。维护企业核心价值观，倡导风清气正的廉洁文化，护航企业业务行稳致远。

7.1.10.3.2 反腐败主要/核心合规内容

a) 禁止对外行贿

i)与公职人员的往来

企业在与各国政府及公职人员往来的过程中，注意企业的行为是否可能违反当地法律的禁止性规定。企业不允许员工及商业伙伴以任何形式故意地支付贿赂款项以获取不正当利益或竞争优势。

ii)礼品招待

企业与员工不得以任何借口主动向任何商业伙伴或寻求合作的第三方索要礼品与招待，不得提供意在产

生不当影响或可能产生行贿嫌疑的礼品招待。

iii)捐赠与赞助

任何直接或间接的公益捐赠与赞助，不得存在腐败或腐败嫌疑。

iv)与商业伙伴交往

员工在与商业伙伴交往过程中恪守职业道德，严禁任何腐败行为，并对合作伙伴进行适当监督，以防企业利益受损。

v)差旅资助

企业为外部人员承担或支付差旅费用，宜存在正当合理的商业目的，并且企业提供差旅的内容、金额和方式是恰当、得体的。

vi)外部索贿与勒索

外部人员（例如公职人员、客户、商业伙伴等）利用自身权力或职务便利，直接或间接向企业或员工代表索要财物或好处的，予以明确拒绝。

b) 禁止内部腐败

i)索贿与受贿

企业禁止员工进行任何形式的索贿与受贿行为，员工亦不以接受方的身份收受商业伙伴相关人员的不当给付，员工任何形式的消费不得让商业伙伴相关人员代为付费。

ii)职务侵占

企业合法合规运营，禁止员工实施、参与、协助或默许任何职务侵占行为。禁止员工利用职务便利，挪用、占有、盗窃或不正当使用企业财产或资源，为本人、其利害关系人或他人谋取利益。

iii)人事腐败

- 对外招聘与雇佣员工时，遵循企业廉洁要求，避免谋求不正当利益或通过违规方式，进行招聘与雇佣活动。
- 避免任人唯亲、偏袒特定人员，以给予不符合其工作表现的人事考评结果和内部待遇，如绩效、薪酬、奖金、晋升等。
- 帮助违纪员工免受处罚，或帮助其减轻处罚。

iv)利益冲突

企业可要求员工在处理利益冲突事项时，做到合法合规、以企业利益为先，主动规避利益冲突，自觉评估利益冲突风险，对利益冲突事项进行主动报备。

7.1.10.3.3 主要责任人和职能部门

a) 合规管理责任人（首席合规官）

合规管理责任人对实施和符合反腐败合规管理体系的情况负总责，合规管理责任人可通过下述方面证实

其在反腐败合规管理体系方面的领导作用和承诺：

i)确保建立、实施、保持和评审反腐败合规管理体系，包括方针和目标，以充分处置企业的腐败风险。

ii)确保反腐败合规管理体系得到适当设计以实现其目标，为反腐败合规管理体系的有效运行配备充足的和适宜的资源，确保反腐败合规管理体系要求融入企业的过程；

iii)内、外部沟通有效的反腐败合规管理和符合反腐败合规管理体系要求的重要性，支持其他相关管理角色在预防和发现腐败方面展示其职责范围内的领导作用；指导并支持员工对反腐败合规管理体系的有效性做出贡献；

iv)鼓励使用报告涉嫌或实际腐败的程序，确保没有员工因善意的或基于合理的判断对违反或涉嫌违反企业反腐败方针进行报告，或因拒绝参与腐败（即使拒绝会造成企业失去业务）而遭受报复、歧视或处罚（个人参与违反活动时除外），在企业内部推动适宜的反腐败文化；

v)按照计划的时间间隔向治理机构（如有）报告反腐败合规管理体系，以及严重的或系统性腐败指控的内容和运行情况；推动持续改进。

b）反腐败管理职能部门

合规管理责任人（首席合规官）给反腐败合规职能部门分配以下方面的职责和权限：

i)监督企业反腐败合规管理体系的设计和实施；

ii)为员工在反腐败合规管理体系和腐败相关问题方面提供建议和指导；

iii)适用时，向合规管理责任人报告反腐败合规管理体系的绩效。

- 提供充分的资源并分配有适当能力、地位、权限和独立性的人员给予反腐败合规职能。
- 如果需要提出与腐败或反腐败管理体系有关的任何事项或关注重点，反腐败合规职能可以直接并迅速联系合规管理责任人。
- 合规管理责任人可以将一些或全部反腐败合规职能分配给企业外部人员。如果对外授权，合规管理责任人确保这些人员对那些分配给外部的职能负责并对其有权限。

7.1.10.3.4 具体实施措施

a）确定反腐败管理体系

i)企业可建立、记录、实施、保持和持续评审、并且在必要时完善反腐败管理体系，包括所需过程及其相互作用。反腐败管理体系可包含设计旨在识别和评估腐败风险，并预防、发现和对腐败作出响应的措施。

ii)企业确定反腐败管理体系的边界和适用性，以建立其范围。确定范围时，可考虑所涉及的内外部事项、涉及的要求、涉及的腐败风险评价结果等因素。

b）腐败风险评价

i)企业定期进行腐败风险评价：

- 考虑到企业和环境因素，确定企业可以合理预期的腐败风险；

- 对识别的腐败风险进行分析、评价和排列优先顺序；
- 评价企业中现有降低已评价腐败风险的控制措施的适用性和有效性。

ii)企业为评价腐败风险水平建立准则，并考虑企业的方针和目标。

iii)腐败风险评价得到评审：

- 定期根据企业确定的时间和频率对变化和新信息适当评价；
- 在企业架构或活动发生重大变化时。

iv)企业宜保留证明已进行腐败风险评价并用于设计或改进反腐败管理制度的文件资料。

c）意识和培训

企业宜给员工提供足够和适宜的反腐败意识和培训。组织员工参与反腐败合规培训，针对关键业务环节以及高风险部门，开展常态化合规培训。

d）运行策划与控制

企业可策划、实施、评审和控制满足反腐败合规管理体系要求所需过程，通过：

i)建立过程准则；

ii)按照准则实施过程控制；

iii)保存必要的文件化信息以达到对过程按照策划实施有信心的程度。关键确认节点可进行电子签约、可信存证，规避系统性风险。

e）尽职调查

腐败风险评审时，发现以下较高腐败风险的，开展尽职调查：

i)特定交易、项目或活动；

ii)计划或正在与特定类型的商业伙伴建立或维持业务关系；或

iii)担任某些职位的特定员工。

企业宜评估属于这些类型的特定交易、项目、活动、商业伙伴和员工相关的腐败风险性质和程度。评估可包括任何必要的尽职调查，以获得足够的信息来评估腐败风险。尽职调查应按规定的频率更新，充分考虑新的变化和信息。

f）财务控制与非财务控制

i)企业可实施管理腐败风险的财务控制。

ii)企业可在采购、运营、销售、业务、人力资源、法律和监管活动以及其他非财务业务管理方面采取措施以降低腐败风险。

制定完善商业行为准则相关规章制度，落实员工日常行为的要求准则，如《员工行为准则》等规章制度，明确员工实施商业贿赂行为将受到的纪律处分措施和法律责任。

g）对受控企业和商业伙伴实施的反腐败控制

i)企业可实施程序要求其受控企业实施企业的反腐败管理体系，或实施自身的反腐败控制。

ii)对于不受企业控制且腐败风险评审和尽职调查已经识别具有较高腐败风险的商业伙伴，当企业实施的反腐败控制有助于降低相关腐败风险时，企业可按照以下实施程序：

- 企业确定商业伙伴是否有管理相关腐败风险的反腐败控制；
- 当商业伙伴没有反腐败控制，或无法验证其是否有反腐败控制时：企业可适时要求商业伙伴实施与交易、项目或活动相关的反腐败控制；或当要求商业伙伴实施反腐败控制不可行时，这可作为评价与商业伙伴关系合作关系以及企业管理这些腐败风险的考虑因素。

iii)反腐败承诺

对于造成较高腐败风险的商业伙伴，只要可行，企业应实施程序要求：

- 商业伙伴承诺在相关交易、项目、活动或关系中，防止存在由商业伙伴、代表商业伙伴或为商业伙伴的利益而进行的腐败行为；
- 当在相关交易、项目、活动或关系中，存在由商业伙伴、代表商业伙伴或为商业伙伴的利益而进行的腐败行为时，企业能够终止与商业伙伴的关系；
- 当满足以上两点要求不可行时，可作为评价与商业伙伴关系合作关系以及企业管理这些腐败风险的考虑因素。

h) 管理反腐败控制的不足

当对特定交易、项目、活动或与商业伙伴关系进行的尽职调查证实现有的反腐败控制管理不了腐败风险，并且企业不能或不希望实施额外的或增强的反腐败控制或采用其他适宜措施（如改变交易、项目、活动或关系的性质）使企业能够管理相关腐败风险时，企业可：

- 如果是已经开展的交易、项目、活动或业务关系，根据交易、项目、活动或关系的风险和性质采取合适的措施；如果可行，尽快终止、停止、暂停或撤销交易、项目、活动或业务关系。
- 对于提出的新交易、项目、活动或关系，推迟或拒绝继续。

i) 提出关注

企业可实施以下程序：

- 鼓励和使人们能够善意的或基于合理的信心向反腐败合规职能或适当人员（可以是直接的，也可以通过适当的第三方）报告有企图、涉嫌和实际的腐败，或任何对反腐败管理体系的违反或反腐败管理体系的弱点；
- 除了推进调查的需要，要求企业对报告进行保密，以便保护报告人和报告中所涉及或提到的其他人员的身份；
- 允许匿名举报，鼓励实名举报；
- 禁止报复，并保护举报人在善意或基于合理判断的情况下，提出或报告有关企图、实际或涉嫌腐败以及违反反腐败方针或反腐败管理体系的问题时，免遭报复；
- 如果面对可能涉及腐败的关注或状况时，使员工能够从适当的人员处得到做什么的建议。
- 企业宜确保所有员工知道、能够使用报告程序，并且知道到该程序中自己拥有的权利和得到的保护。

j) 调查和处理腐败

i)企业可建立腐败调查程序，以实现：

- 要求评价、适当时调查任何报告、发现或合理怀疑的腐败或违反反腐败方针或反腐败管理体系的行为；
- 调查发现腐败或对反腐败方针或反腐败管理体系的违反，采取适当措施；
- 授权或批准调查人员；
- 要求相关人员在调查过程中配合；
- 确保向反腐败合规职能和适当时其他合规职能报告调查的状态和结果；
- 要求调查的实施和输出是保密的。

由独立于被调查角色和职能的人员实施调查和接受报告。企业可以委派商业伙伴实施调查并向独立于被调查角色和职能的人员报告。

ii)畅通反腐败监督举报机制，以实现：

- 提供多种举报渠道，如实体举报箱、举报热线电话、举报邮箱、邮寄地址等。举报途径区分外部独立第三方合规举报、内部合规举报。
- 谨慎甄别有效举报与恶意举报。对于有效举报行为，根据规定程序开展合规调查。

7.1.10.3.5 纠错与持续改进机制

a) 不符合和纠正措施

当出现腐败风险时，企业可：

i)立即对腐败风险做出反应，并且在适用时：

- 采用相应调查取证设备收集、固定、恢复相关证据；
- 采取措施控制和纠正腐败风险；
- 处理后果；

ii)为防止腐败风险再次发生或在其他地方发生，通过以下方式评估消除腐败风险原因所需的措施。

- 评审腐败风险；
- 确定腐败风险的原因；
- 确定是否存在或可能发生类似的腐败风险；

iii)确定需要采取的措施；

iv)评审所采取纠正措施的有效性；

v)必要时，对反腐败合规管理体系进行变更。

b) 持续改进

企业宜持续改进反腐败管理体系的适宜性、充分性和有效性。

7.1.11 反垄断

7.1.11.1 平台经济领域反垄断制度概述

7.1.11.1.1 相关术语概念及其定义

a) 平台：本章节内所称平台为互联网平台，是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。
b) 平台经营者：向自然人、法人及其他市场主体提供经营场所、交易撮合、信息交流等互联网平台服务的经营者。
c) 平台内经营者：在互联网平台内提供商品或者服务（以下统称商品）的经营者。平台经营者在运营平台的同时，也可能直接通过平台提供商品。
d) 平台经济领域经营者：包括平台经营者、平台内经营者以及其他参与平台经济的经营者。
e) 平台经济领域垄断协议：经营者排除、限制竞争的协议、决定或者其他协同行为。协议、决定可以是书面、口头等形式。其他协同行为是指经营者虽未明确订立协议或者决定，但通过数据、算法、平台规则或者其他方式实质上存在协调一致的行为，有关经营者基于独立意思表示所作出的价格跟随等平行行为除外。

7.1.11.1.2 相关主要依据

a) 《中华人民共和国民法》
b) 《中华人民共和国反垄断法》（以下简称“《反垄断法》”）
c) 《中华人民共和国电子商务法》
d) 《国务院反垄断委员会关于平台经济领域的反垄断指南》
e) 《国务院反垄断委员会经营者反垄断合规指南》
f) 国家市场监督管理总局《禁止滥用市场支配地位行为暂行规定》
g) 国家市场监督管理总局《禁止垄断协议暂行规定》
h) 国家市场监督管理总局反垄断局《关于经营者集中申报的指导意见》

7.1.11.2 主要合规风险点

a) 垄断协议

i)横向垄断协议

平台经营者与竞争者之间的沟通互动宜保持审慎原则，下列行为存在高度违规风险：

- 与竞争者达成固定价格、分割市场、限制产（销）量、限制新技术（产品）、联合抵制交易等《反垄断法》禁止的横向垄断协议；
- 《国务院反垄断委员会关于平台经济领域的反垄断指南》等相关法律法规和规范性文件中规定的具有竞争关系的平台经营者可能达成横向垄断协议的情形；

ii)纵向垄断协议

平台经营者在与平台内经营者等交易相对人互动过程中，不宜实施下列行为：

- 直接固定交易相对人向第三人转售商品的价格，或者限定交易相对人向第三人转售商品的最低价格等《反垄断法》禁止的纵向垄断协议；
- 《国务院反垄断委员会关于平台经济领域的反垄断指南》等相关法律法规和规范性文件中规定的具有竞争关系的平台经营者与交易相对人可能达成纵向垄断协议的情形。

iii)轴幅协议

平台经营者利用与平台内经营者的上下游关系时，宜对下列行为高度注意：

利用其与平台内经营者的上下游交易关系，通过技术手段、平台规则、数据和算法等方式，组织或帮助具有竞争关系的平台内经营者，达成或实施具有排除、限制竞争效果的协议、决定或其他协同行为。

b）滥用市场支配地位风险

i)合规风险识别和提醒

平台经营者可客观评估自身财力、技术条件及控制市场的能力，所占据的市场份额以及相关市场竞争状况，来认定自身是否具备市场支配地位。如存在《反垄断法》《国务院反垄断委员会关于平台经济领域的反垄断指南》《国务院反垄断委员会经营者反垄断合规指南》规定的平台经营者可能被推定为具有市场支配地位的情况，平台经营者应更谨慎评估自身所实施的单方行为及其他多方协作行为。

ii)主要合规风险点

可能具有市场支配地位的平台经营者实施下列行为，存在较高合规风险，宜审慎评估：

- 以不公平的高价销售商品或者以不公平的低价购买商品；
- 以低于成本的价格销售商品；
- 利用平台规则、算法以及其他技术手段设置不合理的限制或者障碍，拒绝与交易相对人交易；
- 要求交易相对人在其与竞争性平台之间进行“二选一”，限定交易相对人与其进行独家交易，或者限定交易相对人只能与其指定的经营者交易，或者限定交易相对人不得与特定经营者进行交易；
- 利用格式条款、弹窗、操作必经步骤等交易相对人无法选择、更改、拒绝的方式将不同商品进行捆绑销售，或无正当理由，以搜索降权、流量限制、技术障碍等惩罚性措施，强制交易相对人接受其他商品，或者附加不合理交易条件；
- 基于大数据和算法，根据交易相对人的支付能力、消费偏好、使用习惯等，实行差异性交易价格或者其他交易条件；
- 要求交易相对人在商品价格、数量、品类等方面向其提供等于或者优于其他竞争性平台的交易条件；
- 法律行政法规规定的其他可能构成滥用市场支配地位的情形。

c）经营者集中

平台经济领域经营者在进行投资并购、设立合营企业等经营行为时，宜主动评估是否需要开展经营者集中申报，如达到国务院规定的以下申报标准应依法进行申报：

- 参与集中的所有经营者上一会计年度在全球范围内的营业额合计超过 100 亿元人民币，并且其中至少两个经营者上一会计年度在中国境内的营业额均超过 4 亿元人民币；
- 参与集中的所有经营者上一会计年度在中国境内的营业额合计超过 20 亿元人民币，并且其中至少两个经营者上一会计年度在中国境内的营业额均超过 4 亿元人民币。

未达申报标准的情况下，平台经济领域经营者可以自愿进行经营者集中申报。当参与集中的一方经营者为初创企业或者新兴平台、参与集中的经营者因采取免费或者低价模式导致营业额较低、相关市场集中度较高、参与竞争者数量较少等类型的经营者集中，参与集中的平台经济领域经营者应高度关注并审慎评估集中是否具有排除、限制竞争效果。

d）滥用行政权力排除、限制竞争行为

平台经济领域经营者宜知悉反垄断法相关规定所禁止的行政机关和法律、法规授权的具有管理公共事务职能的组织滥用行政权力，实施排除、限制竞争的行为。

行政机关和法律、法规授权的具有管理公共事务职能的组织滥用行政权力要求平台经济领域经营者实施垄断行为的，应当及时评估相应的法律风险，依法依规生产经营，避免实施违反《反垄断法》的行为。积极抵制对未列入政府定价目录内的商品制定政府定价或者政府指导价及其他的强制性市场干预行为，并向反垄断执法机构投诉和举报。

e）配合外部调查

反垄断执法机构已经对涉嫌垄断行为立案并启动调查程序时，平台经济领域经营者宜立即停止实施相关行为，主动向反垄断执法机构报告，并积极配合反垄断执法机构的调查。如果符合《国务院反垄断委员会横向垄断协议案件宽大制度适用指南》要求的，可以申请适用宽大制度。

7.1.11.3 具体实施措施

7.1.11.3.1 平台反垄断基本原则

平台反垄断合规工作宜遵循诚实守信、公平竞争、开拓创新、推动经济发展的原则。平台宜诚信经营，维护消费者利益和社会公共利益；主动承担起维护市场秩序的职责，保护市场公平竞争；投入有效资源，创新合规管理的方式，完善合规管理制度；促进平台经济健康有序发展，构筑经济社会发展新优势和新动能。

7.1.11.3.2 平台反垄断工作目标

建立健全平台反垄断管理制度，依法开展公平竞争，防止垄断协议、滥用市场支配地位、限制排除竞争等行为，共同营造公平有序的市场竞争环境，维护互联网行业市场秩序、维护消费者利益和社会公共利益。

7.1.11.3.3 建立合规制度

鼓励平台建立并有效执行反垄断合规管理制度，有助于提高经营管理水平，避免引发合规风险，树立依法经营的良好形象。

平台可以根据业务状况、规模大小、行业特性等，建立反垄断合规管理制度，或者在现有合规管理制度中开展反垄断合规管理专项工作。设置反垄断合规管理部门或指定反垄断合规管理负责人，明确合规管理职责，建立完善的合规管理体系。

7.1.11.3.4 平台反垄断合规管理机构和合规管理负责人

鼓励具备条件的平台经营者建立反垄断合规管理部门，或者将反垄断合规管理纳入现有合规管理体系；明确合规工作职责和负责人，完善反垄断合规咨询、合规检查、合规汇报、合规培训、合规考核等内部机制，降低平台及员工的合规风险；平台宜配置必要的资源，保证反垄断合规管理部门及其负责人具备足够的独立性和权威性。

鼓励平台设置反垄断合规负责人，领导合规管理部门执行决策管理层对反垄断合规管理的各项要求，协调反垄断合规管理与平台各项业务的关系，监督合规管理执行情况。鼓励平台高级管理人员领导或者分管反垄断合规管理部门，承担合规管理的组织实施和统筹协调工作。

鼓励反垄断合规管理部门和合规管理负责人履行以下职责：

- 加强对国内外反垄断法相关规定的研究，推动完善合规管理制度；定期进行合规风险识别、评估，涉外业务中，及时进行境外风险提示，加强风险研判能力；组织开展反垄断合规培训，建立专业化、高素质的合规管理队伍；鼓励平台高级管理人员作出并履行明确、公开的反垄断合规承诺，鼓励其他员工作出并履行相应的反垄断合规承诺，在合规管理制度中明确有关人员违反职责的后果。

- 组织开展合规检查、监督、审核、评估平台及员工经营活动和业务行为的合规性，及时制止并纠正不合规的经营行为，对违规人员进行责任追究或者提出处理建议；定期向企业管理层、决策层递送反垄断合规管理情况报告；积极主动地配合反垄断执法机构依法对涉嫌垄断行为进行调查，及时提供相关文件资料、信息或者获取相关文件资料、信息权限。
- 建立健全风险处置机制，对识别、提示和评估的各类合规风险采取恰当的控制和应对措施；在发现合规风险时，立即停止实施相关行为，依法及时采取补救措施；主动向反垄断执法机构报告并配合工作，争取适用承诺制度和宽大制度，减轻损失。

7.1.11.3.5 宽大制度

宽大制度是指达成横向垄断协议的平台经营者，主动向反垄断执法机构报告达成垄断协议的有关情况并提供重要证据，反垄断执法机构可以酌情减轻或者免除对该平台经营者的处罚。

a）满足以下条件的平台经营者可以适用宽大制度：

i)平台达成横向垄断协议，是指《反垄断法》第十三条第一款所规定的具有竞争关系的经营者达成的垄断协议；

ii)经营者申请宽大应按照要求提交报告、证据,并且全部满足下列条件,可以获得宽大：

- 申请宽大后立即停止涉嫌违法行为,但执法机构为保证调查工作顺利进行而要求经营者继续实施上述行为的情况除外。经营者已经向境外执法机构申请宽大，并被要求继续实施上述行为的，应当向执法机构报告；
- 迅速、持续、全面、真诚地配合执法机构的调查工作；
- 妥善保存并提供证据和信息,不得隐匿、销毁、转移证据或者提供虚假材料、信息；
- 未经执法机构同意不得对外披露向执法机构申请宽大的情况；
- 不得有其他影响反垄断执法调查的行为。
- 平台经营者组织、胁迫其他经营者参与达成、实施垄断协议或者妨碍其他经营者停止该违法行为的，执法机构不对其免除处罚，但可以相应给予减轻处罚。

b）平台经营者申请适用宽大制度的程序：

- 参与垄断协议的平台经营者可以在执法机构立案前或者依据《反垄断法》启动调查程序前，也可以在执法机构立案后或者依据《反垄断法》启动调查程序后、作出行政处罚事先告知前，向执法机构申请宽大；
- 平台提交垄断协议有关情况的报告及重要证据。
- 重要证据是指：（一）执法机构尚未掌握案件线索或者证据的，足以使执法机构立案或者依据《反垄断法》启动调查程序的证据；（二）执法机构立案后或者依据《反垄断法》启动调查程序后，经营者提供的证据是执法机构尚未掌握的，并且能够认定构成《反垄断法》第十三条规定的垄断协议的；
- 申请宽大报告可以是口头或者书面形式；
- 对垄断协议案件平台主动报告并提供重要证据直至持续配合调查终结的，依申请，反垄断执法机构会根据平台主动报告的时间顺序、提供证据的重要程度以及达成、实施垄断协议的有关情况，决定是否减轻或者免除处罚。

对于第一个申请者，反垄断执法机构可以免除处罚或者按照不低于百分之八十的幅度减轻罚款；对于第二个申请者，可以按照百分之三十至百分之五十的幅度减轻罚款；对于第三个申请者，可以按照百分之二十至百分之三十的幅度减轻罚款。

经营者申请宽大的具体适用标准和程序等可以参考《禁止垄断协议暂行规定》、《国务院反垄断委员会横向垄断协议案件宽大制度适用指南》。

7.1.11.3.6 鼓励建设合规文化

a) 积极培育合规文化，通过合规管理培训、签订合规承诺书等方式，帮助和督促员工了解并遵守反垄断法相关规则，强化合规意识，培养在调查工作中积极配合的自觉。

b) 可以建立内部反垄断合规举报政策，并承诺为举报人的信息保密以及不因员工举报行为而采取任何对其不利的措施，鼓励员工敢于举报，形成良好的竞争风气。

c) 鼓励平台强化合规管理信息化建设，建立合规管理专门系统，通过信息化手段优化管理流程，提升工作效率，加强对合规管理情况的监控和分析。

d) 鼓励平台建立专业化、高素质的合规管理队伍，根据业务规模、合规风险水平等因素配备合规管理人员，提升队伍能力水平，增强团队凝聚力。

7.1.11.3.7 鼓励平台建立动态反垄断风险预防与识别体系机制

平台宜对反垄断合规管理体系的运行效果进行定期评估，对于合规管理体系自身的漏洞宜进行完善和修改，对于运行过程中面临的主要反垄断风险宜制定针对性的合规管理措施，明确合规风险重点，降低合规风险。平台宜根据自身需要和实际情况及时调整风险评估、风险处置等具体规定，对现实发生的合规风险采取恰当的应对措施，强化合规管理的针对性和科学性。同时，平台宜根据实际情况灵活调整培训计划，投入有效资源，提高合规队伍能力水平，持续全方位完善合规管理体系。

平台宜适时更新合规管理制度，顺应反垄断相关法律制度的更迭和监管趋势的变化，确保合规管理机制的持续有效性。

7.1.12 反不正当竞争

7.1.12.1 反不正当竞争合规管理概述

7.1.12.1.1 术语和定义

下列术语和定义适用于本章节。

a) 反不正当竞争合规风险：企业及其员工因实施反不正当竞争领域的不合规行为，引发法律责任、受到相关处罚、造成经济或声誉损失及其他负面影响的可能性。

b) 第三方：除企业及其员工之外的自然人、法人和非法人组织。

c) 经营者：从事商品生产、经营或者提供服务的自然人、法人和非法人组织。

7.1.12.1.2 相关主要依据

《中华人民共和国反不正当竞争法》（以下简称“《反不正当竞争法》”）

7.1.12.2 合规职能部门及职责

企业合规职能部门和职责参见第5条。在此基础上，企业宜根据自身业务状况、经营规模、合规需求等实际情况，设立反不正当竞争合规管理组织或指定反不正当竞争合规管理负责人，相关人员宜具备专业知识、经验和技能，以协助企业有效开展合规工作。

7.1.12.3 主要合规风险

企业从事生产经营活动，应当遵守《反不正当竞争法》以及相关法律法规和规范性文件的规定，不应实施《反不正当竞争法》以及其他法律法规和规范性文件禁止的不正当竞争行为。
信息通信和互联网企业应特别注意以下反不正当竞争合规风险：

7.1.12.3.1 仿冒混淆行为风险

企业不得实施混淆行为，引人误认为是他人商品、服务或者与他人存在特定联系。除《反不正当竞争法》第六条规定的情形外，擅自使用他人有一定影响的应用软件、网店、自媒体、游戏界面的页面设计、名称、图标、形状等相同或近似的标识，引人误认为是他人商品或者与他人存在特定联系，存在反不正当竞争合规风险。

7.1.12.3.2 虚假或引人误解商业宣传行为风险

企业不得通过虚假交易、组织虚假交易等方式进行虚假宣传，不得故意帮助其他经营者实施虚假交易行为，或者故意为虚假交易行为提供便利条件。

企业实施下列行为宣传自身或商品的性能、功能、质量、销售状况、用户评价、曾获荣誉等，进行虚假或引人误解的商业宣传，存在反不正当竞争合规风险：

- 虚构交易量、成交量、预约量等与经营有关的数据信息。
- 伪造物流单据。
- 虚构用户评价、诱导用户作出指定好评，或者无正当理由删除、隐匿、屏蔽、压制用户负面评价等。

7.1.12.3.3 商业诋毁行为风险

企业不得编造、传播虚假信息或者误导性信息，损害竞争对手商业信誉、商品声誉。企业组织、指使他人对竞争对手或其商品进行恶意评价，或者利用大众媒介、信息网络散布虚假或者误导性信息，损害竞争对手商业信誉、商品声誉的，存在反不正当竞争合规风险。

7.1.12.3.4 干扰、恶意不兼容风险

企业不得利用技术手段，通过影响用户选择或者其他方式，实施妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的不正当竞争行为。企业实施下列行为干扰、恶意不兼容其他经营者合法提供的网络产品或者服务的，存在反不正当竞争合规风险：

- 违背用户意愿下载、安装、运行应用程序，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行；
- 无正当理由，对其他经营者合法提供的网络产品或者服务实施屏蔽、拦截、拖延审查，以及其他干扰接入、下载、安装、运行、升级、更新、转发、传播等的行为；
- 恶意不兼容其他经营者合法提供的网络产品或者服务等。

企业利用技术手段，导致其他经营者合法提供的网络产品或者服务无法正常下载、安装、运行、更新或者卸载，或者以其他方式导致其他经营者、用户利益遭受不合理损失的，存在反不正当竞争合规风险，企业实施相关行为需高度谨慎。

7.1.12.4 具体实施措施

7.1.12.4.1 反不正当竞争合规原则、目标、方针

a）合规原则

企业合规管理总体原则参见第4条。在此基础上，企业反不正当竞争合规管理应确保企业从事生产经营活动遵循自愿、平等、公平、诚信的原则，遵守法律法规，遵循商业道德，公平参与市场竞争，不实施或者帮助他人实施不正当竞争行为、扰乱市场正常的竞争秩序、损害其他经营者和消费者的合法权益。

b）合规目标和方针

企业合规管理总体目标参见引言部分。在此基础上，企业开展反不正当竞争合规管理工作的目标在于自主防范反不正当竞争合规风险，预防和避免实施不正当竞争行为，维护公平竞争的市场秩序，保护经营者和消费者的合法权益。企业反不正竞争合规方针应与合规目标保持一致。

7.1.12.4.2 主要合规内容

企业宜建立健全反不正当竞争合规管理制度，制定全体员工普遍遵守的竞争行为规范和准则，识别、应对、预防反不正当竞争合规风险。

7.1.12.4.3 合规管理重点环节

企业合规管理重点环节参见第7.2条。在此基础上，企业进行反不正当竞争合规管理，宜对经营活动中可能存在的反不正当竞争合规风险进行全面梳理，对风险发生的可能性、影响程度、潜在后果进行系统整理和分析，对于典型性、普遍性和可能产生较严重后果的风险及时预警，并按照影响程度大小确定合规整改优先级，逐步推进整改工作。

7.1.12.4.4 合规培训

企业宜定期开展反不正当竞争合规培训，以确保企业各部门及员工充分理解、遵循企业竞争合规目标和合规管理制度。合规培训宜覆盖企业全体员工，针对核心业务部门和重要风险部门及所属员工可进行重点培训。培训可由企业合规管理部门组织安排，也可委托第三方专业机构。

7.1.12.4.5 举报和投诉

企业宜建立不正当竞争行为举报投诉机制或将其纳入企业已有的监督机制中，鼓励企业员工、用户、客户、供应商以及其他合作方，针对企业或员工的不合规行为进行举报、投诉、报告和反馈（以下统称为“举报”），以防范和纠正企业的反不正当竞争合规风险。

企业应当保护举报人的人身权利、财产权利、名誉权利和其他合法权益，对举报人的信息履行严格保密义务。企业应禁止任何部门或员工对举报人进行任何形式的报复，对于员工不得采取降低绩效考核等级、降薪、扣减奖金、调职、降职、解除劳动合同以及其他任何经济或声誉方面的报复行为。对经过调查核实的举报，企业可以给予举报人相应的奖励。

7.1.12.4.6 调查

企业宜依据企业合规制度、政策、流程要求，基于企业现有资源和组织架构，建立内部调查流程，及时处理举报事项并向相关人员反馈处理结果，确保内部调查流程合法合规。

7.1.12.4.7 合规问责

经过调查核实确有不合规行为的，调查部门应通知不合规部门进行合规整改，不合规部门应及时整改并反馈整改结果。

企业宜建立并完善反不正当竞争合规风险行为内部惩处机制，明确责任范围，细化处罚标准和处理措施，

严肃追究相关方的责任。对涉嫌构成犯罪的人员和组织，应移送司法机关处理。

7.1.12.4.8 合规文化培育

企业宜将反不正当竞争合规文化作为企业文化建设的重要内容，积极培育竞争合规文化，可通过组织合规培训、撰写合规手册、制作传播合规宣传媒介等方式，增强全体员工的竞争合规意识，树立合规经营、公平竞争的价值观，自觉维护市场公平竞争秩序。

7.1.12.4.9 合规管理有效性评估

企业宜针对反不正当竞争合规管理机制的运行和效果进行专门的审核或评估，以确保反不正当竞争合规管理的有效性。审核和评估可由企业内部审计部门或其他内部监督部门进行，也可委托独立、专业的第三方机构。

7.1.12.4.10 纠错和持续改进

企业宜根据反不正当竞争合规运行情况和合规管理有效性评估结果，对于合规管理体系进行分析，针对重大和重复出现的反不正当竞争合规风险，以及出现重大不合规和重复不合规的部门和员工，彻查不合规原因和管理漏洞，完善和修改具体的合规管理制度，强化对合规管理流程的管控，加大培训力度，持续完善合规管理体系。

企业宜实时跟踪反不正竞争相关法律制度的更迭和监管趋势的变化，及时更新合规管理制度，确保合规管理机制持续改进。

7.1.13 知识产权

7.1.13.1 知识产权概述

7.1.13.1.1 术语与定义

a) 知识产权是权利人依法就下列客体享有的专有的权利：

- 作品；
- 发明、实用新型、外观设计；
- 商标；
- 地理标志；
- 商业秘密；
- 集成电路布图设计；
- 植物新品种；
- 法律规定的其他客体。

7.1.13.1.2 合规主要依据

a）《中华人民共和国专利法》
b）《中华人民共和国商标法》
c）《中华人民共和国著作权法》
d）《中华人民共和国专利法实施细则》
e）《中华人民共和国商标法实施条例》

f）《中华人民共和国著作权法实施条例》
g）《计算机软件保护条例》
h）《中华人民共和国植物新品种保护条例》
i）《集成电路布图设计保护条例》

7.1.13.2 合规主要风险点

7.1.13.2.1 资源管理风险

a）人事合同：在劳动合同、劳务合同等方式中没有对员工进行知识产权权属规定、保密限制和竞业限制，会导致出现知识产权权属纠纷，泄露技术秘密和知识产权侵权等风险。
b）入职：对新入职员工没有进行适当的知识产权背景调查，导致侵犯他人知识产权。
c）离职：涉及核心知识产权的员工离职时，没有签署离职知识产权协议或执行竞业限制协议，很难规避企业的知识产权被侵权。
d）外部合作：在与合作方的合作合同、合作协议中，未对各方的知识产权权属进行约定，以及备选地未对必要的保密限制和相关参与人员的竞业限制等进行约定，导致出现知识产权权属纠纷，以及可能存在的泄露技术秘密和知识产权侵权等风险。
e）供应链管理：在采购、销售合同中未对各方的知识产权权属进行约定，以及备选地未对必要的保密限制和相关参与人员的竞业限制等进行约定，导致出现知识产权权属纠纷，以及可能存在的泄露技术秘密和知识产权侵权等风险。

7.1.13.2.2 知识产权全过程管理风险

在知识产权获取、维护、运用和保护过程中，没有建立合规的知识产权合规管理运行体系，导致存在发生知识产权纠纷的风险。

7.1.13.3 合规管理措施

7.1.13.3.1 知识产权合规管理原则

a）战略导向：统一部署经营发展、科技创新和知识产权战略，使三者互相支撑、互相促进。
b）领导重视：领导的支持和参与是知识产权管理的关键，管理层应全面负责知识产权管理。
c）全员参与：知识产权涉及企业各业务领域和各业务环节，应充分发挥全体员工的创造性和积极性。

7.1.13.3.2 具体实施措施

a）提升企业知识产权保护与合规意识，加强对企业创新创意成果的知识产权保护，规范企业对知识产权的使用管理，防止侵权行为的发生。包括但不限于：

- 建立并完善知识产权合规管理组织体系，明确合规职责、建立合规组织保障、加强内部职能配合；
- 加强完善知识产权合规管理制度体系，落实合规审查、监察、举报、绩效评价、调查、保密等合规环节，确保其有效性；
- 加强知识产权合规管理运行体系建设，确保各类知识产权获取、维护、运用；
- 完善知识产权合规风险识别处理体系，强化知识产权合规风险识别、预警、监察、评估管理，降低知识产权侵权风险；
- 加强知识产权合规文化建设， 在组织内提升知识产权合规意识，提供和保持有利的知识产权合规环境。

b) 及时通过适当方式获得知识产权保护。

- 商业秘密
- 专利
- 著作权
- 商标
- 其他知识产权类型

c) 依法行使知识产权，不得滥用权利或存在其他不合规行为。

- 不得从事非正常专利申请
- 不得从事不以使用为目的的恶意商标注册
- 不得滥用知识产权，排除、限制竞争
- 不得假冒专利。

d) 及时给予发明人知识产权创造、实施运营的奖励和报酬。

- 根据规章制度规定、与发明人的约定及时足额给予奖励和报酬；
- 没有规章制度规定、也没有与发明人约定的，依据相关法律法规规定的标准及时足额给予奖励和报酬。

e) 加强与知识产权有关的资源风险防控。

- 人事合同：通过劳动合同、劳务合同等方式对员工进行管理，约定知识产权权属、保密条款；明确发明创造人员享有的权利和负有的义务；必要时应约定竞业限制和补偿条款；
- 入职：对新入职员工进行适当的知识产权背景调查，以避免侵犯他人知识产权；对于研究开发等与知识产权关系密切的岗位，应要求新入职员工签署知识产权声明文件；
- 离职：对离职的员工进行相应的知识产权事项提醒；涉及核心知识产权的员工离职时，应签署离职知识产权协议或执行竞业限制协议；
- 外部合作：在与合作方的合作合同、协议中对各方的知识产权权属、保密限制条款进行约定；明确发明创造人员享有的权利和负有的义务；必要时应约定相关参与人员的竞业限制条款；
- 供应链管理：在采购、销售合同中对各方的知识产权权属、保密限制条款进行约定；明确发明创造人员享有的权利和负有的义务；必要时应约定相关参与人员的竞业限制条款。

7.1.14 广告合规

7.1.14.1 平台广告合规

7.1.14.1.1 平台广告概述

7.1.14.1.1.1 相关术语概念及定义

a) 互联网广告：指在中华人民共和国境内，通过网站、网页、互联网应用程序等互联网媒介，以文字、图片、音频、视频或者其他形式，直接或者间接地推销商品或者提供服务的商业广告。广告表现形式有横幅广告、文本链接广告、弹出式广告、视频广告等。

b) 平台广告：指提供互联网广告服务、互联网信息服务的平台经营者为入驻平台的自然人、法人或者其他组织发布的介绍推销该自然人、法人或者其他组织的商品或服务的互联网广告。

c) 广告主：为推销商品或者服务，自行或者委托他人设计、制作、发布广告的自然人、法人或者其他组

织。

d) 互联网广告经营者：指接受委托提供互联网广告设计、制作、代理服务的自然人、法人或者其他组织。

e) 互联网广告发布者：指利用互联网媒介为广告主或者广告主委托的广告经营者发布广告的自然人、法人或者其他组织。

f) 互联网信息服务提供者：指通过互联网提供信息服务，未参与互联网广告设计、制作、代理、发布等活动的自然人、法人或者其他组织。

7.1.14.1.1.2 相关主要依据

a)《中华人民共和国广告法》（以下简称“《广告法》”）

b)《中华人民共和国刑法》

c)《互联网广告管理暂行办法》

d)《医疗广告管理办法》

e)《房地产广告发布规定》

f)《医疗器械广告管理办法》

g)《化妆品监督管理条例》

h)《网络直播营销管理办法（试行）》

i)《医疗美容服务管理办法》

j)《药品、医疗器械、保健食品、特殊医学用途配方食品广告审查发布管理办法》

7.1.14.1.2 主要合规风险点

a) 主要刑事合规风险点

- 平台广告业务的经营者明知其他经营或者应知者利用信息网络犯罪，为其犯罪提供广告推广的，如推广含有违法犯罪信息的网站、APP 以及其他广告，明知其他经营者实施的犯罪行为主要包括电信网络诈骗犯罪、网络赌博犯罪、非法吸收公众存款犯罪、诈骗罪、组织播放淫秽音像制品罪、组织淫秽表演罪、组织传销活动罪以及制作、复制、出版、贩卖、传播淫秽电子信息犯罪等；
- 平台广告业务的经营者违反国家规定信息网络安全管理义务，致使虚假违法广告大量传播；
- 平台广告业务的经营者违反国家规定，利用广告对商品或者服务作虚假宣传且情节严重。

b) 主要行政监管合规风险点

- 提供互联网信息服务的平台经营者未按照国家有关规定建立、健全广告业务管理制度的，或者未对广告内容进行核对；
- 提供互联网信息服务的平台经营者发布广告法律法规禁止的违法广告，如发布烟草广告、推广法规禁止生产和销售的产品以及发布处方药广告、药品类易制毒化学品广告、戒毒治疗的医疗器械和治疗方法广告等；
- 提供互联网信息服务的平台经营者明知或者应知广告虚假仍进行发布，以及明知或者应知广告活动违法不予制止；
- 提供互联网信息服务的平台经营者发布互联网广告，未遵守行政监管要求，如未显著标明关闭标志，对于法律法规要求一键关闭的广告，未确保一键关闭。

c) 主要民事风险点

- 提供互联网信息服务的平台经营者发布关系消费者生命健康的商品或者服务的虚假广告，具有与其他广告相关经营者承担连带责任的风险；

- 提供互联网信息服务的平台经营者明知或者应知广告虚假仍发布的，具有与其他广告相关经营者承担连带责任的风险；
- 提供互联网信息服务的平台经营者在广告中损害未成年人或者残疾人的身心健康的、假冒他人专利的、贬低其他生产经营者的商品或服务的、在广告中未经同意使用他人名义或者形象的等侵权行为的。

7.1.14.1.3 具体实施措施

7.1.14.1.3.1 平台广告合规基本原则

广告应当真实、合法，以健康的表现形式表达广告内容，符合社会主义精神文明建设和弘扬中华民族优秀传统文化的要求，不得含有虚假或者引人误解的内容，不得欺骗、误导消费者。

平台作为互联网信息服务提供者的，对其明知或者应知利用其信息服务发布违法广告的，应当予以制止。

平台作为互联网广告发布者、广告经营者的，应当按照国家有关规定建立、健全互联网广告业务的承接登记、审核、档案管理制度；审核查验并登记广告主的名称、地址和有效联系方式等主体身份信息，建立登记档案并定期核实更新；查验有关证明文件，核对广告内容，对内容不符或者证明文件不全的广告，不得设计、制作、代理、发布。

7.1.14.1.3.2 平台广告合规管理部门

平台宜设立广告合规管理部门或广告合规管理岗位，负责广告合规制度建设、广告审核规范制定；同时宜设立专业的广告审核团队/岗位，向广告合规管理部门/岗位汇报，负责依据国家法律法规、平台广告合规/审核规范对平台广告内容进行审核及复核。

广告审核人员或机构宜独立于广告销售团队。

7.1.14.1.3.3 平台广告合规管理具体措施

平台广告的合规管理要遵循国家法律法规的相关的规定，宜建立健全平台广告合规审核制度、组建广告审核、风险识别团队，完善风险防范及监管机制，确保广告行为/内容符合国家法律法规规定，符合社会主义精神文明建设和弘扬中华民族优秀传统文化的要求。

a) 平台企业宜建立广告合规审核制度/规范

- 广告审核规范的制定：平台宜依据《广告法》等相关国家法律法规的要求以及平台自身管理需要，制定相应的广告审核规范，明确广告审核的基本原则，禁止投放情形以及区别各特殊行业商品、服务广告的具体审核要求。
- 禁投类目清单搭建：平台可以梳理禁止投放广告的商品、服务类目清单（例如：处方药广告、烟草广告等），给广告主明确的广告禁止投放指引。
- 高风险类目管控方案搭建：为降低广告投放违法风险，平台宜搭建高风险类目（例如：三品一械广告、投资金融类广告、教育类广告等）具体的管控措施及方案，对广告投放的资质要求、内容、形式以及广告位置制定明确的要求及规则。
- 建立健全完善违规处罚制度：平台可根据自身需求和定位，制定平台规则及处罚规范，应对广告主、广告经营者及其相关主体在广告经营中的违法违规行为，以保护平台的合法权益，维护良好的竞争环境。

b) 广告审核机制建设

- 审核团队的配备：平台宜配备专业的审核团队和审核系统，对广告审核内容及经营资质进行审核，降低广告投放风险。
- 广告资质审核：平台应对广告主的行业经营资质及广告投放资质两部分资质文本进行审核。确保广告主在宣传特定行业商品、服务前，应当具备相应的经营资质；同时，确保特殊行业广告主在广告投放

前，其广告投放内容满足监管审批要求。

- 广告素材审核：平台应依据《广告法》等相关法律法规以及平台制定的广告合规审核规范的基本原则及要求对禁止情形进行审核判断；同时针对特定行业的广告要求及规范进行审核。

c) 监测预警机制

平台可以统筹开展广告内容监测、分析和通报工作，及时发布广告内容安全监测预警信息，预测事件发生的可能性、影响范围和危害程度，并建立相应的响应机制。

d) 广告投诉举报机制

- 侵权投诉：广告素材存在侵犯他人合法权益的内容（知产侵权、肖像权侵权、个人信息侵权等）。平台在接到侵权投诉后，应核查广告内容、审核记录以及广告主资质，如发现广告存在违法违规情况，应对广告予以下线或采取其他处罚措施，并转通知投诉人。
- 消费者投诉：消费者因虚假广告而购买商品或服务的消费者的合法权益受到损害，据此要求平台维护其合法权益的诉求。平台在接到消费者投诉后，确定被投诉广告，核查广告内容、审核记录以及广告主资质，如发现广告存在违法违规情况，应对广告予以下线或采取其他处罚措施，并转通知消费者。
- 用户举报：用户发现平台投放的广告存在违法违规问题，反馈给平台。接到用户投诉后，应根据用户提供线索定位广告，核查广告是否违法，并依据相关法律法规及平台规则进行处理.

7.1.14.2 企业自行发布广告合规

7.1.14.2.1 企业自行发布广告概述

7.1.14.2.1.1 相关术语概念及其定义

a) 广告：在中华人民共和国境内，商品经营者或者服务提供者通过一定媒介和形式直接或者间接地介绍自己所推销的商品或者服务的商业广告活动。

b) 企业自行发布广告：指通过报纸、杂志、电视、广播、网络等媒介向公众介绍企业自己所推销的商品或服务的商业广告活动，形式包括文字、图片、视频等。

c) 企业自行发布广告合规评审：企业在自行发布广告进行宣传活动前，宜组织相关人员进行评审。

d) 业务部门：指所有负责企业对外广告宣传内容设计、制作、投放等相关工作的部门。

7.1.14.2.1.2 相关主要依据

a) 《中华人民共和国广告法》

b) 《中华人民共和国反不正当竞争法》

c) 《中华人民共和国电子商务法》

d) 《中华人民共和国中华人民共和国价格法》

e) 《中华人民共和国消费者权益保护法》

f) 《中华人民共和国刑法》

g) 《互联网广告管理暂行办法（征求意见稿）》

7.1.14.2.2 主要合规风险点

a) 行政处罚风险

企业进行广告宣传时，因素材违规、滥用极限词、虚假宣传等违法行为，被监管机关行政处罚的风险。

b) 民事侵权风险

未经授权使用他人享有权利的图片、字体、视频、商标等，被权利人追究侵权责任的风险。

c) 不正当竞争风险

因宣传中弄虚作假、引人误解、贬低其他商品或服务等，遭到监管机关处罚或被他人起诉的风险。

d）刑事风险

违反国家规定，利用广告对商品或者服务作虚假宣传，情节严重的，存在构成虚假广告罪的风险。

e）声誉风险

企业自行发布广告不合规，导致利益相关方、社会公众、媒体等对企业形成负面评论，从而损害品牌价值、不利于正常经营的风险。

7.1.14.2.3 具体实施措施

7.1.14.2.3.1 企业自行发布广告合规基本原则

企业自行发布广告进行宣传，宜遵循相关法律法规要求及本指南合规管理原则要求。

7.1.14.2.3.2 企业自行发布广告合规管理部门

企业可设置广告宣传合规管理部门或者广告宣传合规管理岗，负责审核广告内容，识别合规风险，并提供修改建议。

该部门或岗位负责识别广告内容存在的合规风险，提示业务部门核实第三方相关内容的授权与资质，避免宣传内容违反法律法规的规定；关注法律法规的更新动态，及时解读有关内容，帮助业务部门自查自纠。

7.1.14.2.3.3 企业自行发布广告合规管理目标

更好地识别企业自行发布广告宣传活动中的法律风险，提高广告内容评审的效率和质量；确保广告内容符合相关法律法规的要求，防范企业对外宣传的法律风险。

7.1.14.2.3.4 企业自行发布广告合规管理具体措施

a）可以设置广告宣传合规管理部门或者广告宣传合规管理岗。

b）宜建立广告审核规则，并根据各相关法律法规的规定及时对广告审核规则更新修订。

c）可以指派专人负责广告审核规则的管理工作，及时对规则更新修订，并关注规则的执行情况。

d）宜重点关注的广告审核要点：

- 不得使用国家形象、违背公序良俗
- 广告内容不得虚假宣传
- 广告不得使用国家级、最高级、最佳等极限用语
- 涉及他人权利的，应获相应授权
- 不得损害国家尊严或利益
- 互联网广告应当具有可识别性，显著标明“广告”，使消费者能够辨明其为广告
- 广告内容不得贬低其他经营者的商品或服务

7.1.15 内容合规

7.1.15.1 内容合规概述

内容合规，即企业平台内容应当合乎政策法规和监管要求。大体上可包括：第一，国家法律法规，包括法律、行政法规、行政规章、司法解释等，所有具有法律渊源资格的规范文件都是需要遵守的对象。第二，行业规范惯例，如各行业协会颁布的行为准则等。第三，企业内部制定的规章制度。内容合规是围

绕着合规风险而展开的，可联系合规风险的层面加以理解。

在内容合规方面，相关依据主要有：《中华人民共和国电信条例》《信息网络传播权保护条例》《互联网信息服务管理办法》《关于加强网络直播规范管理工作的指导意见》《互联网用户公众账号信息服务管理规定》《网络信息内容生态治理规定》《互联网新闻信息服务单位内容管理从业人员管理办法》《微博客信息服务管理规定》《互联网新闻信息服务管理规定》《互联网群组信息服务管理规定》《互联网跟帖评论服务管理规定》《互联网新闻信息服务许可管理实施细则》等。

7.1.15.2 主要合规风险点

a) 信息通信及互联网内容服务提供者或从业人员把关不严，造成意识形态错误倾向或产生重大负面影响。
b) 信息通信及互联网内容服务提供者或从业人员未能依法依规使用国家标准要素规范，如地图、地名、国旗等具有法律规范的要素。
c) 信息通信及互联网内容服务提供者或从业人员未能严格坚持内容的真实性和权威性，对新闻内容做出误导性加工。
d) 信息通信及互联网内容服务提供者或从业人员制作、复制、发布、传播法律、行政法规禁止的信息内容。
e) 信息通信及互联网内容服务提供者或从业人员以权谋私，如通过采编、发布、转载、删除新闻信息，干预新闻信息呈现或搜索结果等手段谋取不正当利益。
f) 信息通信及互联网内容服务提供者或从业人员对用户信息与用户生成内容（UGC）审核不严，如用户头像或昵称等含有不良信息或不当元素；对评论、发帖等用户生成内容（UGC）审核存在严重漏洞。
g) 信息通信及互联网内容服务提供者或从业人员在转载新闻时，未保证新闻来源可追溯。
h) 信息通信及互联网内容服务提供者未建立完整的制度体系，如针对信息发布、审核、巡查等环节相关制度。
i) 信息通信及互联网内容服务提供者安全投入相对不足，安全防护手段滞后，安全保障能力不强，造成网站被攻击、内容被篡改以及重要敏感信息泄露等重大后果。未能保证重要内容、重要位置实现巡查，及时处置有害信息。

7.1.15.3 具体实施措施

7.1.15.3.1 内容合规管理原则

内容合规管理需遵循内容相关法律法规要求并把握正确的政治方向和舆论导向。

7.1.15.3.2 主要责任人和职能部门

企业可成立内容管理部门，负责完善内容业务工作机制，并根据法律法规变化和监管动态，及时将外部有关合规要求转化为内部规章制度。

7.1.15.3.3 内容合规管理目标

互联网信息单位内容发布符合相关法律法规要求，维护网络意识形态安全。

7.1.15.3.4 内容合规管理具体措施

a) 宜建立内容来源管理制度。可建立信息内容评价体系，注重遴选优质信息来源，保障信息内容安全。
b) 宜制订内容人员管理规章制度，配备适当的业务从业人员。可定期开展内容人员的合规风控培训，持续提升从业人员能力素质。
c) 宜建立内容审核机制。可完善内容采集、制作、发布合规流程，建立定期核查机制，能够自我发现漏洞并及时封堵。可完善人工审核制度，细化审核标准，提升审核质量；也可充分利用技术手段，提升

对历史数据、大量新增数据、多维度数据的内容合规风控效率。

d) 宜建立违法违规信息样本库。可采取动态更新机制，分级分类管理，定期丰富扩充，提升技术审核效率和质量。可健全重点信息多节点召回复核机制，明确重点信息范围、标准、类别等，对关系国家安全、国计民生和公共利益等重点领域信息，加大审核力度，科学把握内容，保障信息安全。

e) 宜加强内容产品的合规检测。可对产品内容合规方面定期测试抽查，体现正确价值观导向。

f) 宜建立互动环节把关机制。按照网络平台主体责任制度，可对用户生产和使用内容的环节进行监督。宜规范话题设置，防止蹭热点、低俗媚俗、造谣传谣、负面信息集纳等恶意传播行为。

g) 可按照未成年人保护法律法规要求，开发升级未成年人防沉迷、青少年模式等管理系统，不断提高系统辨识度，增强识别精准性，合理设置未成年人使用服务的时间、权限等。宜提供适合未成年人的优质内容，保障未成年人健康科学用网。面向未成年人提供产品和服务，可清晰界定服务内容，高标准治理产品生态，严防不良信息影响未成年人身心健康。

7.1.15.3.5 内容不合规纠错机制与持续改进机制

a) 宜建立快速应急响应机制，按突发事件级别明确风控标准，在操作系统设置突发状况应急管控功能，可及时采取措施防止危害扩大，消除安全隐患。

b) 宜健全舆情预警机制，重点关注敏感热点舆情，及时发现不良倾向，进行科学有效引导，防止误导社会公众。

c) 可优化信息推荐机制，优先推送优质信息内容，加强防范和抵制不良信息，禁止传播违法信息，切实维护版面页面良好生态。

d) 可建立信息传播人工干预制度规范，严格操作标准，规范操作流程，全过程留痕备查，及时主动向监管部门报告重大事项。

e) 宜从人员、技术、产品等多方面，加大对内容合规风控的投入。部分缺乏自研能力的企业，可从外部引入成熟的内容合规风控产品。

7.1.16 网络游戏合规

7.1.16.1 网络游戏合规概述

7.1.16.1.1 相关术语概念及定义

a) 网络游戏：由软件程序和信息数据构成，通过互联网、移动通信网等信息网络提供的游戏产品和服务。

b) 网络游戏研发方：负责网络游戏的制作和开发，一般作为软件著作权人登记在《计算机软件著作权登记证书》。

c) 网络游戏运营方：通过信息网络提供网络游戏产品和服务，并取得收益行为的个人、法人或其他组织。

d) 网络游戏分发平台方：提供网络游戏分发服务的平台方。

e) 网络游戏企业：网络游戏研发方、网络游戏运营方与网络游戏分发平台方的总称。

f) 网络游戏虚拟货币：由网络游戏运营方发行，网络游戏用户使用法定货币按一定比例直接或者间接购买，以电磁记录方式存储于服务器内，并以特定数字单位表现的虚拟兑换工具。

g) 防沉迷规定：为防止未成年人沉迷网络游戏，网络游戏运营方需履行的实名认证、身份识别、游戏游玩时长、充值金额限制等义务。

h) 游戏版号：监管机构同意相关网络游戏出版运营的批准文件，即《网络游戏出版物号（ISBN）核发单》。

7.1.16.1.2 网络游戏合规相关依据

a) 《中华人民共和国出版管理条例》

b) 《互联网信息服务管理办法》

c）《网络出版服务管理规定》
d）《关于进一步加强网吧及网络游戏管理工作的通知》
e）《关于加强网络游戏虚拟货币管理工作的通知》
f）《关于开展棋牌类网络游戏专项核查工作的通知》
g）《中华人民共和国网络安全法》
h）《中华人民共和国未成年人保护法》
i）《儿童个人信息网络保护规定》
j）《网络游戏防沉迷系统开发标准》
k）《关于启动网络游戏防沉迷实名验证工作的通知》
l）《关于防止未成年人沉迷网络游戏的通知》
m）《关于进一步严格管理切实防止未成年人沉迷网络游戏的通知》
n）《未成年人网络保护条例（送审稿）》
o）《关于联合开展未成年人网络环境专项治理行动的通知》

7.1.16.2 主要合规风险

7.1.16.2.1 资质缺失

网络游戏运营方在开展网络游戏相关服务及/或网络游戏出版运营前，应当根据其业务类型获取相关电信业务经营许可证照（ICP许可证）、游戏版号（《网络游戏出版物号（ISBN）核发单》）、《计算机软件著作权登记证书》等相关资质，否则将可能遭受包括但不限于没收违法经营所得、罚款、责令关闭/下架网络游戏、吊销营业执照等处罚。

7.1.16.2.2 实名认证与防沉迷未有效管控

网络游戏企业未遵循相关法律法规对游戏账号/用户未进行实名认证，未接入国家防沉迷系统，未按照版署要求对未成年用户实行网络游戏游玩时间与充值限制，未采取有效技术手段识别未成年人等。

7.1.16.2.3 内容违法

网络游戏存在法律法规禁止性内容，包括但不限于：

a）违反宪法确定的基本原则的；
b）危害国家统一、主权和领土完整的；
c）泄露国家秘密、危害国家安全或者损害国家荣誉和利益的；
d）煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的；
e）宣扬邪教、迷信的；
f）散布谣言，扰乱社会秩序，破坏社会稳定的；
g）宣扬淫秽、色情、赌博、暴力，或者教唆犯罪的；
h）侮辱、诽谤他人，侵害他人合法权益的；
i）违背社会公德的；
j）有法律、行政法规和国家规定禁止的其他内容的。

7.1.16.2.4 虚假宣传

网络游戏企业违反《中华人民共和国广告法》相关法规，发布虚假不实广告（例如网络游戏中夸大或虚假宣传充值福利、游戏规则）侵犯用户权益。

7.1.16.2.5 知识产权侵权

网络游戏侵犯第三方软件著作权、商标权等合法权益，以及网络游戏用户发表的文字、图片等内容侵犯第三方合法权益而导致网络游戏运营方承担信息网络传播权侵权责任。

7.1.16.2.6 网络安全与个人信息保护

网络游戏企业未采取相应技术或管理措施，或违反网络安全相关规定，侵犯第三方商业秘密（包括但不限于违法获取、超范围使用、擅自披露三方商业秘密），以及违反《中华人民共和国个人信息保护法》规定违法收集、处理、使用用户信息。

7.1.16.2.7 运营终止

网络游戏运营方在游戏运营终止前，未提前予以公告，未对用户未消耗完毕的虚拟货币退还或退换。

7.1.16.3 网络游戏合规具体实施措施

7.1.16.3.1 网络游戏合规原则

遵循网络游戏相关法律法规要求及本指南。

7.1.16.3.2 网络游戏研发方、网络游戏运营方合规管理指南

a) 网络游戏研发

- 合规要求：网络游戏研发方在网络游戏研发过程中应明确该游戏产品未侵犯任何第三方合法权益（例如著作权、商标权）。
- 具体合规措施：网络游戏研发方可将相关责任部门/人员落入游戏研发流程当中，未经责任部门/人员审核或批准，该游戏不得自行或委托网络游戏运营方上线发行。

b) 网络游戏资质取得

- 合规要求：网络游戏出版运营前，网络游戏运营方应取得法律规定的相应资质文件，非自研游戏产品还应取得网络游戏研发方的合法授权。
- 具体合规措施：制定资质清单，并以符合清单所列资质文件作为游戏运营前置要求。

c) 网络游戏合规运营

- 合规要求：网络游戏上架前以及运营过程中，网络游戏运营方应保证网络游戏运营的合法合规，在网络游戏终止前应依法通知游戏用户并采取相应补偿或费用退还措施。
- 具体合规措施：建立实名认证机制并接入国家防沉迷管控系统。制定符合法律法规要求、且具有实践性和针对性的审核制度、审核标准与审核流程。

d) 客诉处理

- 合规要求：网络游戏运营方应及时处理用户或第三方投诉。
- 具体合规措施：建立健全的客诉处理机制，包括但不限于客诉处理流程、客诉上升机制、客诉处理规范等标准制度及流程。

e) 合规培训

- 合规要求：网络游戏运营方应向各部门/人员普及和宣传网络游戏合规法律要求。
- 具体合规措施：建议定期向各业务或责任部门进行合规培训，进行周期性（如每年一次）合规考试。

7.1.16.3.3 网络游戏分发平台方合规管理指南

a) 网络游戏资质审核

- 合规要求：网络游戏分发平台方应就在其平台上架的网络游戏运营方及其上架网络游戏产品是否符合准入资质进行必要审查。
- 具体合规措施：制定网络游戏运营方及网络游戏软件准入标准与资质要求清单，并执行。

b) 客诉处理

- 参考网络游戏研发方、网络游戏运营方合规管理指南客诉处理。

c) 合规培训

- 参考网络游戏研发方、网络游戏运营方合规管理指南合规培训。

7.1.17 算法合规

7.1.17.1 算法合规概述

7.1.17.1.1 术语与定义

a) 算法：是一种计算机指令集，通过该指令集，符合单一或系列预设的入参信息或条件后，通过机器语言编排的特定逻辑、规则等，得到预定结果或解决相应问题的决策逻辑，获取相比人工决策更加高效快速的结果。
b) 算法推荐技术：利用生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术向用户提供信息。
c) 算法推荐服务：在中华人民共和国境内应用算法推荐技术提供互联网信息服务。
d) 算法服务提供者：在中华人民共和国境内应用算法技术提供互联网信息服务的组织、个人。
e) 算法合规：企业及其员工应用算法技术提供互联网信息服务的行为符合法律法规、规章、规范性文件等有关规定。

7.1.17.1.2 相关主要依据

a) 《中华人民共和国国家安全法》
b) 《中华人民共和国网络安全法》
c) 《中华人民共和国数据安全法》
d) 《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”）
e) 《中华人民共和国电子商务法》
f) 《互联网信息服务算法推荐管理规定》

7.1.17.2 主要合规风险点

a) 算法服务提供者在算法研发、使用以及提供算法服务时，未遵守《个人信息保护法》等相关法律法规规定，违规收集、存储、使用、分析、加工、传输、对外提供个人信息，存在对个人信息主体合法权益造成损害的情形。

b) 算法服务提供者在算法研发、使用时，将违法和不良信息关键词记入用户兴趣点或者作为用户标签以及采用其他类似技术路径并据以推送信息，或诱导用户沉迷、过度消费等违反法律法规或

者违背伦理道德的情形。

c) 算法服务提供者利用推荐算法向用户个性化推荐服务时，设置交易门槛、实施不同的交易价格、针对不同用户适用不同的交易条件等造成具有相同交易条件的交易对象适用不合理的差别待遇的情形，以及造成人身领域歧视的情形。

d) 算法服务提供者利用推荐算法向用户个性化推荐服务时，未提供不针对其个人特征的选项，或者未向用户提供便捷的关闭个性化推荐服务的选项。

e) 算法服务提供者利用算法对其他互联网信息服务提供者进行不合理限制，或者妨碍、破坏其合法提供的互联网信息服务正常运行，实施垄断和不正当竞争行为。

f) 算法服务提供者向未成年人用户提供可能引发未成年人模仿不安全行为或违反社会公德行为等影响未成年人身心健康的算法推荐服务。

g) 算法服务提供者向老年人用户提供服务时，未充分考虑老年人的智能适老化需求，未有效开展电信网络诈骗信息的监测、识别和处置。

7.1.17.3 具体实施措施

7.1.17.3.1 算法合规管理原则

算法合规管理需遵循算法相关法律法规要求及本指南4合规管理原则要求。

7.1.17.3.2 算法合规管理部门

企业宜设立算法合规管理部门或算法合规管理岗位，负责算法合规风险评估及处置，算法合规管理部门或算法合规管理岗位向企业合规管理负责人汇报。

7.1.17.3.3 算法合规管理目标

遵守法律法规，尊重社会公德，遵守商业道德、职业道德和技术伦理，遵循公正公平、公开透明、科学合理和诚实信用的原则，坚持主流价值导向，优化算法推荐服务机制，积极传播正能量，促进算法应用向上向善。

7.1.17.3.4 算法合规管理具体实施步骤

a) 企业宜建立算法合规管理制度，如算法安全评估、应急处置、培训等，明确算法合规管理具体操作流程、人员及责任，有效保障算法及算法服务从研发到部署运维全周期风险可控。
b) 算法合规管理部门负责对算法及算法服务合规性进行全面评估，根据法律法规及相关要求提出合规建议。算法合规管理部门可同时会同其他职能部门对算法进行科技伦理审查，并估算法在开发、测试、应用过程中是否符合主流价值导向。提供互联网新闻信息服务或其他需先行获得资质许可的算法推荐服务，应要求先行获得相应的资质许可。
c) 企业宜建立算法类别管理及日志留存制度，并按照有关规定进行备案。
d) 企业宜通过服务热线、网页入口等方式收集用户对于推荐算法服务反馈，持续优化推荐算法服务。
e) 企业宜建立算法及算法服务相关信息披露渠道，对算法原理进行解释和说明，并根据法律法规相关要求进行信息披露。
f) 算法合规管理部门宜对算法开发、测试、应用、风险监测、用户投诉处理等情况进行定期或不定期检查，并积极探索采用技术措施，保证算法及算法服务持续符合合规要求、合规管控措施实施到位。企业宜根据自身情况建立合规审计制度，定期对算法及算法服务相关合规情况进行梳理总结.

7.2 合规管理重点人员

7.2.1 管理人员

促进管理人员提高合规意识，带头依法依规开展经营管理活动，认真履行承担的合规管理职责，强化考核与监督问责。

7.2.2 重要风险岗位人员

根据合规风险评估情况明确界定重要风险岗位，有针对性加大培训力度，使重要风险岗位人员熟悉并遵守业务涉及的各项规定，加强监督检查和违规行为追责。

7.2.3 境外工作人员

境外工作人员包括企业驻外人员和项目所在地本地雇员。企业宜将合规要求及合规培训作为境外工作人员任职、上岗的必备条件，临时出差人员出境前需接受相应的合规培训，确保遵守我国和所在国（地区）的法律法规等相关规定。

7.2.4 其他人员

其他需要重点关注的人员，如商业合作伙伴、利益相关方等。

8 合规管理制度建设

8.1 合规管理制度体系

建立健全合规管理制度，制定全员普遍遵守的合规行为规范，针对重点领域制定专项合规管理制度，并根据法律法规变化和监管动态，及时将外部有关合规要求转化为内部规章制度。

8.2 合规方针

确立企业合规方针，加强合规管理的顶层制度构建。

合规方针是合规管理的指导思想，是落实企业合规管理各项措施的基础和依据。

8.3 合规行为规范

合规行为规范规定企业国（境）内外经营活动需遵守的基本原则和标准，包括但不限于企业合规理念、目标、内涵、适用范围、合规行事标准、违规的应对方式和后果等。

合规行为规范是企业合规管理基本制度，适用于企业全体员工以及代表企业从事经营活动的工作人员。

8.4 合规管理基本制度

合规管理牵头部门根据合规管理体系的主要构成要素，制定合规管理基本制度。

8.5 合规管理专项制度

合规管理牵头部门、各相关业务部门宜协作配合，针对重点领域制定合规管理专项制度。

8.6 合规管理操作流程和指引

各相关责任部门结合业务实际，合规方针、合规行为规范及合规管理专项制度， 制定合规管理操作指引和流程，细化合规工作的标准和要求。将标准和要求融入业务流程中，推进合规管理工作切实落地，确保各项经营行为合法合规。

9 合规培训

9.1 定期开展合规培训

建立合规管理培训常态机制，将合规培训纳入企业员工培训计划。

企业宜针对不同的培训对象，采用适合的培训方式、培训内容，定期开展合规培训。

当企业所处内外部环境发生重大变化、同类型企业出现严重合规风险事件等情形，宜对企业员工进行相应合规培训。

9.2 合规培训的内容与测试

企业合规管理培训内容主要包括法律法规、政府监管政策、企业合规行为规范、合规典型案例、影响性合规事件等。

企业宜通过培训测试与不定期测试等方式检验合规培训效果。

企业宜依据培训内容制定、测试检验流程与标准。企业设定检验标准可以参考企业人员岗位职责要求、企业合规管理制度、专业领域或行业职业技术技能标准等。

10 举报

10.1 举报机制

企业宜建立违反企业行为规范的内部举报制度及企业外部人员投诉管理制度，建立畅通有效的举报与投诉渠道及对举报人、投诉人的保护措施。

10.2 举报渠道

建立畅通有效的举报投诉电话、邮箱等举报投诉渠道，保障举报人、投诉人安全畅通地进行举报、投诉。

10.3 举报人保护

对举报人、投诉人的相关信息予以保密，保障举报人和投诉人免遭报复。

11 合规调查

对举报投诉线索展开调查。合规管理牵头部门负责组织职责范围内的违规事件调查，参与由具有合规监督职能的部门组织展开的调查活动；对于严重违规事件，合规管理牵头部门应主动配合执法机关展开调查。

12 合规监督审查与合规报告

12.1 合规监督机制

建立合规管理监督机制，对企业合规管理体系构建和实施状况进行监测，并详细记录合规监测结果。

12.2 合规审查机制

建立健全合规审查机制，将合规审查作为规章制度制定、重大事项决策、重要合同签订、重大项目运营等经营管理行为的必经程序，及时对不合规的内容提出修改建议，未经合规审查不得实施。

12.3 合规监督、审查主体

合规管理牵头部门负责合规管理体系的监督、审查工作。

12.4 合规管理信息化建设

具备条件的企业，宜积极开展合规管理工作的信息化建设，保障企业合规义务的实施、监测、管理。

12.5 合规报告

建立并完善合规报告机制。合规管理牵头部门负责定期向合规负责人、决策层报告企业合规管理工作情况。合规报告一般以年度为单位，视企业实际情况可进行相应调整。

13 绩效考核

13.1 合规绩效考核机制

企业决策层、管理层协同合规管理牵头部门参考企业关键绩效指标(KPI)及其他关键信息，定期开展合规管理体系绩效评审，保障合规管理体系有效运行。

13.2 考核奖励

建立企业合规管理考核评价机制。将企业合规管理完成情况纳入对企业各部门、各单位的定期综合考核计划，细化评价指标，考核结果与各部门、各单位综合绩效相衔接。

13.3 违规惩戒

完善违规惩戒机制，明晰责任范围，细化惩戒标准。对违规行为及违规人员及时开展调查，严肃追究违规人员责任。

14 合规管理体系有效性评估

14.1 合规管理体系有效性评估机制

互联网行业组织与国家企业合规促进机构共同建立企业合规管理体系评估机制，对企业合规管理体系的构建与实施情况进行评估。

14.2 合规管理体系有效性评估主体

企业的上级主管部门、互联网行业组织与国家企业合规促进机构等负责企业的合规管理评估工作，并依据被评估企业实际情况，提出相应改进建议。

14.3 合规管理体系有效性评估内容

开展合规管理体系有效性评估，应对合规管理体系的设计、执行、效果展开实时评估，确保合规管理体系制度设计完整、实施有效、持续更新。

15 合规文化

企业宜加强合规意识，树立诚信、创新、合作的行业核心价值观，将合规文化作为企业文化建设的重要内容，培育良好的企业合规文化氛围，加快提升企业合规经营管理水平，保障企业科学、持续、健康发展。

16 持续改进

企业宜持续改进合规管理体系的适配性、充分性和有效性。

当违规发生时，企业宜审慎评估，采取适当措施，消除造成不合规的原因，以防止其再次或在其他情景发生；企业宜持续改进和完善相关制度、流程，强化合规管理工作，提升企业合规管理水平。

参 考 文 献

[1] 中央企业合规管理指引（试行）（国资发法规〔2018〕106 号）

[2] 企业境外经营合规管理指引（发改外资〔2018〕1916 号）

[3] ISO37301:2021 Compliance management systems — Requirements with guidance for use

[4] Good practice guidance on internal controls, ethics, and compliance（OECD）

[5] 《中华人民共和国民法典》

[6] 《中华人民共和国政府采购法》

[7] 《中华人民共和国招标投标法》

[8] 《中华人民共和国招标投标法实施条例》

[9] 《中华人民共和国政府采购法实施条例》

[10] 《中华人民共和国网络安全法》（2016）

[11] 《中华人民共和国个人信息保护法》（2021）

[12] 《中华人民共和国数据安全法》（2021）

[13] 《关键信息基础设施安全保护条例》

[14] 《网络安全等级保护条例（征求意见稿）》

[15] 《网络安全审查办法（修订草案）》

[16] 《国家网络安全事件应急预案》

[17] 《网络安全威胁信息发布管理办法（征求意见稿）》

[18] 《中华人民共和国出口管制法》

[19] 《中华人民共和国对外贸易法》

[20] 《中华人民共和国反外国制裁法》

[21] 《中华人民共和国货物进出口管理条例》

[22] 《中华人民共和国技术进出口管理条例》

[23] 《中华人民共和国核材料管制条例》

[24] 《中华人民共和国核两用物品及相关技术出口管制条例》

[25] 《中华人民共和国生物两用品及相关设备和技术出口管制条例》

[26] 《阻断外国法律与措施不当域外适用办法》

[27] 《不可靠实体清单规定》

[28] 《两用物项和技术进出口许可证管理办法》

[29] 《两用物项和技术进出口许可证管理目录》

[30] 《禁止出口限制出口技术管理办法》

[31] 《商务部关于两用物项出口经营者建立出口管制内部合规机制的指导意见》

[32] 《两用物项出口管制内部合规指南》

[33] 《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》

[34] 《中华人民共和国消费者权益保护法》

[35] 《互联网信息服务管理办法》

[36] 《移动互联网应用程序信息服务管理规定》

[37] 《中华人民共和国反洗钱法》

[38] 《信息安全技术 ICT供应链安全风险管理指南》

[39] 《联合国反腐败公约》
[40] 《经济合作与发展组织反腐败公约》
[41] 《中华人民共和国刑法》
[42] 《中华人民共和国反不正当竞争法》
[43] 《中华人民共和国公司法》
[44] 《中华人民共和国监察法》
[45] 《最高人民法院、最高人民检察院关于办理贪污贿赂刑事案件适用法律若干问题的解释》
[46] 《中华人民共和国反垄断法》
[47] 《中华人民共和国电子商务法》
[48] 《国务院反垄断委员会关于平台经济领域的反垄断指南》
[49] 国家市场监督管理总局《禁止滥用市场支配地位行为暂行规定》
[50] 国家市场监督管理总局《禁止垄断协议暂行规定》
[51] 国家市场监督管理总局反垄断局《关于经营者集中申报的指导意见》
[52] 《中华人民共和国反不正当竞争法》
[53] 《中华人民共和国专利法》
[54] 《中华人民共和国商标法》
[55] 《中华人民共和国著作权法》
[56] 《专利法实施细则》
[57] 《商标法实施条例》
[58] 《著作权法实施条例》
[59] 《计算机软件保护条例》
[60] 《植物新品种保护条例》
[61] 《集成电路布图设计保护条例》
[62] 《中华人民共和国广告法》
[63] 《互联网广告管理暂行办法》
[64] 《医疗广告管理办法》
[65] 《房地产广告发布规定》
[66] 《医疗器械广告管理办法》
[67] 《化妆品监督管理条例》
[68] 《网络直播营销管理办法（试行）》
[69] 《医疗美容服务管理办法》
[70] 《药品、医疗器械、保健食品、特殊医学用途配方食品广告审查发布管理办法》
[71] 《中华人民共和国价格法》
[72] 《中华人民共和国电信条例》
[73] 《信息网络传播权保护条例》
[74] 《互联网信息服务管理办法》
[75] 《关于加强网络直播规范管理工作的指导意见》
[76] 《互联网用户公众账号信息服务管理规定》
[77] 《网络信息内容生态治理规定》
[78] 《互联网新闻信息服务单位内容管理从业人员管理办法》
[79] 《微博客信息服务管理规定》
[80] 《互联网新闻信息服务管理规定》

[81] 《互联网群组信息服务管理规定》
[82] 《互联网跟帖评论服务管理规定》
[83] 《互联网新闻信息服务许可管理实施细则》
[84] 《出版管理条例》
[85] 《网络出版服务管理规定》
[86] 《关于进一步加强网吧及网络游戏管理工作的通知》
[87] 《关于加强网络游戏虚拟货币管理工作的通知》
[88] 《关于开展棋牌类网络游戏专项核查工作的通知》
[89] 《中华人民共和国未成年人保护法》
[90] 《儿童个人信息网络保护规定》
[91] 《网络游戏防沉迷系统开发标准》
[92] 《关于启动网络游戏防沉迷实名验证工作的通知》
[93] 《关于防止未成年人沉迷网络游戏的通知》
[94] 《关于进一步严格管理切实防止未成年人沉迷网络游戏的通知》
[95] 《未成年人网络保护条例（送审稿）》
[96] 《关于联合开展未成年人网络环境专项治理行动的通知》
[97] 《中华人民共和国国家安全法》
[98] 《中华人民共和国信息安全法》
[99] 《互联网信息服务算法推荐管理规定》