

- 管理理念 • 吸引、保留和激励人才 • 培养人才 • 建立多元、共融和协作的工作场所 • 关注员工健康与福利 • 鼓励沟通与发声

## 2.6

# 鼓励沟通与发声

腾讯着力营造平等、开放、透明的沟通氛围，鼓励员工发声。我们通过员工大会、内部论坛和年度敬满度调查等多种渠道，积极倾听员工的声音，以增强团队的凝聚力，推动企业的共同发展和创新。

## 管理层牵头，建立坦诚沟通文化

公司高级管理层定期举行内部交流活动，以帮助员工及时了解腾讯的战略和管理决策。交流活动包括年度Link Time、员工大会、战略管理大会等。其中，Link Time是腾讯周年庆活动的重要环节，所有高级管理层都会出席，与员工进行坦诚沟通，并现场回答员工的提问。2024年，我们开通了“一起debug”通道，通过问卷，收集关于管理和业务精进的建议，推动管理者带头建立坦诚透明的解决问题机制，鼓励员工积极反映真实问题。

## 内部沟通平台，自由表达想法

我们倡导组织扁平化，设有多个内部平台，支持员工表达意见和建议。其中，“乐问”是内部最大的问答沟通社区，涵盖产品建议、经验分享、员工生活等话题。员工可以选择匿名或者实名提问，打破了职级和部门的限制，实现了广泛的互动。于2024年，员工在“乐问”提出了超过1.9万个问题，获得了9.4万个回答，浏览量突破5,700万。此外，部分事业群还建立了内部沟通与交流平台，用于深入的技术和专业分享。



## 全员敬满度调查，聆听反馈

我们每年都会委托独立的第三方机构对全体员工进行匿名的敬满度调查，旨在了解员工的工作投入度、留任意愿、宣传腾讯的意愿，以及他们在工作中的感受，包括成就感、压力感、团队协作、工作支持，以及对企业战略、组织活力的看法和建议等。于2024年，调查问卷的有效回复率达到了95.1%；与2023年相比，整体敬业度提升了4.4个百分点，满意度提升了4.7个百分点。企业文化价值观、职场公平和瑞雪+已经连续3年成为员工最满意的三个维度，这充分体现了员工对腾讯努力营造的尊重、公平和价值观驱动的工作环境的认同。

我们重视员工在敬满度调查中提出的意见和建议，并将其作为优化管理、提升员工工作体验的重要依据。员工的积极建议已经在多个方面推动了我们的改进：通过优化审批流程，提高了管理效率；创新职业发展机制，为更多优秀的员工提供更广阔的发展空间；同时，丰富了沟通渠道，以便更好倾听一线员工的声音等。2024年，我们在敬满度调查开放题环节共收集到超过3万条建议和意见反馈，这些反馈将成为我们进一步改进企业管理的重要参考。

## 违纪投诉、员工申诉和反舞弊举报

我们倡导员工坚守正直的价值观，制定并执行《腾讯阳光行为准则》，明确腾讯员工及其他相关方应遵循的行为规范，并设立员工申诉和投诉违纪行为的渠道。当发现违规行为，员工可以进行反馈，相关部门会严格遵循既定程序跟进。

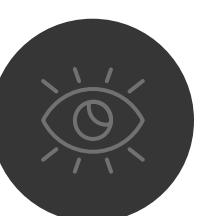
- **职场员工公约瑞雪+：**是腾讯员工文明行为的代称。我们鼓励所有员工通过“瑞雪大侠”微信账号反馈违反职场不文明的行为。如果反馈内容属实，我们将对违规人员进行通报批评，情节严重的将移交其他渠道进一步处理。



- **员工申诉渠道：**我们设立了员工申诉渠道，如员工对试用期、绩效、离职等相关流程持有异议或者认为管理人员违纪，可提交申诉或投诉，按照程序通过间接上级、人力资源部门、专门调查小组逐步升级解决问题。



- **反舞弊举报制度：**我们制定并实施《腾讯反舞弊举报制度》。如果员工发现任何涉嫌违规的行为，可通过实名或匿名的方式进行举报，相关举报将由反舞弊调查部门进行独立调查。详情请参见本报告商业道德—坚守阳光行为章节。



# 保障数字权益

腾讯通过构建管理架构、制定内部制度、秉持公平透明原则及加强安全运营，形成了保障数字权益的多维体系。在隐私保护、信息安全、AI安全治理和平台信任维护上，我们不断创新技术应用，加强监督与自律，确保用户在数字环境中享有安全、合法、信任且富有创新活力的体验。

- 3.1 隐私保护
- 3.2 网络与数据安全
- 3.3 AI安全治理
- 3.4 可信赖的互联网平台

## 联合国可持续发展目标一致性



## 联合国全球契约十项原则一致性

原则一：企业应该尊重和维护国际公认的各项人权；  
原则二：企业决不参与任何漠视与践踏人权的行为。

## 3.1

# 隐私保护

## 理念与原则

### 理念

腾讯以“数据安全是我们的生命线”为数据保护理念，始终坚持一切以用户价值为依归，这与我们的使命愿景“用户为本，科技向善”一脉相承，也是科技惠及用户的首要选择、是践行社会责任的应有之义。

我们始终坚持把个人信息和数据保护放在最优先地位，致力于为用户提供更安全、有保障的产品和服务；将安全、透明和可控作为隐私保护目标，坚持数据全生命周期合规，全链路治理，全方位保护；坚持创新与安全并重，让数据安全成为科技惠及用户和产业高质量发展的基石。

腾讯严格遵守业务运营所在司法管辖区的所有保护用户隐私及数据安全的法律法规，积极践行全球领先的隐私保护标准和规范。其中包括《中华人民共和国个人信息保护法》《欧盟通用数据保护条例》(The EU General Data Protection Regulation, GDPR)《英国数据保护法案》《加州消费者隐私法案》(The California Consumer Privacy Act, CCPA)以及其他运营地的相关法律法规，全方位保障用户隐私及数据安全。

### 原则

腾讯在严格遵守相关法律法规，充分尊重并保护用户权利的前提下，通过数据分析来改善用户的产品和服务体验。对于收集和使用的个人信息，我们严格保密，杜绝信息泄露、篡改、破坏、出售或非法提供给第三方，并充分保障用户对个人信息的管理。

#### 腾讯用户隐私保护原则：

##### ● 安全可靠

我们通过合理有效的信息安全技术及管理流程，防止用户信息外泄、损毁及遗失。

##### ● 自主选择

我们为用户提供便利的数据管理选择，以便作出适当选择及管理个人数据。

##### ● 保护通信秘密

我们严格遵守法律法规，保护用户的通信秘密，并提供安全的通信服务。

##### ● 合理必要

为了向用户提供更好的服务，我们只收集合理必要数据。

##### ● 公开透明

我们努力使用简明易懂的表述，向用户介绍隐私政策，以便用户清晰了解我们的信息处理方式。

##### ● 隐私设计

我们在产品和服务研发、运营的各个环节，融入隐私保护的理念。



\*腾讯混元AI生成

## 管理架构与制度

### 管理架构

腾讯在各个层面高度重视隐私保护工作，并已将其纳入集团的风险管理框架中。管理层致力于隐私优先的管治方法，制定并实施全面的内部评估流程，确保对所有产品进行充分评估，以遵守所有适用的数据隐私法律。此外，我们确保所收集的数据均安全传输及存储。从自上而下，到自下而上，数据隐私保护是一项有组织的工作。

高级管理层设立虚拟组织，负责隐私保护工作的体系化管理，推动制度建设和实施，进行工作指导和监督。在执行层面，我们设立有数据合规和隐私保护部，依据不同运营地区的隐私相关法律要求，负责统筹相关工作。例如，在欧盟地区，基于GDPR的要求，我们设立数据保护官(Data Protection Officer, DPO)。

此外，我们的隐私保护团队还会深入各个事业群，负责与产品团队紧密合作，确保产品和服务从最初就考虑到包括隐私设计和默认隐私在内的隐私措施，并确保遵守所有适用的法律法规；以及与工程团队协作，确保我们的数据收集和使用过程的透明度，并提供相应功能帮助用户管理自己的数据。

### 制度

腾讯制定覆盖数据保护和隐私的制度，适用于内部所有事业群的各类数据产品。这些制度从数据收集、分类分级、用户信息合规、数据应用、合规性检测等多个方面，为腾讯相关工作提供规范和指引。

在网络世界保护好未成年人，其个人信息与隐私保护是必要环节。我们构建了未成年人个人信息保护体系，成立了核心小组专门负责未成年人保护事务的调研与处理。同时，我们在内部知识分享平台上发布多篇未成年人保护合规宣传文章并多次组织内部宣讲会，以推动业务加强未成年人个人信息保护措施。我们为产品配置了多项未成年人个人信息保护指引，如《未成年用户保护合规指引》《游戏开发者隐私合规指南》等。我们已于腾讯隐私保护平台发布《儿童隐私保护声明》，并设置专门电子邮箱dataprivacy-kids@tencent.com接收并响应儿童个人信息相关的请求。针对国际业务，我们发布了《海外未成年人隐私保护管理标准》等进行业务规范和指引。



\*腾讯混元AI生成

## 以用户为中心的隐私保护方案

腾讯构建以用户为中心的隐私保护方案，通过完善隐私合规评估流程和工具，同时结合国际标准、技术创新、员工培训，将保护隐私融入企业文化建设等多个方面的工作，确保用户隐私得到最大程度的严格保护。

### 贯彻与审计

腾讯秉持“将隐私保护融入设计”的方法论，建立数据隐私合规检测的制度流程，将用户隐私的保护贯穿整个产品生命周期。此外，我们要求产品具备隐私管理功能，并提供隐私管理指引，帮助用户能够有效掌控个人信息。

腾讯在全球范围内遵守各地的数据保护法律，实施了一系列隐私保护策略。在中国内地，我们建立隐私影响评估 (Privacy Impact Assessment, PIA) 的机制和流程，并推进在各类业务场景中落地，精准识别和管理隐私风险，最大程度降低对用户个人权利的潜在影响。在国际市场，我们的全球隐私合规体系深度融入产品开发过程，通过技术检测进行复审，以确保遵守GDPR和CCPA等隐私法规。

我们的安全团队对自身业务的数据隐私保护负责，按照法规开展日常隐私保护工作。同时，我们还设立专业团队，对公司重点产品的敏感信息及数据的管理情况进行独立审核。

### 主动防御与应急响应

腾讯拥有完善的制度和流程，覆盖从被动防御到主动防御的运营环节。我们通过安全演练等措施，定期对用户隐私保护和数据安全的风险进行测试、发现、评估和缓解工作；持续识别系统漏洞或计划风险点，确保主动防御和应急响应计划的有效落实。如需了解更多应对措施和数据泄露响应措施，请参见保障数字权益 – 网络与数据安全。

### 员工意识与培训

腾讯通过开展多样化的隐私培训，包括但不限于线下和线上课程、内部博客、微报等方式，多渠道全方位传达公司个人信息与隐私保护政策、流程以及规范，确保所有员工都能意识到他们保护用户数据隐私的责任，并具备必要的技能来落实数据保护。其中，隐私和数据安全等重要原则与内容，已经纳入新员工入职培训、员工必修的年度阳光行为准则课程等环节，覆盖包括正式员工、顾问、实习生和外包员工在内的全部成员。

这些培训让员工了解隐私和数据保护的关键事项，不仅覆盖“将隐私保护融入设计”和“默认保护隐私”原则，还包括研发和操作规范。对个人信息处理岗位上的相关人员，我们还开展个人信息保护的专项培训和考核。

\*腾讯混元AI生成

## 管理监督供应商的隐私保护工作

腾讯已将隐私管理纳入供应商管理体系，在供应商ESG行为准则中，明确要求供应商承诺依法保护所有业务相关人员隐私权益，包括与其关联的消费者、客户、员工和供应商等。

我们通过一系列综合性的供应商隐私保护措施，进一步确保数据处理活动遵循腾讯的隐私保护要求。我们通过供应商调查问卷评估其数据保护措施的有效性。此外，我们还与供应商签订数据处理协议(Data Processing Agreements, DPAs)，要求他们履行腾讯的数据保护义务，包括采取加密、脱敏、匿名化处理等必要的技术和组织措施，并同意腾讯对供应商有审计权。在适用GDPR的业务场景中，我们还会对供应商进行严格的隐私尽职调查，以确保数据在收集、处理、存储和传输过程中的安全合规。

## 认证与认可

腾讯通过第三方审核和认证，包括ISO 27018公有云隐私保护认证和ISO 27701隐私信息管理体系等，来满足隐私要求。我们的重点业务始终保持着多项广受认可的隐私保护和数据安全认证，证明了腾讯的实践符合数据泄露事件响应管理的国际标准和最佳实践。

截至2024年底，

- WeChat、微信和QQ均获得TrustArc认证，微信和QQ具有中国网络安全等级保护三级认证。此外，微信还通过了ISO 27001信息安全管理体系认证。
- 腾讯云获得ISO 27701、ISO 27018、ISO 29151个人可识别信息保护实践准则等多项安全与合规认证。请参见本报告附录—腾讯云安全合规认证。
- 企业微信通过SOC 2 Type 2服务审计，获得ISO 20000信息技术服务管理体系认证、ISO 27001信息安全管理体系、ISO 27018和中国网络安全等级保护三级认证。
- 腾讯广告获得ISO 27001和ISO 27701等国际认证。
- 腾讯游戏海外发行平台Proxima Beta拥有ISO 27001和ISO 27701等国际认证。
- 腾讯文档等业务也获得ISO 27001认证。



\*代表性安全合规资质

## 用户权利保障

腾讯致力于为用户提供一个安全、透明和可信赖的数字环境，确保用户的隐私权利得到充分保障。对于未成年用户，我们的产品设置了更严格的保护机制。

### 数据收集与使用

腾讯遵循数据保护原则，在向用户提供产品和服务时，仅在必要范围内收集用户数据，确保数据处理的最小化，以符合预定的处理目的。我们的产品隐私政策明确规定我们可向用户请求的信息类型以及使用方式。此外，我们建设有内部访问控制，通过业务鉴权管控等措施，进一步保障用户数据安全性，防止隐私泄露。

### 用户数据的访问、更正与删除

腾讯为用户提供了多种便捷的渠道和简单的操作程序来行使与个人信息相关的权利，包括访问、更正个人信息以及删除包含所有数据在内的账户。用户可以通过自助简单流程或通过电邮联系腾讯，寻求其隐私权得到维护。

### 数据存储期限

腾讯遵守业务所在地区的数据保护法律法规，通过建立全流程数据处理规范，确保用户信息在达成使用目的后实现安全删除或完成合规匿名化处理。

### 沟通和申诉

腾讯已设置数种用户权利响应渠道，包括腾讯隐私保护平台、个人信息保护和隐私问题反馈问卷、邮箱、产品客服及信件邮寄，便于用户提出查阅、复制、更正、补充、删除等个人信息权利请求，并确保用户的个人信息权利请求得到及时响应和处理。当前，我们的产品均已建立针对个人信息主体权利的全面响应流程和处理机制。

### 第三方信息处理

腾讯在与第三方合作时严格遵循相关法律法规。在处理用户数据方面，我们秉承必要性和数据最小化原则，对数据处理涉及的第三方进行严格的限制。我们要求第三方对个人信息来源的合法性和合规性作出法律承诺，如第三方有违反法律行为的，我们会明确要求对方承担相应法律责任。

### 数据请求响应

当政府、监管机构等发出数据披露请求时，我们会充分征求内部和外部法务意见，依从以下原则制定合适的应对方案：

- 我们对全球范围内所有提供产品和服务的地区的机构所发出的合法请求，均保持一致性和公正性进行响应，确保符合当地法律法规的要求，并充分理解不同地区间的法律差异；
- 在遵守法律规定且条件允许的前提下，我们向用户公开因响应合法请求所采取的行动，以便相关用户有机会对此类请求作出反馈；
- 我们严格审核所有请求，确保在响应过程中严格遵守相关法律法规，并充分尊重和保护用户的合法权益。

\*腾讯混元AI生成

## 3.2

## 网络与数据安全

网络与数据安全是数字信任实现的重要基础，是用户信息与隐私权利的保障前提。我们在网络与数据安全领域持续投入，建立了专业的安全团队，并构建了自适应的闭环安全防护体系，以守护网络基础设施和数据资产的安全。腾讯云还获得全球多个地区的高级别安全资质认证，详情请参见本报告“附录一腾讯云安全合规认证”。

报告期内，未发生网络安全或数据泄露事件。

### 安全管理

腾讯设立安全技术委员会和不同职能、不同领域的专业安全团队。我们持续深耕技术前沿，广泛开展业务协作，拥有20多年海量业务安全运营和黑灰产对抗经验，在顶尖安全专家、安全大数据和AI技术积累上具有组织优势。我们致力于提升整体安全能力，提供业务需要的安全最佳实践，履行对用户、股东和社会的责任与义务，为腾讯的可持续发展保驾护航。

#### 我们的专业安全团队主要有：

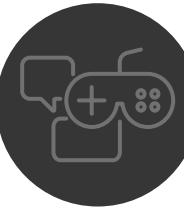
- 面向云与智慧产业的专业云安全团队，负责开展云平台安全治理、安全验证、产业互联网安全的技术创新。



- 技术工程事业群的安全团队，聚焦AI、数据、广告等领域的安全技术研究和工程实践，并联动内外的“白帽子”安全研究员，共同保障腾讯业务及数亿用户的网络安全。



- 面向社交、游戏、内容和支付金融等核心业务的安全团队，保障业务和产品安全运营。



- 多个安全联合实验室在车联网、物联网和AI等领域也对外联合相关产业，共同助力数字化时代的信息安全。



\*腾讯混元AI生成

## 安全技术

腾讯在公有云上开发和运营全部产品，向用户提供7×24小时不间断的高品质产品和服务。云平台安全是保障业务运营和维护用户权益的前提，我们在云安全、零信任、AI安全等领域保持高强度研发投入，增强云安全能力，以应对不断涌现的威胁，确保网络稳定可靠运行，保障信息系统的数据安全与业务连续性，让所有产品和业务的信息资产得到充分保护。

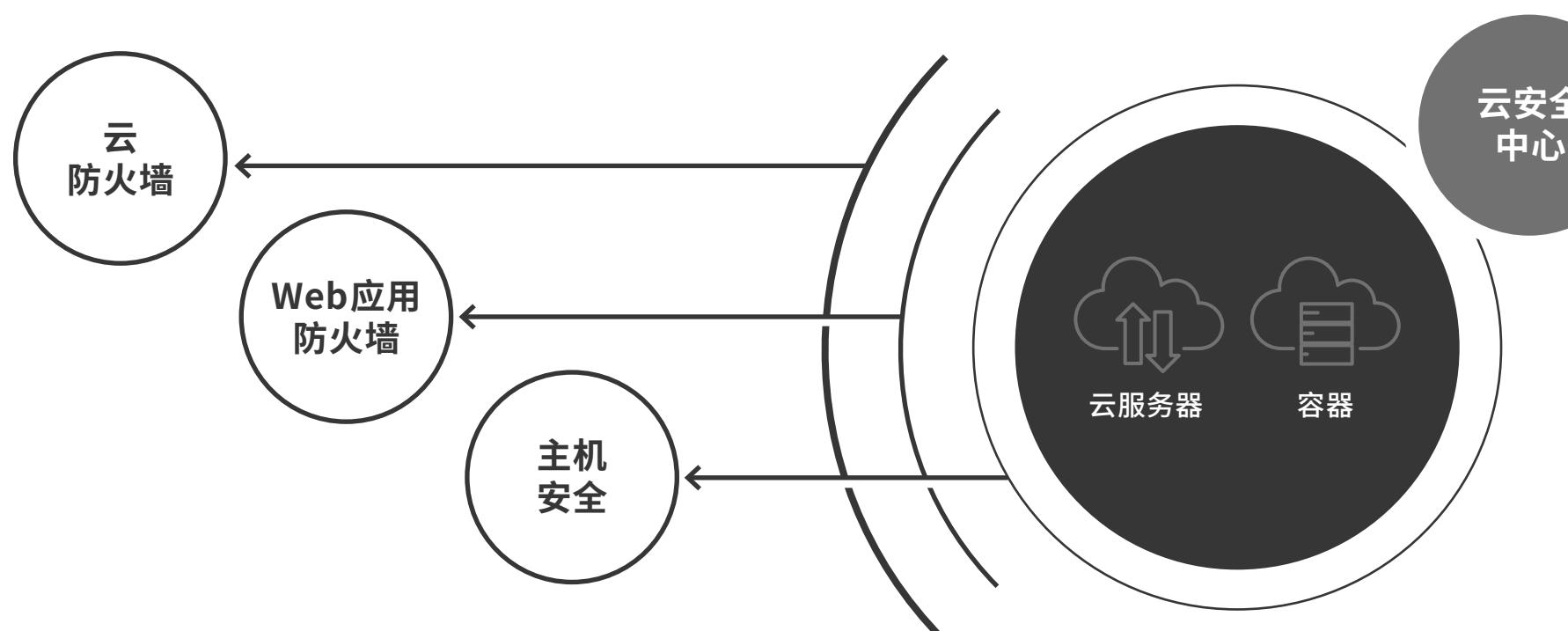
### 云安全防护体系

腾讯云以一个中心、三道防线建立了多层次的安全体系。该体系以云安全中心为核心，构建了三层防御架构：云防火墙、Web应用防火墙和主机安全。该安全体系不仅涵盖了物理安全、网络安全和主机安全等基础安全层面，还包括了数据安全、应用安全、业务安全、安全审计和安全管理等方面，形成了全方位的安全防护。

腾讯云安全运营注重发现和消除潜在的安全威胁，通过纵深防御、默认安全和智能提效，保障云上业务的安全稳定运行。2024年，我们进一步加强云基础设施、权限和密钥管理，构建数据安全边界，提高安全监控和应急响应的智能化水平，有效应对外部攻击和内部治理挑战，为全球数百万台服务器及亿级云资产提供了高效的安全保护。

在数字化转型过程中，终端安全正成为云安全的威胁来源。腾讯基于“持续验证，永不信任”原则构建零信任体系，是推动零信任发展的早期践行者。我们作为主要成员参与全球多个行业标准、团体标准的制定，其中包括由ITU-T<sup>1</sup>国际标准立项的全球首个零信任国际标准等。2024年，腾讯云的零信任安全解决方案iOA继2023年后再次入选Gartner中国零信任市场指南代表供应商。

2024年，腾讯持续迭代零信任方案，成为集成了下一代VPN、防病毒、桌面管理、端点检测与响应、数据丢失防护、软件管家和远程桌面等多重能力的办公安全一体化平台。我们积极探索大模型与安全的结合，完成更多云安全场景下的复杂任务。



### 数据安全策略

在遵循全球各运营区域数据安全相关法律法规的基础上，腾讯持续完善数据安全治理体系，通过在集团层面建立覆盖数据全生命周期的管理制度、系统来强化数据传输、存储、使用等关键环节的安全防护能力。我们的数据安全治理与业务场景紧密融合，在数据分级分类、数据访问代理、机密计算、运维管控等关键领域已经形成成熟和领先的工程实践。

我们在数据的全生命周期实施精细化管理，包括数据分类、分级、脱敏、加密和标记，通过以下措施确保数据在存储、处理和传输过程中的安全。

- 对数据访问权限实行了全结点实名制审核和维护，以保障数据资产的完整性和业务服务的可靠性。
- 建立了实时监控和拦截机制，以检测和阻止任何异常的数据访问行为。
- 对于处理敏感信息的关键业务，实施了网络隔离，确保数据只在受控环境中传输和处理。
- 通过智能监控和自动修复技术，可以有效应对大数据平台、数据库和存储设施的漏洞风险，防止数据泄露。

## 业务连续性保障

腾讯始终将业务连续性置于网络安全核心位置，通过持续加强核心技术研发，构建起一套全面的业务连续性管理体系。我们的数据中心遍布全球多个重要市场，网络出口分多个地域对接多个运营商。为此，我们构建了腾讯云网络跨地域的灾备能力，有效地降低运营商公网故障等带来的连续性影响。

腾讯云已经通过ISO 22301业务连续性管理体系的国际标准认证，彰显了我们在业务连续性管理方面的水平。我们对云产品的连续性进行风险评估和应急预案管理，并通过开展混沌工程验证其有效性。此外，腾讯还制定了一系列内部管理规定，并组建了专业的研发和运维团队，为业务连续性提供有力保障。

腾讯不断强化业务连续性自动化能力，将演练频率由季度提升到月度，加强测试系统的抗压和灾难恢复能力。这些演练模拟真实的经典容灾场景，包括攻防对抗和大规模故障等，全面检查系统的响应速度和恢复能力，确保真实容灾场景下的高效应对。通过这些举措，腾讯能够在突发状况发生时，确保业务可以迅速恢复正常。

## 软件供应链安全管理

保障软件供应链安全是实现腾讯云网络和数据安全的重要支撑。腾讯建立相关安全管理体系，明确管理层、业务层和技术层的分工与岗位职责，同时通过多种措施提高员工、供应商和云端客户的供应链安全意识，确保整个供应链中数据传输和处理的保密性、完整性和可用性。

腾讯对软件供应链的供应商制定了风险管理程序，涵盖风险评估、风险控制、风险监控及复盘改进等环节。我们要求供应商在商业项目启动前完成相关信息安全培训，并协助供应商提升信息安全意识和能力。同时，供应链安全管理体系的风险识别是一个持续的过程，包括年度整体风险识别和日常风险识别。此外，我们密切关注供应链安全威胁和风险相关的法律法规及其他合规要求的变化，并与相关方协作，确保将新增的法律法规要求能够及时应用于腾讯云的安全和风险识别评价中。

## 第三方审计与资质

腾讯云为腾讯全部产品提供开发运营环境，每半年接受独立第三方会计师事务所依据美国注册会计师协会的相关准则，对云服务体系安全控制的设计适当性和执行有效性出具报告。我们通过提供具有鉴证性质的系统与组织控制报告，向云用户机构、独立审计师、监管机构、公司股东及其他相关利益方公开腾讯云最新的服务组织内部控制情况。

符合国际认可的信息安全与IT管控标准是腾讯云信息安全建设基准的核心。我们已获得ISO 27001等多项行业领先的管理体系和管理认证，充分体现了我们在信息安全管理方面的高标准和专业性。

更多关于腾讯云安全合规认证的内容，请参看本报告附录—[腾讯云安全合规认证](#)。

\*腾讯混元AI生成

## 安全运营

腾讯持续整合安全能力和资源，优化网络安全风险的发现和修复流程，实现风险管理闭环、数据可视化、自动化修复及验证等一系列功能。

### 主动防御

腾讯致力于构建“情报—攻防—管理—规划”的主动防御安全能力体系，通过整合威胁情报、人工智能、大数据等技术，提升安全事件的响应能力和效率。目前，腾讯安全已建立百亿级的威胁情报体系，覆盖情报收集、分析和处置，并集成于全系安全产品中，能够快速识别并防御各类网络威胁。此外，腾讯安全还设立安全运营中心，以云原生技术为基础，结合技战术框架的最佳实践，聚焦威胁检测、调查和响应，提升安全运营效率，实现全网安全态势的可知、可见、可控。

安全技术委员会每月对安全事项进行评估，包括政策、系统和风险等，并就重要事项向高级管理层汇报，以保障信息安全管理的有效性和可靠性。安全团队每年对重要信息系统进行至少一次内部安全审计，确保信息安全措施的有效执行和相关法律法规的合规水平。

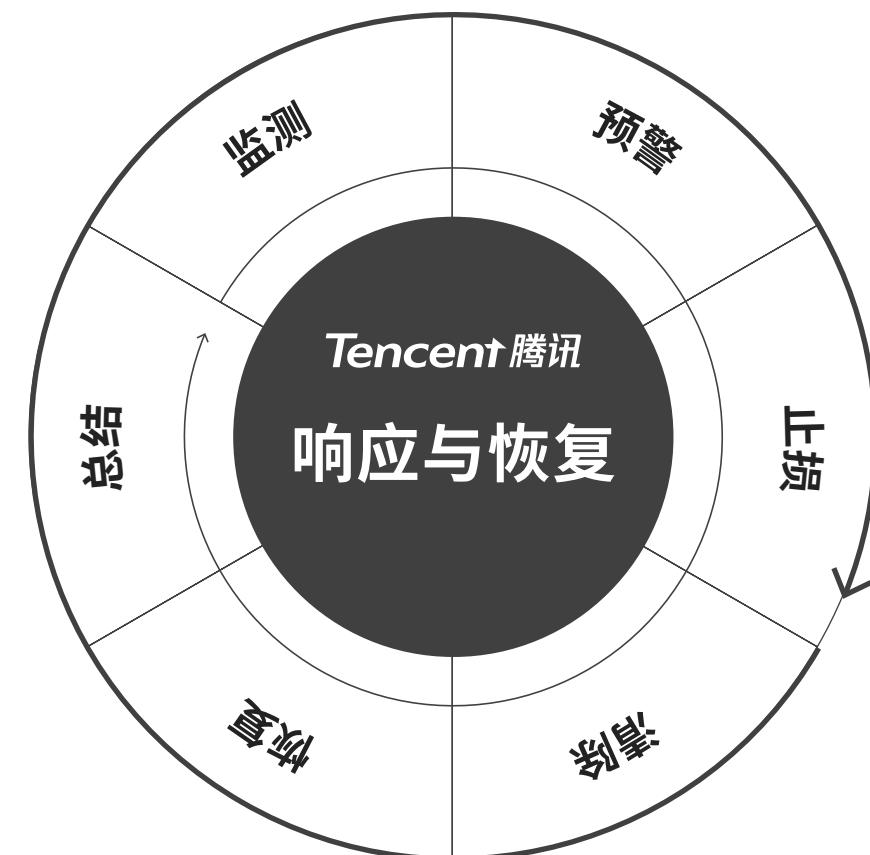
腾讯进一步加强主动防御的安全能力，提出“安全融入”理念，强调安全与业务的深度融合。通过构建安全防护体系，我们实现对安全风险的主动感知、有效掌控以及对业务增长的推动。例如，腾讯研发了安全大数据分析平台，以解决拍字节(PB)数量级的安全数据难以分析和回溯的难题。同时，我们还强化了终端安全能力，以终端检测与响应技术为核心，结合安全专家团队的支持，构建起了立体化的终端安全防护体系。

### 响应与恢复

腾讯按照ISO 27001信息安全管理标准开展网络安全的应急响应和恢复工作。我们每年对信息系统进行安全测试、风险评估和内部审计，确保安全防御能力始终处在合理状态，符合相关安全管理和标准的规定与要求。

在管理制度上，我们制定并实施了《腾讯安全事件管理制度》，详尽规定了安全事件的检测、报告以及应急处理流程，保障了对各类安全威胁的快速、有效及有序响应。

在安全运营中，我们的应急响应工作聚焦于漏洞发现、入侵排查、攻击防御，7×24小时开展专业的安全运营工作。团队能够迅速介入并处理安全告警，完成初步分析并制定遏制方案，并完成安全组件的规则调整和删除后门木马等行动，有效阻断攻击者的利用路径。



### 培训与宣导

对员工开展信息安全培训是腾讯加强网络与数据安全的重要举措。我们建立了多样化的培训课程，包括全员必修培训、重点岗位培训和自选专业课培训等，内容覆盖基础安全意识、漏洞与防御、研发安全规范和数据安全要求等方面。

腾讯要求所有正式员工入职后必须学习信息安全培训课程，顾问、实习生和外包员工也需要学习工作规范须知及信息安全必修课。此外，我们还面向不同岗位的员工开展专项培训，包括《研发工作的安全规范》《软件源代码安全规范》《运维工作的安全规范》等。同时，我们会根据安全技术发展和形势，对安全团队的员工进行技术培训，确保他们了解并遵守最新的安全规定和操作流程，掌握最新的信息安全标准和最佳实践，并能够在安全事件发生时迅速有效地响应。

2024年，  
参加腾讯信息安全专项培训的总人次达到  
**33,145**名，  
累计培训时长超  
**69,724**小时。

此外，我们明确了《腾讯阳光行为准则》的信息安全要求，并制定了安全规范。这些要求和规范是员工在年度考评中必须学习的内容之一，未完成者将影响绩效考核结果。对于明确违反安全高压线并造成实际影响的员工，腾讯将按事故管理办法处理，严重者将被解除劳动关系。

我们还每年举办腾讯安全技术峰会和腾讯技术周安全分会场，并开展日常安全测评、内部博客宣导和有奖问答等活动，持续提升全体员工对个人信息和隐私保护的重视程度，确保其及时更新相关工作要求。



## 共建与合作

腾讯在零信任、云安全、隐私保护及区块链等领域积极参与国际标准制定，或建设最佳实践案例，并通过技术开源及产学研合作，推动数字安全生态发展。

- 在零信任领域，腾讯和微软、谷歌、思科等企业主导研制全球首个零信任国际标准——《服务访问过程持续保护指南》。我们积极推动全球零信任标准化应用以及落地国内，并成为中国零信任产业标准工作组主要创始会员，促进行业安全理念从“持续验证”向“持续保护”落实。
- 在云安全方面，腾讯云是国际云安全联盟 (Cloud Security Alliance, CSA) 高级会员，积极参与全球云安全标准制定。依托内部安全团队开展前沿技术研究，腾讯云安全能力已经获得国际权威认证。
- 在隐私保护领域，腾讯是可信计算联盟 (Confidential Computing Consortium, CCC) 的创始会员，其成员来自全球的多家科技企业。我们致力于推动可信计算技术在全球的普及和发展，以解决数据安全保护中的薄弱环节，同时积极参与多项行业标准、和落地中国标准的起草和修订工作。我们的产品也广泛通过多项国际认证，与国际主流标准全面接轨。
- 在区块链技术方面，我们构建开放生态，发起成立产业区块链联盟，推动标准制定与跨行业协作。2024年我们主导研制了《基于区块链技术的数字藏品服务技术要求》(IEEE Standard Technical Requirements for Digital Collection Services Based on Blockchain Technologies)《基于分布式账本技术的数字藏品服务框架与要求》(ITU-T F.751.10 Framework and requirements for DLTbased digital collection services)等数个国际标准建设。

2024年，腾讯安全有七项技术入选国际研究机构 Gartner发布的《2024中国网络安全技术成熟度曲线》报告。入选的技术包括软件成分分析、安全事件管理、攻击面管理、零信任网络访问、安全服务边缘、机密计算和多方安全计算，用于在网络环境中加强安全防护，提升业务敏捷性。

\*腾讯混元AI生成

### 3.3

## AI安全治理

腾讯将负责任的人工智能(AI)发展视为我们长期的战略重点之一，在推动业务增长的同时，致力于将伦理与安全融入AI技术的开发与应用，以此促进负责任的创新。我们高度重视人工智能带来的安全挑战，积极与国际治理前沿趋势接轨，持续提升AI治理水平，从而应对和缓解潜在风险。在遵守运营所在地法律法规的基础上，我们把数据质量、安全合规及伦理道德作为重要考量，实施了一系列风险管理措施。

### 治理体系

#### 治理原则

腾讯于2018年就提出“可知、可控、可用、可靠”的AI治理原则，并长期探索和深化科技价值观，坚持以“科技向善”引领AI治理工作，致力于对社会负责并造福人类。同时，我们在AI生命周期各阶段进行风险评估，将多方因素纳入安全管理流程，确保风险可控且符合法律法规。

2024年12月，我们参与签署由中国人工智能产业发展联盟发布的《人工智能安全承诺》，在设置安全团队、开展安全测试、保障数据安全和增强透明度等方面，对外界作出应对风险和开展治理的承诺。

#### 管理制度

腾讯设立了AI技术委员会，旨在促进跨团队的AI技术交流、评估和指导AI项目，并推动AI技术在公司内的长足发展。AI技术委员会下设多个技术协作团队，专注于解决AI系统的开发原则、性能评测和伦理考量等问题。此外，腾讯AI实验室还积极探索基础模型的可靠性和智能风险治理等前沿领域，以构建更加可靠和安全的AI系统。针对内容安全、隐私保护和模型安全等议题，腾讯AI安全团队在公司内部多次发起过超千人的大规模安全测试，以提前发现并收敛AI安全风险。

我们参考全球AI安全与治理领域的积极探索和优秀实践，制定并实施了《腾讯AI数据安全管理制度》《AIGC新产品新功能评估报批管理制度》等一系列人工智能管理规范，并在业务发展中持续完善和更新这些规范。同时，我们对现有的数据安全、数据治理等规范进行修订，新增人工智能相关数据和内容的处理规定。腾讯AI安全治理团队基于这些规范，构建了高效的业务和管理流程，形成与国际前沿趋势保持一致的治理框架。

我们在安全类别体系、对抗攻防、隐形毒性内容检测、训练数据脱敏、社会伦理道德植入等方面持续投入研发资源，助力AI产品的安全运营，以应对人工智能领域新兴的数据安全、模型安全和伦理风险等问题。

## 安全治理

### 治理框架

腾讯重视人工智能的安全治理，从数据、算法和运营三个维度开展治理工作。

在数据治理方面，腾讯通过制定并贯彻数据安全策略，全面规范管理AI数据处理的全生命周期活动，明确责任部门的职责范围，严格审核并筛选高可信数据源，运用先进算法进行深度数据清洗和安全过滤等方式，保障AI数据始终处于有效保护状态并合法使用，为用户隐私和数据安全构筑坚固防线。

在算法治理方面，腾讯持续开展AI算法安全性评测与调校，定期识别并修复潜在的安全漏洞，测试并强化模型的抗攻击能力，优化模型性能并减少偏见，同时建立跨部门安全团队审查机制，确保模型在技术实现和数据使用上均符合业务需求和安全标准。

在运营治理方面，腾讯持续对风险进行监测、预防及应对，采取多层次安全防护，确保模型输出安全准确。此外，我们通过应用内容标识技术追踪风险内容，不断提升模型的安全水平，以实现对用户和社会责任的持续承诺。

### 用户权利保障

在AI安全治理的原则与框架下，我们进一步细化和规范AI产品的数据处理，以确保用户权益得到充分保障。腾讯AI相关产品的数据管理严格遵循合法、正当、必要的原则，并建立相应的隐私保护管理制度、流程和组织架构。我们通过安全保障机制和安全技术体系，致力于守护用户信息安全。同时，腾讯高度重视用户权利保障，提供投诉举报渠道，并在法律规定期限内(如有)及时响应用户诉求，确保用户的个人权利得到有效满足。

### 安全合规

腾讯的AI业务和产品聚焦于民用领域的创新和应用，将安全合规要求融入AI研发全流程。我们紧跟最新的AI法规及行业发展趋势，并实施全生命周期数据管控。同时，我们积极探索隐私计算等前沿技术，以应对AI领域的新兴挑战。此外，我们积极规划内部安全管理流程与框架，致力于实现更加可信和负责任的AI系统。腾讯混元首批通过备案，符合中国生成与合成内容、服务管理、算法推荐等监管与标准要求，并获得相关认证，为用户和合作伙伴提供安全可靠的服务。

- **2024年4月**，腾讯参与编制了由世界数字技术院 (World Digital Technology Academy, WDTA) 发布的《生成式人工智能应用安全测试标准》和《大语言模型安全测试方法》两项国际标准。
- **2024年5月**，腾讯混元通过了由中国网络安全等级保护中心组织的中国首批大模型系统安全能力验证活动，凭借在设计开发安全层面的卓越表现，获得“大模型系统安全能力评价证书”。
- **2024年12月**，腾讯获得WDTA和云安全联盟大中华区颁发的首批“人工智能安全、可信和负责任”测评资质。该资质标志着腾讯在人工智能领域的安全标准化建设达到行业领先水平。

## 发展与应用

### 利用AI推动可持续增长

腾讯致力于运用人工智能技术推动可持续发展，从而惠及企业和社会各界。我们投入大量研发资源深耕人工智能核心能力及自研混元大模型，值此为我们的消费者业务和企业服务业务奠定了重要的技术底座。目前人工智能技术已应用于700多个业务场景中，并拓展至可持续社会价值创新项目。更多详情请参看本报告数字技术助力可持续发展目标章节。

### 拥抱开源发展战略

腾讯积极拥抱开源发展，腾讯混元的开源模型已经覆盖文生文、文生图、文生3D及文生视频等多个模态，降低个人了开发者和中小企业的开发成本，推动了促进人工智能技术的普惠化发展。腾讯开源模型得到了开源社区的高度认可，在GitHub上的星标数接近1.4万颗，并多次登顶该行业趋势热榜。

### 安全合作与共建

腾讯在内部积极开展AI安全治理的宣导工作，通过腾讯技术文化周、ESG文化周等活动，邀请内外部专家共同研讨当前的主要风险、技术趋势和发展方向。同时，我们还将内部的技术实践通过标准建设、行业交流的方式与外部共享，例如参与共建深圳地方标准《人工智能预训练模型价值对齐技术框架》等。

- **2024年1月**，腾讯朱雀实验室、腾讯研究院与合作伙伴联合研究并发布《大模型安全与伦理研究报告2024——以负责任AI引领大模型创新》。报告对大模型安全框架和AI价值对齐进行了系统性剖析和展望，并围绕大模型安全分享相关实践做法。
- **2024年5月**，腾讯云在中国生成式AI产业应用峰会上发布生成式AI安全解决方案，涵盖全链路内容安全和数据安全解决方案，帮助企业筑牢“数据”和“内容”安全防线。
- **2024年6月**，腾讯研究院发起了“科幻与AI新技术”研究项目，从科幻、人文与技术的交叉视角，前瞻性探索人工智能新技术的未来场景与社会影响，并探索AI治理与AI向善的原则、场景及行动路线。



\*腾讯混元AI生成

### 3.4

## 可信赖的互联网平台

腾讯致力于为用户构建安全、可信赖的互联网平台，在内容生态、商品交易、广告责任、客服沟通等方面落实平台责任。

我们遵循包括《世界人权宣言》《公民及政治权利国际盟约》《经济、社会及文化权利国际公约》《儿童权利公约》《儿童权利与企业原则》等国际原则和公约的要求，积极响应联合国《可信赖的互联网》倡议以及世界经济论坛《全球数字安全原则》，致力于为用户提供一个安全、健康且积极的数字环境。

### 维护健康的内容生态

腾讯持续促进各平台的内容生态健康，严格防范虐待、暴力、毒品、诈骗、恐怖主义、极端主义、仇恨、虚假、歧视、骚扰、自我伤害、色情等各类有害信息。

#### 内容安全与可靠

我们制定并实施了《信息内容安全管理规范》《信息内容安全事件应急处置工作规范》等内容安全管理政策，把内容安全融入到整个产品生命周期管理的各环节中。业务团队根据产品功能特点开展风险评估，制定和实施了有针对性的内容安全政策和防护措施。这些措施能及时识别并处理有害内容，在自有及运营的内容平台上为用户提供有效的保护。我们还制定了内容创作规范与指引，帮助创作者避免生成违法、违规及有害内容。

微信辟谣助手小程序帮助用户识别网络谣言，防止其受到虚假信息的侵害。该小程序整合了数百个权威信息源，持续更新辟谣信息。用户遇到存疑信息时，可搜索关键词进行核实，获取真实情况，从而避免误信不实信息。

我们为创作者提供生成式人工智能或深度合成等技术的创作指引，明确使用人工智能生成内容必须严格遵守法律要求。同时，我们识别和标记人工智能生成或合成的非真实内容，帮助用户清晰辨别。

用户在遇到各类有害或虚假信息时可以在产品端进行反馈和投诉。产品团队核实确认用户提交的证据后，会根据违规严重程度，对违规账号进行相应处理。

#### 保护与激励内容创作

我们持续完善创作者知识产权保护体系，以防止侵权为核心，严厉打击抄袭、搬运、仿冒等违规行为。我们建立“电子授权—监测—维权”防侵权平台，为创作者提供全网盗版监测和一键维权服务。各创作平台开设了专门的申诉渠道，供创作者在遇到侵权行为时进行反馈。我们依据法律法规积极处理侵权申诉，如删除、屏蔽侵权内容，维护创作者权益。

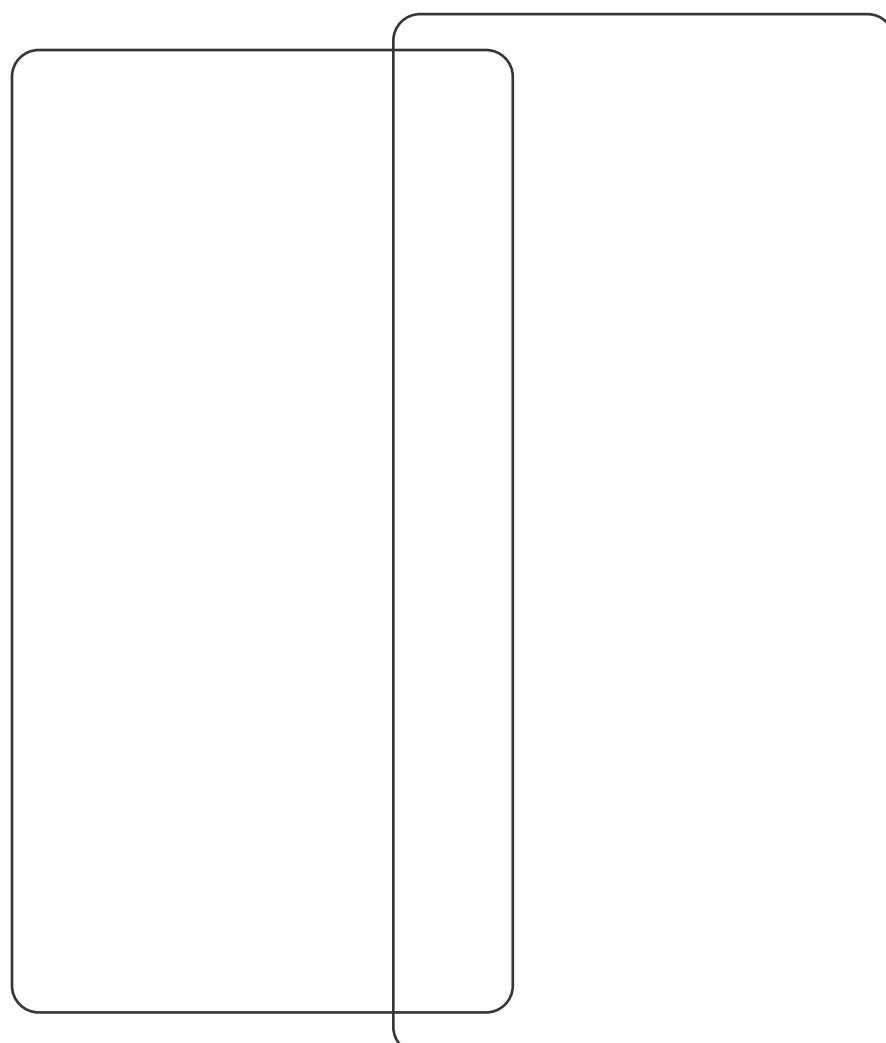
我们为创作者提供便捷的内容管理工具，包括内容分发、账号管理、收益管理、数据分析和宣传推广等流程工具，帮助创作者提升创作效率，促进优质内容的生产和传播。我们还提供线上课程，帮助创作者掌握内容生产技巧，提升运营水平。

我们的平台为创作者提供多种收益途径，包括广告分成、付费订阅、电商合作、品牌代言等，使其内容创作得到合理回报。我们还在短视频、图文、小游戏、音乐、网络文学等各类型的平台推出了一系列创作者激励和培养计划，如面向短视频制作者的北极星计划、面向网络文学写作人才的青年作家扶持计划、面向原创音乐人的新势力计划等，帮助他们持续成长。

- 隐私保护 • 网络与数据安全 • AI安全治理 • 可信赖的互联网平台

## 打击网络诈骗

在严格保护用户个人隐私的基础上，针对诈骗行为，我们在微信支付建立了预防和应对机制。当系统识别交易存在欺诈风险时，微信支付会在转账页面中给予风险提醒，并推送语音风险预警进行劝阻。如果劝阻无果，微信支付还会通过延迟支付机制启动时长15分钟的转账冷静期，保护用户免受损失。截至2024年底，我们累计向超过156万用户推送微信支付防诈骗自动语音预警，协助用户避免了超过人民币68亿元潜在损失。根据用户举报案例，我们建立了可以提供特征分析的反诈案例库，持续强化反诈策略模型，提升风险管控的覆盖率、及时性和有效性，并为银发族和未成年人进行优化。



\*微信支付风险提醒

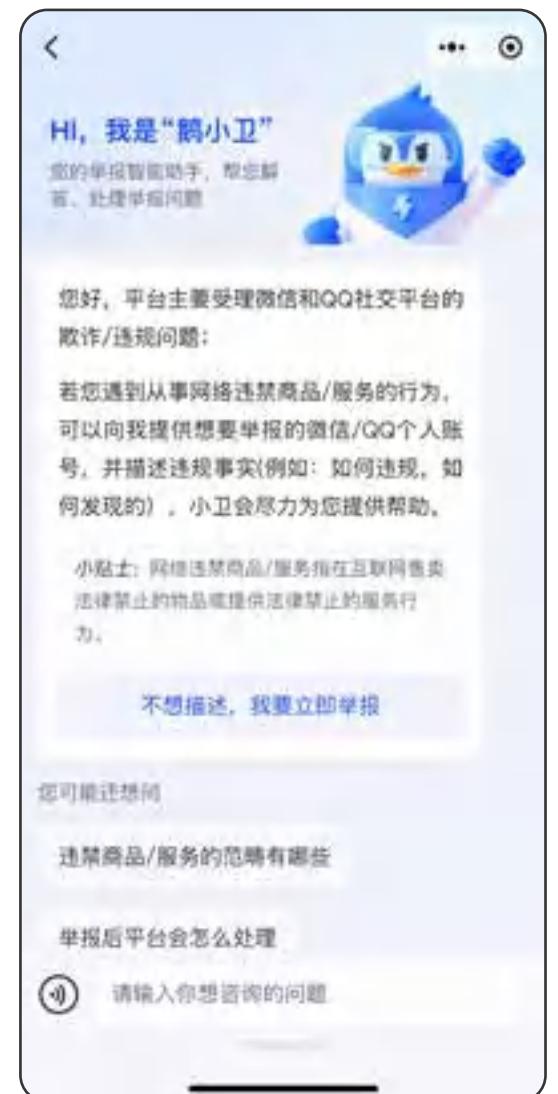
## 严禁网络销售假冒品与违法商品

为保护用户和品牌权利人的合法权益，我们严格禁止销售假冒商品。以微信为例，用户若怀疑他人发布假冒商品营销信息或销售假货，可通过微信品牌维权平台提交侵权线索。经品牌权利人鉴定确认后，我们将根据鉴定结果进行相应处理，包括移除侵权信息、封禁账号等。截至2024年底，微信品牌维权平台已接入超过640个国际知名品牌。在微信视频号直播平台，我们已针对售假内容建立主动防控机制，并持续更新和优化识别模型，自动巡查并中断涉嫌售假直播。此外，微信小店采取了多种措施，包括在商家开店和商品上架时审核资质，防范假冒商品发布，并对违法销售行为及违规商品持续进行巡查，确保及时处理侵权行为。

除打击假冒产品外，我们各平台也禁止营销任何法律法规禁止和限制销售的商品或服务。通过关键词检索和图片识别等技术，我们持续打击平台上的各类违法产品，包括但不限于枪支弹药、爆炸物、管制刀具、受保护的野生动植物活体及其制品、烟草、医疗服务和器械，以及药物等。

## 举报网络违法行为

我们在各产品页面中设置了专门的入口，方便用户便捷、高效地提交投诉或争议。通过腾讯卫士小程序，我们将及时响应用户对网络违法行为的举报，并在核实情况后对违规账号采取相应措施。



\*腾讯卫士小程序举报页面

\*微信品牌维权平台运作流程

## 落实平台的广告责任

### 管理准则

腾讯制定并持续优化《腾讯广告审核通用规则》以及相关系列政策，内容覆盖承接登记广告业务、审核、档案管理制度，查验核实广告主身份文件，以及审核广告内容合规性等，这些政策已在腾讯广告官网[“帮助中心”](#)公开。这体现了我们根据《中华人民共和国广告法》《互联网广告管理办法》等相关法律法规要求，履行审核广告主资质和广告内容合规的责任，并在此基础上积极协助广告主保障广告内容的真实性。

《腾讯广告审核通用规则》明确规定，广告不得包含赌博、暴力、歧视、影响儿童福祉、危害健康与安全、武器、非法野生动物与濒危动物的活体及其制品等相关内容。我们对此项规定的内容进行公示和宣导，让广告主和各业务环节的合作伙伴都能知晓并严格遵守。

《广告服务商管理规范》明确规定了广告服务商的责任、义务，以及对违规服务商的处罚措施。我们还为服务商提供专项培训，协助其识别不符合资质要求的广告主以及不合规的广告内容。这些措施有效支持广告服务商和广告主履行合规责任。

### 流程管控

针对广告投放前、中、后环节，我们构建了有效的管理机制，实施全流程风险管控。

#### 广告投放前

我们通过多种手段核验广告主身份和资质的真伪，确保广告主真实、合法、有效。审核系统中的广告主黑名单功能可以自动拦截违规广告主。此外，我们还设置了一系列前置措施，防范广告中可能存在的违法违规内容，包括线下预审、对推广链接进行审核、系统自动识别并过滤广告违规内容。



#### 广告投放中

我们运用大模型技术提升广告审核系统对违规行为的自动识别和拦截能力，辅助审核人员及时发现和处置可疑或存在违规风险的广告。我们也通过专项培训提升审核人员的识别和处理能力。



#### 广告投放后

我们通过自动巡查系统结合人工复查，对所有审核通过的广告进行全面复检，以防止违规行为的发生，特别是常见的广告链接跳转页被篡改的情况。我们持续提升广告审核与治理机制的可靠性与有效性，并通过与相关方的沟通收集反馈。

### 宣导与培训

我们持续对广告服务商、广告主等宣传有关广告合规知识，通过在线课程、线下培训等方式，普及法规及审核规则、介绍典型违规案例、给出合规建议，并安排专人答疑。

- **培训：**我们每半年为全体广告服务商组织一次常规培训。针对风险较高的服务商，还会安排一对一的合规宣讲培训。2024年，我们累计组织培训超过40场。



- **认证：**我们为全体广告服务商开展了风控师资格认证。认证培训内容涵盖广告业务中的各类风险管理，帮助服务商学习并建立自己的风控管理体系。



- **沟通：**我们为广告主和广告服务商提供了多种沟通渠道，包括广告帮助中心、QQ客服、微信客服、邮箱等，以提升信息沟通的有效性和时效性，并增强他们的合规意识及能力。



## 提供便捷的用户沟通渠道

腾讯持续提升客服能力，致力于提供以客户为中心、及时的优质服务，满足客户的期望。

### 消费互联网

我们设有智能自助和人工专业客服，提供包括汉语、英语、土耳其语和阿拉伯语在内20多种语言服务，妥善处理用户就各类产品的问询。对于重点群体，包括创作者、未成年人、银发族以及支付用户，我们更设置了专属的沟通和申诉渠道。2024年，消费互联网客服系统引入了腾讯混元，进一步增强了智能客服的问题分析和应答能力，提升了用户体验。

我们的消费互联网业务客服体系包括互联网服务客服和视频号客服。

- 2024年，消费互联网业务客服体系接收用户投诉153,962,802宗；其中，由互联网服务客服受理的投诉在三个工作日内的闭环处理率达99%。
- 互联网服务客服年服务次数（含自助服务）超过45亿次。

### 产业互联网

我们配备了专业全球技术服务团队，为企业、组织和个人开发者等客户提供高效支持。通过电话热线、在线客服及服务群组等渠道，实现全天候快速响应和优质服务。2024年，我们引入腾讯混元，进一步提升智能化服务的效率和专业性。

我们的产业互联网业务客服体系包括云业务客服和企业微信客服。

- 2024年，产业互联网业务客服体系受理用户投诉15,141宗。
- 云业务客服受理的投诉在7天内处理完成率85%，客户五星满意度达96.2%。
- 企业微信客服服务的大客户满意度为98.1%。



- 为未成年人构建适龄的网络环境
- 助力银发族享受数字时代
- 助力身体障碍人士跨越数字鸿沟
- 数字技术助力农村地区发展

# 数字包容

腾讯致力于为所有人提供覆盖健康、教育、金融服务等领域的安全、普惠、有意义的数字产品和解决方案，尤其关注未成年人、银发群体、身体障碍人士，以及欠发达农村社区，推动社会进步与包容性发展。通过这些举措，我们践行“用户为本，科技向善”的愿景使命，积极响应联合国和国际电信联盟提出的《数字包容》倡议。

- 4.1 为未成年人构建适龄的网络环境
- 4.2 助力银发族享受数字时代
- 4.3 助力身体障碍人士跨越数字鸿沟
- 4.4 数字技术助力农村地区发展

## 联合国可持续发展目标一致性



## 联合国全球契约十项原则一致性

原则一：企业应该尊重和维护国际公认的各项人权。

## 4.1

## 为未成年人构建适龄的网络环境

互联网为未成年人的沟通、学习和社交提供了前所未有的机会。腾讯致力于构建适龄的网络环境，让未成年人能安全地探索新想法，学习新技能，助力他们健康成长。

我们密切关注与互联网儿童权利保护及安全相关的国际公约、原则和倡议，并采取适当措施跟进。这些重要国际公约、原则和倡议包括《儿童权利公约》《儿童权利与企业原则》，以及联合国儿童基金会《建立以儿童为中心的数字平等框架》和国际电信联盟《儿童在线保护指南》等。我们致力于预防未成年人接触可能对其认知、社交和情感发展产生负面影响的内容，包括色情、暴力、自残、网络欺凌以及性骚扰等。同时，我们严格遵守《中华人民共和国未成年人保护法》《未成年人网络保护条例》等中国法律法规，并密切关注欧盟、英国、澳大利亚、印尼等地相关法律的制定与实施，采取有效措施保障当地未成年人用户的权益。

### 适龄的内容和行为

除了构建适龄的网络安全环境，腾讯也关注自身平台上的内容是否满足适龄需求，积极引导未成年人形成正面的网络素养，助其心智健康成长。

#### 视频与直播内容

在未成年人模式下，我们各视频平台为未成年人推荐适龄的视频内容。仅在启动“监护人授权”功能后，微信视频号入口方可开放。

#### 消费行为

我们为家长提供了未成年人消费限额功能，家长可对未成年人微信支付账户设置每日和单次消费限额。此外，在微信未成年人模式下，我们屏蔽了公众号和视频号资料页上的微信小店入口，并禁止使用直播打赏功能。

#### 广告内容

我们禁止在网站、应用程序、公众号等自身平台上向未成年人发布和推送特定广告内容，包括医疗药品、美容广告、烟酒类、金融贷款、网络游戏、娱乐直播、婚恋交友等，同时，禁止任何可能诱导未成年人模仿不安全行为或具有不良导向的广告。我们严格遵守与未成年人保护及广告监管相关的法律法规。更多关于广告投放要求的细节，请参看保障数字权益—可信赖的互联网平台的相关内容。

## 网络游戏

在中国内地，我们为未成年人提供了一系列游戏保护措施，包括实名验证、适龄提醒、时长限制、家长监护功能，并为不同年龄层用户设置相应的游戏消费限额等，重点措施如下：

- 游戏时长限制：未成年人仅可在周五、周末与法定节假日每日的20时至21时登录游戏；
- 游戏消费限制：禁止12岁以下用户进行游戏消费；
- 限制未成年人使用成年人账号：结合筛查系统和禁止转让游戏账号的措施，防止未成年人使用或购买成年人账号。

中国内地游戏行业积极推进未成年人游戏保护措施，取得了显著成效。根据中国音数协游戏出版工作委员会发布的《2024中国游戏产业未成年人保护报告》，75.1%的未成年人每周游戏时长控制在3小时以内，超过80%的未成年人玩家不充值或月充值金额低于人民币30元。这表明多数未成年人已逐步养成健康游戏习惯，游戏行业的未成年人保护工作成效显著。

## 支持家长

在现实世界中，未成年人的成长需要父母的保护和引导，网络世界也应如此。为此，我们为家长提供了监督和引导未成年人使用网络的功能，并支持他们提升网络安全意识和技能。

- 微信为家长提供未成年人模式下的“监护人授权”功能。家长可批准未成年人用户临时访问公众号、小程序、网页链接，或延长当天使用视频号时间。
- 腾讯成长守护小程序帮助家长监督和限制未成年人的游戏时长和游戏消费。

- 腾讯未成年人家长服务平台小程序为家长提供网络安全教育视频、工具、辅导案例与心得，并邀请专家团队提供专业辅导。

截至2024年底，  
腾讯未成年人家长服务平台小程序累计为超过

**3,600**万用户提供支持。

截至2024年底，  
腾讯成长守护小程序已累计为超过

**7,000**万用户提供支持。

- 为未成年人构建适龄的网络环境
- 助力银发族享受数字时代
- 助力身体障碍人士跨越数字鸿沟
- 数字技术助力农村地区发展

## 网络安全技能与工具

我们协助未成年人及家长掌握必要的网络安全知识和技能，并提供相应的保护机制，帮助未成年人在网络上安全地获取信息并负责任地表达自己。

我们为未成年人提供线上线下多种网络安全教程，帮助他们掌握相关安全技能。通过这些措施，未成年人能够识别有害信息，避免受到侵扰，并在个人信息和金融安全方面进行自我保护。在线上，我们通过微信、QQ、腾讯卫士及腾讯成长守护小程序等渠道，以视频、互动问答等形式，帮助未成年人提升识别和管理网络风险的能力。在线下，“腾讯护苗工作站”和“腾讯未成年人保护营地”等团队走进社区，向儿童及其家庭传递网络安全知识。2024年，我们联合壹基金在中国15个省开展了网络安全专题教育活动。



网络扩大了未成年人的人际交往范围，满足其情感表达需求，但也对其心理健康带来了挑战。腾讯未成年人家长服务平台小程序和QQ企鹅守护站为未成年人提供有关心理健康视频教程，帮助他们及其家长疏导网络不良经历造成的负面情绪。2024年，我们联合公共机构和学术机构推出“正向方程”青少年心理健康项目，开展未成年人心理健康研究与科普，并基于腾讯混元开发了AI工具，协助辅导人员初步评估问诊者的心理状态。

我们在产品中设立了保护未成年人个人信息安全的相关指南，并设置专门的电子邮箱dataprivacy-kids@tencent.com，供未成年人就数据隐私问题提出疑虑或寻求帮助。更详细的关于我们的个人信息保护措施，请参看保障数字权益—隐私保护的相关内容，以及《[儿童隐私保护声明](#)》。

腾讯未成年人家长服务平台小程序配备了专门的客服团队处理未成年人消费申诉，并聘请具有心理学资质的家庭教育专家，为家长提供有关未成年人正确使用网络和消费的专业指导意见。2024年，我们还新增了在线视频客户服务，进一步服务家长。

## 培养未来的科技创新人才

腾讯利用产品能力支持欠发达地区的科技教育，促进当地学生平等获取教育资源。

- 腾讯数字支教平台整合了腾讯文档、企业微信和腾讯会议等线上协作工具，结合专业支教机构提供的课程内容，供志愿者为偏远地区学生远程授课。截至2024年底，中国内地超过40%的专业支教公益机构及10万名志愿者已接入该平台。根据中国教育科学研究院的评测，接受数字支教的学生在阅读和语言表达等多项能力上均有显著提升。
- “智体双百”项目计划为低教育资源地区的学生建设100个教室和100个运动场，并配套科技和体育设备，以及相应的互动课程。截至2024年底，项目已建成48间教室和55个运动场，支持教师累计开展超4.3万课时的科学创新课程。



我们依托在游戏科技、人工智能和产品交互领域的技术积累，为儿童和青少年提供易用的编程及AI学习工具，促进科技教育普惠，激发他们的科技与创新潜能。

- 腾讯扣叮平台运用游戏技术，为6至18岁学生提供编程及人工智能学习内容。2024年，腾讯扣叮进一步推出了3D游戏化编程产品，配备了游戏3D素材和AIGC工具等，帮助教师高效制作3D数字交互课程，让学生快速学习创作3D作品。截至2024年底，腾讯扣叮已发布了超过10款编程产品和500节游戏化编程课程，覆盖超过1.9万所中小学，学生累计学习次数超过800万次。
- 腾讯AI创想家平台为青少年提供AI学习资源及竞赛项目。截至2024年底，已有超过40万青少年参与了该平台举办的系列竞赛项目。
- 基于微信小程序编程环境，我们打造了微信小程序教育平台。教师可利用该平台的教学模板和管理工具，指导学生结合多学科知识制作小程序，解决实际问题。学生也可通过

AI助手快速学习如何制作小程序。截至2024年底，小程序编程已被全中国上百所学校纳入教学计划；“微信创新实验室全球小程序编程创新挑战赛”已累计吸引了1,000多支全球学生队伍参赛。

- 2021年起，我们和中国儿童少年基金会合作开展了“春蕾科技女孩”项目，为女孩提供科技普惠课程和研究实践项目。截至2024年底，已有超过10,000名女孩参与相关活动。

我们每年联合顶尖科研机构、科学家和科技工作者，举办“腾讯科学WE大会”和“腾讯青少年科学小会”等科学知识分享会。此外，我们还与顶尖科学家合作，制作了“给孩子们的大师讲堂”系列视频，分享科技前沿发展，激发未成年人对科学技术的热情。

## 4.2

## 助力银发族享受数字时代

腾讯挖掘银发族的生活需求，借助科技创新，提供守护安全和健康的解决方案，让他们的生活更加安全和便捷。

### 助力银发族享受便捷和安全的数字生活

我们在微信、QQ、腾讯新闻、微信读书等多项产品中均设置了关怀模式，提供更大字体、更高色彩对比度、更大按钮，以及语音阅读文字等无障碍功能，帮助银发群体更轻松地使用产品。此外，我们还开发了银发青松助手小程序、银发守护助手小程序及《银发守护安全课》线上课程，助力银发族提升网络技能，安全使用互联网。

我们为银发族提供专属客服沟通渠道，帮助他们快速找到客服并描述、解决问题。微信支付“长辈无忧专线”支持多种方言的语音或视频客服，而微信小店简化了客服流程，银发族只需通过语音呼叫即可快速接入人工客服。

### 协助银发族克服体能障碍

我们为银发族开发了多种辅助科技，帮助他们更便捷地获取日常看护和医疗健康服务，享受更自主、舒适的生活。

#### 日常看护

我们与专业机构合作，探索银发族日常看护的辅助技术，进一步提升他们生活的安全性和便捷性。

- 隐形护理员系统能够识别银发族跌倒并主动发出警报，帮助家属和护理人员及时发现并应对。
- 银龄守护卡通讯设备在银发族授权后，可协助家属或养老机构了解其行踪，减少走失风险。

#### 医疗健康

数字化技术可以帮助银发族更方便地获取医疗健康服务，降低维护健康的成本。

- 微信推出“长辈就医”功能，为银发族提供就医全程引导和提醒。该功能覆盖挂号、就诊、支付、检查、报告领取及取药等环节，还支持一键授权诊疗卡，简化信息输入步骤。
- 根据世界卫生组织统计，每三位65岁以上长者中就有一位患听力损伤。腾讯天籁行动将腾讯会议的音频降噪和AI声纹增强技术应用于助听器，显著提升复杂场景下的语音清晰度。我们已技术授权厂商生产优质而实惠的助听器，并支持长者通过腾讯会议远程进行听力验配。我们还开发了银发听力健康小程序，提供普惠便捷的听力筛查服务。
- 我们与广州市和青岛市两地卫健部门合作，开发了数字化筛查工具，并将其应用于早期阿尔茨海默病普查。该项目在7个月内为超过4.1万名65岁以上的长者提供了初步认知评估，识别出超过1,800名高风险长者，帮助他们及早获得干预和治疗。

## 4.3

## 助力身体障碍人士跨越数字鸿沟

腾讯关注身体障碍人士的需求，积极探索无障碍技术及应用，响应联合国《残疾人权利公约》。

我们持续优化和创新无障碍产品与服务，已累计申请超过 90 项无障碍相关专利，涉及超过 40 项产品与功能，实现了主要产品的无障碍优化。此外，我们与中国残疾人联合会共同成立了“无障碍联合创新实验室”，助力建设无障碍环境。我们还开源语音合成、AI 手语翻译等多项无障碍技术专利，推动业界在信息无障碍领域的共同进步。

### 技术解决方案

#### 视障

- 搜狗输入法开发了基于触觉输入的振动反馈功能，帮助视障用户在触屏手机键盘输入时快速定位和识别字符，实现顺畅输入。
- 腾讯地图为视障用户提供步行导航偏移纠正和公交地铁导航震动提醒，还会实时语音提醒用户位置和朝向，帮助他们快速定位。
- 微信、腾讯新闻、微信读书等产品均支持语音阅读文字信息，帮助视障人士更便捷地获取信息并进行沟通交流。
- 腾讯视频基于AI技术制作无障碍影片，通过辅助讲解、自动配音和合成剪辑等功能，大幅提升了制作效率。截至2024年底，腾讯视频已上线193部无障碍影片，并免费向视障人士开放。
- 无障碍版的AI编程第一课已于2024年被纳入广州、北京、南京的特殊教育学校。视障学生可通过语音指令、旁白解说和触觉教具，学习AI和编程的基础知识。

#### 听障

- 通过技术授权，天籁行动项目助力厂商为听障人士制造高质量且实惠的助听器。同时，腾讯天籁远程听力服务平台支持听障人士通过腾讯会议完成远程听力验配，为听障人士提供便捷服务。
- 听障人士高频听力受损后往往仅对低频声音保有听觉，所听到的普通歌曲会断断续续。QQ音乐结合人工智能和音频技术，对音乐进行微调，通过精细化听损代偿，专门为中高频听力障碍人士开发了低频音乐库。

#### 肢障

- 搜狗输入法推出眼动输入解决方案，通过眼球追踪技术，帮助身体障碍用户借助眼球转动和凝视操作电脑进行文字输入。此外，搜狗输入法还提供声文互转、光学字符识别读图等技术解决方案，助力肢体障碍群体在数字世界中实现输入表达。
- 微信支付自2022年12月起发起了自立小店助力行动，为残疾人小商家提供免费无障碍经营工具，包括微信收款音箱、收纳推车和伸缩取物器等，并配套免费意外伤害保险、数字化经营培训，以及针对特定额度的提现费用免除。

## 4.4

## 数字技术助力农村地区发展

腾讯致力于帮助欠发达农村地区培养人才，提供数字化工具和金融科技服务，缩小数字鸿沟，并促进发展。

### 乡村数字化人才培养

我们聚焦乡村治理及乡村经营两大方向的人才培养，通过线上线下结合的培训形式，助力提升乡村治理水平和经济发展。

2021年，我们与农业农村部合作，启动了耕耘者振兴计划，免费为乡村治理人才提供政策、方法、工具及实践培训，目标是三年内完成线下10万人及线上100万人的培训任务。截至2024年底，线下课程累计开班1,245期，培训超11万人；线上学习平台吸引了超过183万人参与。

2021年，我们启动了乡村CEO培养计划，培养乡村经营人才应用现代化管理手段和数字化工具的能力，培训学员分布在云南、广西、浙江、广东等17个省的309个县。此外，我们还开发了共富乡村学堂——乡村经营人才学习交流平台，方便学员在平台上学习和交流乡村经营的理论与实践。截至2024年底，平台已累计服务超过7万名经营人才，其中参与培训的学员累计超过5万人。

### 数字化工具助力乡村经营能力提升

我们基于互联网和大数据能力，助力提升乡村服务和经营水平，并连接农产品生产者以及消费者，助力农产品销售。

我们在2021年开发了村级服务平台小程序，协助村干部和村民在线处理村庄的事务。截至2024年底，该小程序已经服务了7.9万个村庄的1,500多万村民。

我们在2022年推出村庄云服务，协助村庄开发小程序用于线上推广农村旅游资源、农产品及服务。用户可以通过小程序在线预订村庄的餐饮、住宿以及当地特色项目，如手工艺制作和研学等。截至2024年底，201个村庄使用这个数字化解决方案，助力村庄旅游以及农产品销售的收入增长。

视频号可以帮助乡村经营人才更便捷地推广乡村品牌形象，使农产品及乡村的旅游资源触达更多消费者。例如，我们的共富乡村视频号优质内容培养专项培养超过1,000名学员，提升其短视频制作和内容直播能力，促进农产品销售以及吸引消费者到乡村旅游消费。

我们探索将小程序用于增进农民与消费者的连接。通过云认养小程序，消费者不仅可以预定农产品，还可以在线观看农产品的生长过程。

### 金融科技应用提升农村普惠金融

我们通过在金融科技领域的创新，突破了传统金融机构服务网点的区域限制，增强了小型村镇银行的数字化能力，并协助建立县域农户的数字信用系统，实现了农户金融服务的在线授信和审批。

2024年，微信支付联合近30家地方性商业银行，正式推出数字惠农活动。该活动全面覆盖了从农牧产品丰收、批发销售、小微商户采购到加工销售的全产业链场景，旨在为农牧行业用户提供更加便捷和实惠的服务。例如，用户可以在与银行合作的商户中以优惠价格采购生产所需的物资，从而降低经营成本。这一举措不仅推动了农牧行业的数字化转型，也为农村经济的可持续发展注入了新动力，助力乡村振兴战略的深入实施。



# 数字技术助力 可持续发展目标

科技是一种能力，向善是一种选择。

数字技术的发展与应用正在重塑经济、社会与环境格局。腾讯与合作伙伴紧密协作，探索应对社会难题的创新解决方案，致力于创造可持续的社会价值和支持SDGs推进，践行科技向善的理念。

- 5.1 数字技术促进可持续创新
- 5.2 公益行业数字化升级
- 5.3 数字普惠金融
- 5.4 数字技术推动可持续城市发展
- 5.5 数字技术促进健康与福祉

## 联合国可持续发展目标一致性

