落实具有舆论属性或社会动员能力的互联网信息服务安全承诺书

致深圳市腾讯计算机系统有限公司（以下简称“腾讯公司”或“贵司”）：

本公司/本人（以下简称“我方”）在腾讯会议开放平台上的应用：XXX（应用名称，应用版本），根据《具有舆论属性和社会动员能力的评估规定》及《中华人民共和国网络安全法》相关规定。

以落实了以下要求：

一是我方已确定与所提供服务相适应的安全管理负责人（某某某）、信息审核人员（某某某）或者建立安全管理机构的情况；

二是我方已落实手机加短信验证/用户提供身份证号和姓名并通过全国公民身份证号码查询服务中心或授权机构核验/运用其他已确认真实身份的网络服务注册账号进行核验,对用户注册信息应当长期留存，留存项目包括但不限于源网络地址、端口号、时间、目的网络地址、端口号、URL、核验信息（身份证号和姓名或手机号、第三方网络账号）、账号、昵称、用户编码（ID）、客户端硬件特征。

三是我方对用户的账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征等日志信息，以及用户发布信息记录留存6个月以上。

四是我方已制订违法有害信息的防范处置制度，在服务功能中建立相应的技术措施；对用户账号和通讯群组名称、昵称、简介、备注、标识，信息发布、转发、评论和通讯群组等服务功能中违法有害信息，采取技术过滤和人工审核相结合的方法进行防范；新增违法有害信息屏蔽过滤策略在接公安机关等有关部门通知或者自行确认后10分钟内生效，并覆盖原有账号和通讯群组名称、昵称、简介、备注、标识和已发布信息，屏蔽过滤有效率达100%；开展违法有害信息的日常巡查；发现违法有害信息5分钟内处置并在后台保留原始记录。

五是我方已制订覆盖个人信息收集、存储、使用、流转、销毁、事件处置报告等各环节的保护制度并建立配套的技术措施。对个人信息的收集和使用限于提供服务所需，暂不存在采集非服务所需的个人信息；对公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经用户同意；对于客户个人信息如：身份证、手机、密码等重要信息应已使用XXX方式加密存储；采取防范计算机病毒和网络攻击、网络侵入等技术措施；禁止内部人员对个人信息的批量访问和获取，批量访问和获取限于系统迁移或者依法配合执法工作并须经两名以上管理层人员的系统授权；向第三方提供个人信息，应当经用户同意，经过处理无法识别特定个人且不能复原的除外。

六是我方已建立防范违法有害信息传播扩散、社会动员功能失控风险的应急处置预案和技术措施；每年至少进行一次应急处置演练；技术措施须至少具有下列防控风险的功能：封禁特定帐号、禁止新建帐号、禁止分享、禁止留言及回复、控制特定发布来源、控制特定地区或指定IP帐号登陆、禁止客户端推送、切断与第三方应用的互联互通等。

七是我方已建立用户投诉举报接收处理制度，明确用户投诉举报渠道、处理流程、

方式、时限，鼓励用户举报违法有害信息；对举报、投诉信息留存6个月以上。

八是我方已建立执法协助制度，明确协助流程、协助方案、协助时限、责任机构和责任人及联系方式。

对以上措施要求，我方郑重承诺遵守本承诺书的有关条款，如有违反本承诺书有关条款的行为，我方自愿自主下架，如我方未落实以上条款或落实不到位形成危害后果，将依法承担相应法律责任。

本承诺书自签署之日起施行。

责任单位/个人：

授权代表/个人：

年 月 日