短信接口信息安全保障责任书

为保障短信接口使用过程中的信息安全，维护公民、法人和其他组织的合法权益，规范短信服务相关行为，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《通信短信息服务管理规定》等相关法律法规，短信接口使用方（以下简称“经营者”）自愿承担以下信息安全保障责任，特签订本责任书。

一、经营者核心责任

（一）用户信息收集与使用责任

1. 严格按照“合法、正当、必要”原则收集短信接收方的个人信息（如手机号），确保收集行为获得用户明确同意（包括但不限于书面同意、线上勾选确认等可追溯形式），不得通过欺诈、胁迫、诱导等非法方式收集信息，且不得超范围收集与短信服务无关的信息（如用户身份证号、银行卡信息等非必要内容）。
2. 仅可将收集的用户信息用于约定的短信服务场景（如验证码发送、账户安全通知、业务办理提醒等），不得将信息转让、出租、出售给任何第三方，也不得用于其他未经用户明确同意的用途（如商业广告推送、第三方数据共享等）。
3. 建立用户信息台账，记录信息收集时间、用途、来源及使用情况，定期对信息进行清理，对不再需要的用户信息（如服务终止后），应在 15 个工作日内完成彻底删除，不得留存冗余信息。

（二）短信内容合规责任

1. 发送的短信内容必须符合国家法律法规及公序良俗，不得包含以下内容：
    1. 违反国家政治制度、损害国家利益的信息；
    2. 诈骗、赌博、色情、暴力、低俗等违法违规信息；
    3. 未经用户同意的商业广告、推销信息（即垃圾短信）；
    4. 虚假、误导性信息（如虚假中奖通知、虚假服务承诺等）。

1. 建立“双人审核”的短信内容审核机制，在发送短信前，由两名工作人员分别对内容进行独立审查，审核通过后方可发送；对批量发送的短信（单次发送量超过 100 条），需留存审核记录（包括审核人员、审核时间、审核意见），留存期限不少于 1 年。
2. 若因短信内容违法违规导致用户投诉、监管部门处罚（如罚款、停业整顿）或第三方索赔（如用户起诉），由经营者承担全部责任，包括但不限于支付罚款、赔偿损失、承担诉讼费用等。

（三）接口使用安全责任

1. 妥善保管短信接口的访问凭证（如 API 密钥、账号密码、IP 白名单权限），实行 “专人专管” 制度，明确凭证使用人及权限范围，不得将凭证告知无关人员或在非工作设备上使用。
2. 定期更换接口访问凭证（API 密钥、密码等），更换周期不超过 90 天；若发现凭证可能泄露（如设备丢失、账号异常登录），应立即采取以下措施：
    1. 1 小时内通知短信接口服务提供方，申请冻结接口使用权限；
    2. 24 小时内完成凭证重置，并更新内部授权记录；
    3. 排查泄露原因，形成书面报告，留存备查。
1. 不得擅自对短信接口进行修改、破解、反向工程，不得将接口转租、转借给第三方使用，不得超出约定场景（如仅用于内部通知却用于外部营销）使用接口；若需变更接口使用场景或范围，应提前向服务提供方提交书面申请，经同意后方可调整。

（四）安全事件应对责任

1. 建立短信接口信息安全应急预案，明确安全事件（如用户信息泄露、接口被非法调用、短信内容被篡改）的分级标准、响应流程及责任人，每年至少组织 1 次应急演练，并留存演练记录（包括演练方案、过程、总结报告）。
2. 若发生安全事件，应立即启动应急预案，并履行以下义务：
    1. 30 分钟内采取控制措施（如暂停接口使用、隔离受影响系统、阻断非法访问），防止事态扩大；
    2. 1 小时内将事件情况（包括事件类型、影响范围、已采取措施）书面通知服务提供方及相关监管部门（如当地网信办、通信管理局）；
    3. 24 小时内形成初步调查报告，后续每 3 个工作日向监管部门更新事件处理进展，直至事件完全解决；
    4. 对受影响的用户，应在 48 小时内通过电话、短信等方式告知事件情况及补救措施（如修改密码、更换手机号建议）。
1. 不得隐瞒、拖延报告安全事件，若因瞒报、迟报导致损失扩大（如用户信息进一步泄露），由经营者承担额外责任。

（五）内部管理责任

1. 制定《短信接口信息安全管理制度》，明确内部各部门（如技术部、运营部、客服部）的安全职责，将信息安全责任纳入员工岗位职责考核，对违反制度的员工，按公司规定予以处罚（如警告、罚款、调岗）。

2. 每年至少组织 1 次全员信息安全培训，培训内容包括：
    1. 相关法律法规（如《个人信息保护法》《通信短信息服务管理规定》）；
    2. 短信接口安全使用规范（如凭证保管、内容审核要求）；
    3. 安全事件识别与应对流程；
    4. 典型案例分析（如因违规使用接口被处罚的案例）。
1. 定期开展内部安全自查，自查频率为每季度 1 次，自查内容包括用户信息管理、短信内容审核、接口凭证保管等，对发现的安全隐患（如凭证未及时更换、审核记录不全），应在 7 个工作日内完成整改，并形成自查报告与整改记录，留存期限不少于 2 年。

二、责任期限与追究

（一）责任期限

本责任书自经营者签字（或盖章）之日起生效，有效期与经营者使用短信接口的服务期限一致；服务期限届满后，若经营者继续使用接口，本责任书自动延续；若经营者终止使用接口，对使用期间的信息安全责任，仍需承担追溯义务，追溯期限不少于 2 年。

（二）责任追究

1. 若经营者未履行本责任书约定的责任，导致以下后果之一的，需承担相应责任：
    1. 被监管部门处罚的，由经营者全额支付罚款，并承担由此导致的服务中断损失（如接口被暂停使用的业务损失）；
    2. 造成用户或第三方损失的，经营者需依法承担赔偿责任（包括直接损失与间接损失）；
    3. 情节严重的（如多次违规发送诈骗短信、造成大规模用户信息泄露），除承担上述责任外，还需接受服务提供方的永久终止合作处理，并承担相应的法律责任（如刑事责任）。
1. 若因不可抗力（如地震、洪水、战争等无法预见、无法避免的客观情况）导致经营者无法履行责任，经营者应在不可抗力发生后 24 小时内通知服务提供方及监管部门，提供相关证明材料，并在不可抗力结束后 7 个工作日内完成整改，恢复履行责任；不可抗力仅免除经营者因无法履行责任造成的直接损失赔偿责任，不免除整改义务。

三、其他条款

1. 本责任书是经营者使用短信接口的必备文件，经营者签字（或盖章）即视为认可本责任书全部内容，愿意接受本责任书约束。

2. 本责任书未尽事宜，按照国家相关法律法规及短信接口服务协议执行；若本责任书内容与服务协议不一致，以本责任书为准。

3. 若经营者对本责任书内容有异议，应在签字（或盖章）前向服务提供方提出，协商修改；签字（或盖章）后，视为无异议。

4. 本责任书一式两份，经营者执一份，短信接口服务提供方执一份，具有同等法律效力。

特殊情况说明

□ 个体工商户无公章，由法人手印代替（勾选此框后，法人手印与公章具有同等法律效力）

经营者（盖章 / 签字 / 按手印）：_____

法定代表人 / 授权代表（签字 / 按手印）：_____

日期：_____年_____月_____日