|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **网络与信息安全保障措施** | | | | |
| **网络与信息安全责任人** | **姓名** | XXX | **联系方式（手机号）** | 1xxxxxxxxxx |
| ☑我公司承诺如网络与信息安全责任人或联系方式发生变化，至少提前3个工作日提交变更信息。 | | | |
| **网络与信息安全管理组织机构设置及工作职责** | **我公司承诺在从事电信业务经营活动中，严格履行国家要求的网络与信息安全责任，将遵守如下承诺：**  ☑建立网络与信息安全主管部门，负责本企业网络与信息安全相关工作。明确网络数据安全管理责任部门和责任人。  ☑根据国家和行业有关网络与信息安全的政策、法律和法规，批准公司网络与信息安全总体策略规划、管理规范和技术标准；确定公司网络与信息安全各有关部门工作职责，指导、监督网络与信息安全工作。  ☑建立本企业全流程网络数据安全管理制度体系，建立内部数据资产清单和数据分级分类管理制度、用户信息保护制度，配套数据安全技术保障措施，开展内部权限管理和安全审计。  ☑建立健全从业人员网络与信息安全教育培训，制定网络与信息安全工作考核及奖惩机制等内容。  ☑建立健全违法有害信息监测处置制度并加强技术手段建设，严格落实违法违规信息发现处置机制，阻断违法违规信息的发布与传输。  ☑建立新技术新业务安全评估管理制度，固化安全评估工作流程，有效排查安全隐患，及时落实整改工作。  ☑定期开展网络与信息安全风险监测预警和评估控制、隐患排查整改工作，审定公司网站与信息系统的安全应急策略及应急预案。  ☑建立健全网络与信息安全事件应急处置和上报制度，以及组织开展应急演练。  ☑建立健全防范打击通讯信息诈骗相关工作内部管理机制、责任体系和技术保障措施，完善举报通报处置流程。  ☑建立健全网络安全防护工作的内部管理制度和操作规程，确定网络安全负责人，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技术措施，监测、记录网络运行状态、网络安全事件的措施，以及重要数据的备份和加密措施。  ☑明确网络安全威胁监测与处置工作的责任部门、责任人和联系人，加强相关技术手段建设，按电信主管部门要求对网络安全威胁采取处置措施，反馈处置结果。  ☑按照国家相关法律规定和政策要求，建立健全电话用户实名制登记管理制度，完善技术措施，严格落实电话用户实名登记各项要求，加大用户身份信息核查，如实登记用户身份信息，加强销售渠道管理，依法保护电话用户登记信息 | | | |
| **网络与信息安全管理人员配备情况及相应资质** | **我公司承诺在从事电信业务经营活动中，严格履行国家要求的网络与信息安全责任，配备相应的网络与信息安全管理人员，并履行如下工作职责：**  ☑制定完善网络与信息安全制度和监督执行。  ☑负责网络与信息安全事件应急处置和上报。  ☑组织网络与信息安全人员教育培训。  ☑落实网络安全防护措施，定期开展网络单元的定级备案、符合性评测、安全风险评估，及时整改自查和检查中发现的重大网络安全隐患。  ☑开展网络安全威胁监测与处置  ☑落实用户信息保护工作。  ☑开展违法有害信息监测处置。  ☑落实防范打击通讯信息诈骗相关工作。  ☑落实网络数据安全管理，定期开展数据安全风险自查。  ☑按照互联网新技术新业务安全评估相关规定或文件要求，开展业务安全评估，完善业务安全风险管控措施。  ☑严格落实电话用户实名登记制度，加强电话用户实名登记管理等。 | | | |
| **网络与信息安全责任**  **承诺** | **我公司在取得经营许可证以后，在从事电信业务经营活动中，严格履行国家要求的网络与信息安全责任，将遵守如下承诺： 1、建立信息安全管理制度，包括信息安全管理责任制、信息安全评估、用户信息安全管理、违法违规互联网信息服务和违法信息的巡查与处置、重大信息安全事件应急处置和报告制度、信息安全教育培训、用户举报和投诉处理等制度。 2、制定并落实网络与信息安全管理责任制，通过文件形式明确企业网络与信息安全主管部门工作职责、企业其他部门的网络与信息安全工作职责、网络与信息安全工作考核及奖惩机制等内容。工作职责至少包括制定网络与信息安全年度工作计划、制定网络与信息安全相关工作制度、负责网络与信息安全事件的响应/处置/协调、负责网络与信息安全教育培训及应急演练等。 3、严格落实违法违规信息发现处置机制，阻断违法违规信息发布，对于已发布的违法违规信息应当立即停止传输，保存有关记录，并向国家有关机关报告。 4、严格落实违法违规信息投诉受理处置机制，设立网络、电话、邮件等多种违法违规信息投诉渠道，对于举报的违法违规信息进行及时核实并处置。 5、严格落实重大信息安全事件应急处置和报告制度，对于涉及业务相关数据安全、涉及国家网络信息安全的重大事件进行紧急处置，并向主管部门上报。 6、定期开展信息安全相关法律法规及安全政策文件、配合政府监管机制、信息安全保障制度、信息安全技术手段等方面培训，培养员工信息安全意识，提高员工信息安全工作能力。 7、按照相关法律法规及行业主管部门要求建立违法违规信息发现和过滤技术手段，能对违法违规信息进行隔离、过滤处置。 8、按照相关法律法规及行业主管部门要求建设用户日志留存系统，留存规定的日志信息，留存时间满足法律规定要求。 9、制定网络安全防护管理制度，明确并落实网络安全“三同步”、定级备案、符合性评测和风险评估等要求。 10、制定并落实网络安全事件应急预案和网络安全事件应急处置报告制度，明确网络安全事件应急处置机制、网络安全事件上报和网络安全应急演练等要求。 11、按照通信网络安全防护相关标准配套落实网络安全防护技术手段，至少应涉及业务及应用安全、网络安全、设备及软件系统安全和物理安全等相关技术手段。** **12、网络与信息安全联络员或联络方式变动时，在两个工作日内主动向申请机关报备。**    **●承诺**  **🌕不承诺** | | | |
| **法定代表人签字：**  **（公司盖章）**  **日期：** | | | | |
| **填表说明：**  一、网络与信息安全管理组织机构设置及工作职责  1、网络与信息安全责任人：  网络与信息安全第一责任人：企业法定代表人姓名；  工作职责为：对机构内的信息安全工作负有领导责任；  网络与信息安全责任人：分管信息安全工作的负责人姓名；  工作职责为：对企业内信息安全工作负有直接领导责任。  （上述两项请全部填写）  2、网络与信息安全管理组织机构设置及工作职责  企业需设置或指定网络与信息安全主管部门（如信息安全领导小组、信息安全工作组、信息安全部等），负责本企业网络与信息安全相关工作；  企业网络与信息安全管理组织架构：包括主管部门、配合部门，  网络与信息安全管理机构职责（包括但不限于下述内容）：  （1）建立健全网络与信息安全规章制度，以及各项规章制度执行情况监督检查；  （2）开展网络与信息安全风险监测预警和评估控制、隐患排查整改工作；  （3）建立健全网络与信息安全事件应急处置和上报制度，以及组织开展应急演练；  （4）建立健全从业人员网络与信息安全教育培训以及考核制度；  （5）违法有害信息监测处置制度和技术手段建设（如申请信息服务业务，此项必须体现）；  （6）建立健全用户信息保护制度。  二、网络与信息安全管理人员配备情况及相应资质  至少应包括：  1、人员名单：人员姓名、联系方式；  2、归属部门：信息安全部、网络安全部、运维部等；  3、工作内容（包括但不限于下述内容）：  （1）网络与信息安全制度制定和执行检查；  （2）网络与信息安全事件应急处置和上报；  （3）网络与信息安全人员教育培训工作落实；  （4）违法有害信息监测处置（如申请信息服务业务，此项必须体现）；  （5）开展网络安全防护工作，如定期开展病毒检测和网络安全漏洞检测等；  （6）用户信息保护工作落实等；  4、全职或兼职：全职/兼职  5、资质情况等：是否取得CISP、CISSP、CISA等资质以及等级保护测评机构测评师。  企业所列人员必须包括“信息安全”与“网络安全”两方面相关责任人员（可兼任）。 | | | | |