附件一

山西省电信业务经营者网络安全防护管理自查报告

一、基本信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 单位名称 | （公章） | | 单位住所 |  |
| 联系人 |  | | 联系电话 |  |
| 业务种类1 |  | | 许可证号1 |  |
| 业务种类2 |  | | 许可证号2 |  |
| ... |  | | ... |  |
| 网络单元类型 |  | | 网络单元名称 |  |
| 定级级别 |  | | 定级时间 |  |
| 主要硬件使用情况 |  | | | |
| 基础软件使用情况 |  | | | |
| 应用软件情况 |  | | | |
| 通信协议 |  | | | |
| 接入商/接入地 |  | | | |
| 公网IP/端口 | IPv4 |  | | |
| IPv6 |  | | |
| 定级备案网址 | https://mii-aqfh.cn/ | | | |

注：业务种类需为增值电信业务经营许可证表明业务种类，包括：国内呼叫中心业务，信息服务业务（不含互联网信息服务），信息服务业务，互联网数据中心业务，信息服务业务（仅限互联网信息服务），互联网接入服务业务，互联网数据中心业务（含互联网资源协作），国内互联网虚拟专用网业务，互联网数据中心业务（不含互联网资源协作），在线数据处理与交易处理业务，网约车，车联网等。

二、自查对照表（符合性评测表）

|  |  |  |  |
| --- | --- | --- | --- |
| 自查类别 | 自查子项 | 选项 | 说明（必填） |
| 日常工作 | 1.是否建立网络安全管理制度 | □是 | （请在网络安全防护管理报告第3.1节说明） |
| □否 |
| □不适用 |
| 2.是否建立信息安全管理制度 | □有 | （请在网络安全防护管理报告第3.1节说明） |
| □无 |
| □不适用 |
| 3.是否开展网络与信息安全教育培训 | □是 | （请在网络安全防护管理报告第4章说明） |
| □否 |
| □不适用 |
| 4.是否开展网络安全应急演练 | □是 | （请在网络安全防护管理报告第5章说明） |
| □否 |
| □不适用 |
| 网络安全防护管理 | 1.是否配备专业网络安全设备 | □是 | （请列出网络安全设备、数量） |
| □否 |  |
| □不适用 |  |
| 2.是否定期开展网络安全巡检 | □是 | （请在网络安全防护管理报告第3.2.1节说明） |
| □否 |  |
| □不适用 |  |
| 3.是否委托专业机构开展网络安全日常巡检 | □是 | （请在网络安全防护管理报告第3.2.1节说明） |
| □否 |  |
| □不适用 |  |
| 4.是否进行第三方风险评估 | □是 | （请注明评估时间及评估机构） |
| □否 |  |
| □不适用 |  |
| 5.是否进行等级保护测评 | □是 | （请注明评估间隔及评估机构） |
| □否 |  |
| □不适用 |  |
| 信息安全管理 | 1.本单位开展业务是否涉及用户个人信息 | □是 | （请在网络安全防护管理报告第3.3.1节说明） |
| □否 |  |
| □不适用 |  |
| 2.是否对外提供用户个人信息 | □是 | （请在网络安全防护管理报告第3.3.1节说明） |
| □否 |  |
| □不适用 |  |
| 3.是否按照要求与通信管理局信安系统对接 | □是 |  |
| □否 |  |
| □不适用 |  |
| 4.是否定期开展信息安全巡查 | □是 | （请在网络安全防护管理报告第3.3.3节说明） |
| □否 |  |
| □不适用 |  |

注：1.自查表需对“是”“否”“不适用”做详细说明； 2.“第三方风险评估”须为获得中国通信企业协会“网络安全风险评估”通信网络安全服务能力评定证书第三方机构。

填表人： 联系电话： 填表时间： 年 月 日

XX公司

20XX年网络安全防护管理报告

（半年报/年报）

XX公司（公章）

20XX年XX月XX日

**目 录**

[一、企业基本介绍 18](#_Toc2287)

[二、系统介绍 18](#_Toc20658)

[2.1系统功能 18](#_Toc17779)

[2.2系统网络架构 18](#_Toc323)

[三、系统安全防护管理介绍 18](#_Toc17675)

[3.1日常网络与信息安全管理 18](#_Toc956)

[3.2网络安全防护能力建设 18](#_Toc6786)

[3.2.1日常网络安全巡检 18](#_Toc19153)

[3.2.2已有网络安全防护能力 18](#_Toc21610)

[3.2.3计划建设 18](#_Toc16063)

[3.3信息安全 19](#_Toc9813)

[3.3.1用户个人信息日常管理 19](#_Toc2052)

[3.3.2用户个人信息保护情况 19](#_Toc13591)

[3.3.3信息安全巡查 19](#_Toc9518)

[四、网络安全应急演练 19](#_Toc26086)

[五、网络与信息安全教育培训 19](#_Toc19448)

[六、申请电信业务许可时网络与信息安全相关材料 19](#_Toc20359)

[七、其他报告内容 19](#_Toc22584)

一、企业基本介绍

简要介绍本企业主营业务，系统在该业务中的角色/功能，组织架构，网络与信息安全责任管理部门。

二、系统介绍

2.1系统功能

简要说明系统主要功能、覆盖范围、用户规模。

2.2系统网络架构

说明系统网络架构、系统部署位置、IP及端口使用情况等。

三、系统安全防护管理介绍

3.1日常网络与信息安全管理

提供相关网络与信息安全管理制度、人员配备、安全员及联系方式。

如未建立相关制度，请说明原因及制度建立计划。

如不适用该企业，请详细说明原因。

3.2网络安全防护能力建设

3.2.1日常网络安全巡检

提供巡检时间间隔、发现问题、整改情况。如委托第三方开展日常网络安全巡检工作，须说明委托第三方名称、资质等信息。

3.2.2已有网络安全防护能力

说明：（1）系统已有网络安全防护能力（如网页防篡改、IDS、IPS、抗DDoS等，含购买第三方服务）；（2）自有专业网络安全设备类型、数量。

3.2.3计划建设

如有网络安全防护能力建设/升级改造计划，请简要说明建设/升级改造类型、规模等。

3.3信息安全

3.3.1用户个人信息日常管理

本企业开展业务是否涉及用户个人信息采集、存储、使用等。

3.3.2用户个人信息保护情况

说明本企业在用户个人信息保护方面所开展的工作。

3.3.3信息安全巡查

提供巡检时间间隔、发现问题、整改情况。如委托第三方开展日常信息安全巡检工作，须说明委托第三方名称、资质等信息。

四、网络安全应急演练

说明应急演练次数，单独说明每次应急演练项目、时间、参加人员、形式（桌面推演/实操等）、支撑单位等。

如暂未开展应急演练，提供计划开展项目、时间、参加人员、形式（桌面推演/实操等）、支撑单位等。

五、网络与信息安全教育培训

说明教育培训次数，单独说明每次教育培训主题、时间、参加人员、形式（线上/线下等）、支撑单位。

如暂未开展教育培训，提供计划开展主题、时间、参加人员、形式（线上/线下等）、支撑单位等。

六、申请电信业务许可时网络与信息安全相关材料

七、其他报告内容

企业认为需要报告的相关内容或意见建议。