附件 1

博乐市公安局

网络安全监督检查通知书

博公网安 检字[ ] 号

被检查单位名称_____

检查时间_____

检查地点 _____

检查单位 _____

承 办 人_____

批 准 人_____

检查人员_____

填发日期_____

存根

博乐市公安局
网络安全监督检查通知书

博公网安 检字[　　]　　号

_____：

根据《网络安全法》和《计算机信息系统安全保护条例》规定，我单位决定于____年__月__日至___年__月__日对你单位网络安全工作进行监督检查。具体包括下列事项：

□ 1. 《网络安全法》《密码法》《计算机信息系统安全保护条例》等法律法规和网络安全责任制落实情况；

□ 2. 网络安全领导机构、专门管理部门和人员配备情况；

□ 3. 网络安全总体规划和实施情况，网络安全综合防控体系建设情况；

□ 4. 部署落实网络安全等级保护制度情况；

□ 5. 关键信息基础设施安全保护工作开展情况；

□ 6. 行业标准规范、部门规范性文件制定和应用情况；

□ 7. 网络安全监测、通报预警机制建设和工作情况；

□ 8. 网络安全应急预案制定和演练情况；

□ 9. 重要数据和公民个人信息保护情况；

□ 10. 网络安全保护类平台、技术装备等建设和应用情况；

□ 11. 网络安全“实战化、常态化、体系化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”三化六防措施落实情况；

□ 12. 针对演习、等级测评、风险评估、网络安全案件发现重大风险隐患和问题的整改情况；网络安全责任追究情况；

□ 13. 针对云计算、物联网、工控系统、移动互联、大数据、智能制造等新技术新应用的安全管控情况；

□ 14. 重大网络安全事件报告和处置情况；威胁情报工作开展情况；

□ 15. 自主可控和国产化替代、网络安全审查情况；

□ 16. 国产密码应用情况；

□ 17. 国家重大活动网络安保工作部署和开展情况；

□ 18. 网络安全保障情况；

□ 19. 领导和网络安全岗位人员教育训练情况；

□ 20. 其他网络安全保护工作情况。

请你单位分管网络安全工作的负责同志及有关人员届时参加并做好准备工作。

联系人：　　联系电话：

博乐市公安局

年　月　日

一式两份，一份交被通知单位，一份附卷。

附件 2

博乐市公安局

网络安全监督检查记录

博公网安 检字[ ] 号

检查民警（签名）_____

被检查单位（部门）名称_____

_____

检查时间_____年 月 日_____

检查地点_____

被检查单位网络安全负责人_____

联系电话 _____

被检查单位网络安全联系人_____

联系电话 _____

记录人（签名）: _____

被检查单位人员（签名）: _____

被检查单位人员（签名）_____

此记录由公安机关存档。

网络安全监督检查记录单

检查内容	检查结果 （如否说明情况）
一、网络安全工作开展情况	
1-1 是否成立网络安全领导小组（办公室）	□是 □否
1-2 是否由本单位主要领导同志担任小组负责人	□是 □否
1-3 是否成立网络安全专门管理机构，并配备专人开展网络安全工作	□是 □否
1-4 网络安全机构负责人和关键岗位人员是否进行背景审查	□是 □否
1-5 是否制定本行业、本单位网络安全工作规划和实施方案	□是 □否
1-6 是否制定网络安全考核评价制度	□是 □否
1-7 是否制定网络安全责任追究制度	□是 □否
1-8 是否制定网络安全事件报告和处置制度	□是 □否
1-9 是否制定教育训练制度	□是 □否
1-10 是否建立网络安全经费保障机制	□是 □否
1-11 本年度是否发生重大网络安全案（事）件	□是 □否
二、网络安全等级保护工作开展情况	
2-1 是否制定出台本行业、本单位网络安全等级保护政策文件	□是 □否
2-2 是否组织和部署全行业开展网络安全等级保护工作情况	□是 □否
2-3 是否依据有关法律法规和标准规范，制定网络安全等级保护行业标准规范	□是 □否
2-4 新建及在建网络是否及时进行定级、并及时向公安机关备案	□是 □否
2-5 新建及在建网络是否同步规划、同步建设、同步运行网络安全保护措施	□是 □否
2-6 第三级以上网络是否按要求每年开展一次网络安全等级测评工作	□是 □否
2-7 是否按照有关规定的条件选择等级测评机构	□是 □否
2-8 根据等级测评发现的问题，是否制定网络安全建设整改方案并开展整改工作	□是 □否
2-9 是否组织本行业、本单位对网络安全等级保护工作开展自查	□是 □否
三、关键信息基础设施保护工作开展情况	
3-1 是否制定出台本行业、本单位关键信息基础设施保护工作政策文件，并组织、部署全行业开展关键信息基础设施保护工作	□是 □否
3-2 是否依据有关法律法规和标准规范，制定关键信息基础设施保护行业标准规范	□是 □否
3-3 是否制定本行业、本单位关键信息基础设施认定规则	□是 □否
3-4 新建及在建网络是否按认定规则及时认定为关键信息基础设施	□是 □否
3-5 关键信息基础设施认定及变更情况，是否及时向公安机关进行备案	□是 □否
3-6 关键信息基础设施是否同步规划、同步建设、同步运行安全保护措施	□是 □否
3-7 关键信息基础设施是否按要求开展年度检测评估	□是 □否
3-8 是否按要求选择符合条件的测评机构	□是 □否
3-9 根据检测评估发现的问题，是否制定安全建设整改方案并开展整改工作	□是 □否
3-10 是否组织本行业、本单位对关键信息基础设施安全保护工作开展自查	□是 □否
四、网络安全保护平台建设使用情况	
4-1 是否建设网络安全保护类平台	□是 □否
4-2 网络安全保护类平台是否包含实时监测、通报预警、事件处置、威胁情报、态势感知、指挥	□是 □否

调度等基本功能	
4-3 网络安全保护类平台与全行业上下级是否联通	□是 □否
4-4 网络安全保护类平台是否与本地公安网安部门网络安全保卫平台进行对接	□是 □否
4-5 网络安全保护类平台是否开展过网络安全保护、事件处置、重大活动安保、数据共享等工作	□是 □否
五、网络与信息安全信息通报机制建设和工作情况	
5-1 是否加入国家（地方）网络与信息安全信息通报机制	□是 □否
5-2 本行业、本单位是否建立网络与信息安全信息通报机制	□是 □否
5-3 是否能响应本级（国家、地方）网络与信息安全信息通报中心通报预警	□是 □否
5-4 是否组织本行业、本单位开展网络安全监测、通报预警、应急处置工作	□是 □否
六、重大案事件处置情况	
6-1 是否制定网络安全事件应急处置预案	□是 □否
6-2 是否定期开展应急演练或实战演练	□是 □否
6-3 重大网络安全案（事）件是否及时报告公安机关	□是 □否
6-4 重大网络安全案（事）件是否及时处置和整改	□是 □否
七、网络安全产品选择和使用情况	
7-1 采购使用的网络安全产品是否获得计算机信息系统安全专用产品销售许可证	□是 □否
7-2 第三级（含）以上网络是否使用外国品牌的网络安全产品	□是 □否
7-3 是否采购网络安全运维、检测、监测和应急处置等服务	□是 □否
情况说明	

此记录由公安机关存档。

博乐市公安局

年 月 日

被检查单位主管人员（签名）_____

附件 3

博乐市公安局

网络安全监督检查限期整改通知书

博公网安 限字[　　]第　　号

_____:

根据《网络安全法》和《计算机信息系统安全保护条例》，我单位民警_____于_____年___月___日对你单位网络安全保护工作进行了监督检查，发现存在下列违规行为：

1.

根据_____,请你单位于_____年___月__日前改正，并在期限届满前将整改情况函告我单位。

在期限届满之前，你单位应当采取必要的安全保护管理和技术措施，确保网络安全。

（公安机关印章）

年　月　日

一式两份，一份交被检查单位，一份附卷。

附件 4

博乐市公安局
网络安全监督检查情况通报书

博公网安 通字[　　] 第　　号

被通报单位名称_____

通报事由_____

_____

_____

_____

办理单位：_____

承 办 人：_____

批 准 人：_____

填发日期：_____

存根

博乐市公安局
网络安全监督检查情况通报书

博公网安 通字[　] 第　　号

_____：

根据《网络安全法》和《计算机信息系统安全保护条例》，我单位民警_____于_____年___月___日对_____网络安全工作进行了监督检查，发现存在违规行为并发出《网络安全限期整改通知书》（博公网安 限字[　　]第　　号）。但在整改期限结束后，未收到整改结果报告，我单位于_____年____月____日对其做出了警告处罚。

鉴于你单位为其上级主管部门，建议你单位督促其按照《网络安全限期整改通知书》的要求开展整改工作，并及时反馈结果。

特此通报。

博乐市公安局

年　　月　　日

一式两份，一份交被检查单位，一份附卷。

附件 5

2022 年公安机关网络安全监督检查自查表

表一：行业主管部门填写

<table>
<tr><td colspan="8">一、行业主管部门基本情况</td></tr>
<tr><td>行业主管部门名称</td><td colspan="7"></td></tr>
<tr><td>单位地址</td><td colspan="7"></td></tr>
<tr><td>网络安全分管领导</td><td>姓名</td><td colspan="2"></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>网络安全责任部门</td><td colspan="7"></td></tr>
<tr><td rowspan="2">责任部门负责人</td><td>姓　　名</td><td colspan="2"></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>办公电话</td><td colspan="2"></td><td>移动电话</td><td colspan="3"></td></tr>
<tr><td rowspan="3">责任部门联系人</td><td>姓　　名</td><td colspan="2"></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>办公电话</td><td colspan="2"></td><td>移动电话</td><td colspan="3"></td></tr>
<tr><td>传　真</td><td colspan="2"></td><td>邮箱地址</td><td colspan="3"></td></tr>
<tr><td rowspan="2">全行业网络（包括基础网络、信息系统、大数据）总数</td><td rowspan="2"></td><td>第四级网络数</td><td></td><td>第三级网络数</td><td colspan="2"></td></tr>
<tr><td>第二级网络数</td><td></td><td>未定级网络数</td><td colspan="2"></td></tr>
<tr><td rowspan="2">全行业网络等级测评总数</td><td rowspan="2"></td><td>第四级网络数</td><td></td><td>第三级网络数</td><td colspan="2"></td></tr>
<tr><td>第二级网络数</td><td></td><td>未测评网络数</td><td colspan="2"></td></tr>
<tr><td rowspan="2">全行业网络安全建设整改总数</td><td rowspan="2"></td><td>第四级网络数</td><td></td><td>第三级网络数</td><td colspan="2"></td></tr>
<tr><td>第二级网络数</td><td></td><td>未整改网络数</td><td colspan="2"></td></tr>
<tr><td rowspan="2">本级单位网络总数</td><td rowspan="2"></td><td>第四级网络数</td><td></td><td>第三级网络数</td><td colspan="2"></td></tr>
<tr><td>第二级网络数</td><td></td><td>未整改网络数</td><td colspan="2"></td></tr>
</table>

二、行业主管部门网络安全工作情况
1、行业网络安全工作的组织领导情况
（重点包括：行业网络安全领导机构成立情况；行业网络安全职责部门和具体职能情况；全行业网络安全工作部署情况等。）
2、行业网络安全等级保护工作保障情况
（重点包括：行业网络安全等级保护工作年度考核情况；行业主管部门组织对地方对口部门或所属企事业单位网络安全检查情况；行业网络安全工作经费是否纳入年度预算？行业网络安全工作的经费约占行业信息化建设经费的百分比情况等。）
3、行业关键信息基础设施保护工作开展情况
（重点包括：行业制定出台关键信息基础设施保护行业标准规范情况；行业关键信息基础设施认定规则制定情况；关键信息基础设施发生重大威胁报告情况，安全事件、案件发生、处置及整改情况；关键信息基础设施安全保护的保障机制建立和落实情况；对本行业关键信息基础设施安全保护工作开展自查情况。）
4、行业网络安全责任追究制度执行情况
（重点包括：是否建立了行业网络安全责任追究制度？是否依据责任追究制度对行业发生的网络安全事件（事故）进行追责等情况。）

5、行业网络安全与信息通报工作情况
（重点包括：是否加入了国家网络与信息安全通报机制？是否建立了本行业网络与信息安全通报机制？行业组织开展日常网络安全监测情况；本行业开展网络与信息安全通报预警工作的总体情况等。）
6、行业重要网络安全政策和技术标准的制定情况
（重点包括：行业出台网络安全或等级保护政策、管理办法、管理规定等规范性文件情况，具体文件名字和出台时间；行业出台网络安全或等级保护标准规范情况，具体文件名字和出台时间等情况。）
7、行业网络安全顶层设计和统筹规划情况
（重点包括：行业网络安全顶层设计情况；行业网络安全工作的短期目标和长远规划制定情况；全行业的网络安全保护策略制定情况等。）
8、行业大数据、重要敏感信息和公民个人信息保护情况
（重点包括：行业数据中心建设情况；行业数据资源存储情况；行业数据资源安全保护情况；行业数据资源的灾备中心建设情况和数据备份恢复情况，行业数据资源存储和应用是否由社会第三方提供？提供服务单位的具体情况等）

9、行业网络安全应急预案和演练情况
（重点包括：是否制定了行业网络安全预案？行业网络安全预案是否进行了演练？是否根据演练情况对预案进行了修改完善等情况）
10、行业网络安全应急队伍建设情况
（重点包括：是否建立了本行业网络安全应急队伍？是否组建了行业网络安全专家队伍？是否与社会企业签订了应急支持协议？行业应急队伍建设规划等情况。）
11、行业网络安全事件（事故）的处置情况
（重点包括：是否明确了行业网络安全事件（事故）发现、报告和处置流程？年内是否发生重大网络安全事件（事故）？是否与相关部门建立了网络安全应急处置机制等情况。）
12、网络安全保护平台建设使用情况
（重点包括：网络安全保护类平台是否包含实时监测、通报预警、事件处置、威胁情报、态势感知、指挥调度等基本功能，是否满足网络安全保护和工作需要；行业网络安全保护类平台上下级联通情况，与本地公安网安部门网络安全保卫平台对接情况；利用平台联合开展网络安全保护、事件处置、重大活动安保、数据共享等情况。）

13、行业网络安全宣传培训情况
（重点包括：行业组织开展网络安全宣传教育情况；行业组织开展网络安全领导干部培训、业务骨干培训和网络安全员培训等情况。）
14、行业新技术、新应用安全保护情况
（重点包括：行业大数据、云计算、物联网、工业控制系统等应用情况；是否开展等级保护工作情况；新技术、新应用网络安全保护等情况。）
15、网络安全产品选择和使用情况
（重点包括：采购使用网络安全产品是否获得计算机信息系统安全专用产品销售许可证；第三级（含）以上网络使用外国品牌的网络安全产品情况。）

表二：网络运营者填写

<table>
<tr><td colspan="7">一、网络运营者基本情况</td></tr>
<tr><td>单位名称</td><td colspan="6"></td></tr>
<tr><td>单位地址</td><td colspan="6"></td></tr>
<tr><td>网络安全分管领导</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>网络安全责任部门</td><td colspan="6"></td></tr>
<tr><td rowspan="2">责任部门负责人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>办公电话</td><td></td><td>移动电话</td><td colspan="3"></td></tr>
<tr><td rowspan="2">责任部门联系人</td><td>姓名</td><td></td><td>职务/职称</td><td colspan="3"></td></tr>
<tr><td>办公电话</td><td></td><td>移动电话</td><td colspan="3"></td></tr>
<tr><td rowspan="2">单位网络（包括基础网络、信息系统、大数据）总数</td><td rowspan="2"></td><td>第四级网络数</td><td></td><td>第三级网络数</td><td></td></tr>
<tr><td>第二级网络数</td><td></td><td>未定级网络数</td><td></td></tr>
<tr><td rowspan="2">单位网络等级测评总数</td><td rowspan="2"></td><td>第四级网络数</td><td></td><td>第三级网络数</td><td></td></tr>
<tr><td>第二级网络数</td><td></td><td>未测评网络数</td><td></td></tr>
<tr><td rowspan="2">单位网络安全建设整改总数</td><td rowspan="2"></td><td>第四级网络数</td><td></td><td>第三级网络数</td><td></td></tr>
<tr><td>第二级网络数</td><td></td><td>未整改网络数</td><td></td></tr>
<tr><td rowspan="2">单位网络安全自查总数</td><td rowspan="2"></td><td>第四级网络数</td><td></td><td>第三级网络数</td><td></td></tr>
<tr><td>第二级网络数</td><td></td><td>未自查网络数</td><td></td></tr>
</table>

二、网络运营者网络安全工作情况
1、单位网络安全工作组织领导情况
（重点包括：单位网络安全领导机构成立情况；单位网络安全职责部门和具体职能情况；单位网络安全工作部署情况等。）
2、单位对网络安全等级保护工作的保障情况
（重点包括：单位网络安全等级保护工作年度考核情况；单位组织开展网络安全自查情况；单位网络安全工作经费是否纳入年度预算？单位网络安全工作的经费约占单位信息化建设经费的百分比情况；单位网络定级、备案情况；针对单位网络开展恶意代码扫描、渗透性测试、等级测评和风险评估等安全检测情况；根据等级测评发现的问题，制定网络安全建设整改方案并开展整改工作情况等。）
3、关键信息基础设施保护工作开展情况
（重点包括：按照本行业制定的关键信息基础设施认定规则，认定关键信息基础设施及备案情况；关键信息基础设施按要求开展年度检测评估情况；根据检测评估发现的问题，制定安全建设整改方案并开展整改工作情况；组织对关键信息基础设施安全保护工作开展自查情况；关键信息基础设施发生重大威胁报告情况，安全事件、案件发生、处置及整改情况；关键信息基础设施安全保护的保障机制建立和落实情况等。）
4、单位网络安全责任追究制度执行情况
（重点包括：是否建立了单位网络安全责任追究制度？是否依据责任追究制度对单位发生的网络安全事件（事故）进行追责等情况。）

5、单位网络安全管理制度的制定和实施情况
（重点包括：单位网络建设和网络安全“同步规划、同步建设、同步运行”措施的落实情况；单位人员管理，机房管理、设备管理、介质管理、网络安全建设管理、运维管理、服务外包等管理制度的建设情况；管理制度的监督保障和运行情况等。）
6、单位重要数据的保护情况
（重点包括：单位数据中心建设情况；单位重要数据存储和安全保护情况；单位重要数据备份恢复情况，单位重要数据存储和应用是否由社会第三方提供？提供服务单位的具体情况等）
7、单位网络安全监测预警情况
（重点包括：单位开展日常网络安全监测情况；单位网络安全监测技术手段建设情况；单位网络安全预警工作情况等。）
8、单位网络安全应急预案和演练情况
（重点包括：是否制定了单位网络安全预案？单位网络安全预案是否进行了演练？是否根据演练情况对预案进行了修改完善等情况。）

9、单位网络安全事件（事故）的处置情况
（重点包括：是否明确了单位网络安全事件（事故）发现、报告和处置流程？年内是否发生重大网络安全事件（事故）？是否与相关部门建立了网络安全应急处置机制等情况。）
10、单位信息技术产品、服务国产化情况
（重点包括：单位操作系统、服务器、数据库、交换机等核心信息技术产品的国产化比率情况；单位网络安全设备的国产化比率情况；单位信息技术产品国产化替换工作计划情况；单位新建网络是否采用国产化设备；单位信息安全服务情况等。）
11、单位网络安全宣传培训情况
（重点包括：单位组织开展网络安全宣传教育情况；单位组织开展网络安全岗位培训和网络安全员培训等情况。）

三、网络运营者信息系统基本情况

序号	网络名称	安全保护等级	是否备案	备案编号	本年度是否测评	IP 或域名	系统类型
1							□基础网络 □办公系统 □业务系统 □门户网站 □邮件或通信系统 □云平台 □大数据 □移动APP □工控系统 □其他
2							