**网 络 安 全 承 诺 书**

一、本单位因为使用网络（信息）系统，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，由本单位承担由此带来的一切民事、行政和刑事责任。

二、本单位承诺遵守《计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》，《互联网信息服务管理办法》，《计算机病毒防治管理办法》，《互联网安全保护技术措施规定》，《信息安全等级保护管理办法》等国家法律、法规和行政规章制度。

 三、本单位建设、运营和使用网络（信息）系统，按照规定期限到公安机关履行定级备案手续，同时开展安全测评、安全建设整改和安全自查等工作。

四、本单位承诺建立健全各项网络（信息）系统的安全保护管理制度和落实各项安全保护技术措施。

五、本单位承诺当网络（信息）系统发生重大网络安全事件（事故）时，立即启动应急预案，采取有效措施，保留有关原始记录，并在24小时内向公安机关网安部门报告。

六、若违反本承诺有关条款和国家相关法律法规，本单位愿承担相应法律责任；造成第三方财产损失的，本单位将在国家有关机关确认的责任范围内给予赔偿。

七、本承诺书自签署之日起施行。

网络（信息）系统单位

负责人签字： 盖章：

年 月 日

 **网 络 安 全 责 任 书**

根据《网络安全法》《数据安全法》《个人信息保护法》和《关键信息基础设施安全保护条例》等规定，为加强网络（信息）系统安全保护工作，由公安机关与网络（信息）系统安全责任单位共同签订责任书，明确和落实网络（信息）系统安全主体责任和公安机关安全监管责任。具体内容如下：

一、网络（信息）系统单位要高度重视网络安全保护工作，按照“谁主管、谁负责，谁运营、谁负责，谁使用、谁负责”的原则，明确责任，落实网络（信息）系统各项安全保护措施，保障网络（信息）系统安全稳定运行。

二、网络（信息）系统建设和应用要与网络安全同步规划、同步建设、同步实施，开展信息安全等级保护定级备案、安全测评、安全建设整改和安全自查等工作。

三、网络（信息）系统单位要制定完善网络（信息）系统安全应急预案，定期开展应急演练。建设安全监测手段，开展实时监测。对重要数据和系统，建设相应备份措施。做好技术力量、资源的储备，应对重大突发事件的发生。

四，网络（信息）系统单位应配合公安机关开展安全检查，与公安机关建立重大网络安全事件（事故）发现、报告、应急处置等工作机制。

五、公安机关应加强对网络（信息）系统单位网络安全工作的指导，定期进行现场安全检查，技术检测和远程技术检测，对网络（信息）系统存在的安全漏洞和隐患及时通报预警，对发生的案事件及时进行调查侦查，打击攻击网络（信息）系统的违法犯罪活动。

六、对网络（信息）系统安全责任和工作要求不落实的，公安机关应督促网络（信息）系统单位及时整改，情节严重的，依法追究相关单位及责任人的法律责任，并进行通报。

七、本“责任书”一式两份。网络（信息）系统单位和公安机关各存一份。

网络（信息）系统单位 公安机关网安部门

负责人签字： 负责人签字：

盖章： 盖章：

 年 月 日

|  |
| --- |
| 伊犁哈萨克自治州尼勒克县公安局网络安全监督检查通知书尼公网安 检字[ ] 号 ：根据《网络安全法》、《数据安全法》和《关键信息基础设施安全保护条例》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》《数据安全法》《关键信息基础设施安全保护条例》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： 尼勒克县公安局网安大队 年 月 日  |

一式两份，一份交被通知单位，一份附卷。

|  |
| --- |
| 伊犁哈萨克自治州尼勒克县公安局网络安全监督检查记录尼公网安 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）  |

此记录由公安机关存档。

|  |
| --- |
| 伊犁哈萨克自治州尼勒克县公安局网络安全监督检查限期整改通知书尼公网安 限字[ ]第 号 ：根据《网络安全法》、《数据安全法》、《个人信息保护法》和《关键信息基础设施安全保护条例》，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：1．2．3．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。 尼勒克县公安局网安大队年 月 日（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。

|  |
| --- |
| 伊犁哈萨克自治州尼勒克县公安局网络安全监督检查情况通报书 尼公网安 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

|  |
| --- |
| 伊犁哈萨克自治州尼勒克县公安局网络安全监督检查情况通报书尼公网安 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》（伊公网安 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。 尼勒克县公安网安大队年 月 日 |

一式两份，一份交被检查单位，一份附卷。

|  |
| --- |
| 伊犁哈萨克自治州尼勒克县公安局网络安全监督检查反馈意见 尼公网安 检字[ ] 号 ：根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》和《关键信息基础设施安全保护条例》等规定，我单位于 年 月 日对你单位网站安全保护工作进行现场检查。现将有关意见建议反馈如下： 联系单位： 尼勒克县公安局网络安全保卫大队联 系 人： 买尔旦 联系电话：14799900097  尼勒克县公安局网安大队年 月 日 |

一式两份，一份交被检查单位，一份附卷。

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 |  |
| 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、指挥调度等基本功能 | □是 □否 |
| 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。

被检查单位主管人员（签名）