公安机关信息安全等级保护检查工作规范（试行）

第一条为规范公安机关公共信息网络安全监察部门开展信息安全等级保护检查工作，根据《信息安全等级保护管理办法》（以下简称《管理办法》），制定本规范。

第二条公安机关信息安全等级保护检查工作是指公安机关依据有关规定，会同主管部门对非涉密重要信息系统运营使用单位等级保护工作开展和落实情况进行检查，督促、检查其建设安全设施、落实安全措施、建立并落实安全管理制度、落实安全责任、落实责任部门和人员。

第三条信息安全等级保护检查工作由市（地）级以上公安机关公共信息网络安全监察部门负责实施。每年对第三级信息系统的运营使用单位信息安全等级保护工作检查一次，每半年对第四级信息系统的运营使用单位信息安全等级保护工作检查一次。

第四条公安机关开展检查工作，应当按照“严格依法，热情服务”的原则，遵守检查纪律，规范检查程序，主动、热情地为运营使用单位提供服务和指导。

第五条信息安全等级保护检查工作采取询问情况，查阅、核对材料，调看记录、资料，现场查验等方式进行。

第六条检查的主要内容：
（一）等级保护工作组织开展、实施情况。安全责任落实情况，信息系统安全岗位和安全管理人员设置情况；
（二）按照信息安全法律法规、标准规范的要求制定具体实施方案和落实情况；
（三）信息系统定级备案情况，信息系统变化及定级备案变动情况；
（四）信息安全设施建设情况和信息安全整改情况；
（五）信息安全管理制度建设和落实情况；
（六）信息安全保护技术措施建设和落实情况；
（七）选择使用信息安全产品情况；
（八）聘请测评机构按规范要求开展技术测评工作情况，根据测评结果开展整改情况；
（九）自行定期开展自查情况；
（十）开展信息安全知识和技能培训情况。

第七条检查项目：
（一）等级保护工作部署和组织实施情况
1．下发开展信息安全等级保护工作的文件，出台有关工作意见或方案，组织开展信息安全等级保护工作情况。
2．建立或明确安全管理机构，落实信息安全责任，落实安全管理岗位和人员。
3．依据国家信息安全法律法规、标准规范等要求制定具体信息安全工作规划或实施方案。
4．制定本行业、本部门信息安全等级保护行业标准规范并组织实施。
（二）信息系统安全等级保护定级备案情况
1．了解未定级、备案信息系统情况以及第一级信息系统有关情况，对定级不准的提出调整

建议。
2．现场查看备案的信息系统，核对备案材料，备案单位提交的备案材料与实际情况相符合情况。
3．补充提交《信息系统安全等级保护备案登记表》表四中有关备案材料。
4．信息系统所承载的业务、服务范围、安全需求等发生变化情况，以及信息系统安全保护等级变更情况。
5．新建信息系统在规划、设计阶段确定安全保护等级并备案情况。
（三）信息安全设施建设情况和信息安全整改情况
1．部署和组织开展信息安全建设整改工作。
2．制定信息安全建设规划、信息系统安全建设整改方案。
3．按照国家标准或行业标准建设安全设施，落实安全措施。
（四）信息安全管理制度建立和落实情况
1．建立基本安全管理制度，包括机房安全管理、网络安全管理、系统运行维护管理、系统安全风险管理、资产和设备管理、数据及信息安全管理、用户管理、备份与恢复、密码管理等制度。
2．建立安全责任制，系统管理员、网络管理员、安全管理员、安全审计员是否与本单位签订信息安全责任书。
3．建立安全审计管理制度、岗位和人员管理制度。
4．建立技术测评管理制度，信息安全产品采购、使用管理制度。
5．建立安全事件报告和处置管理制度，制定信息系统安全应急处置预案，定期组织开展应急处置演练。
6．建立教育培训制度，定期开展信息安全知识和技能培训。
（五）信息安全产品选择和使用情况
1．按照《管理办法》要求的条件选择使用信息安全产品。
2．要求产品研制、生产单位提供相关材料。包括营业执照，产品的版权或专利证书，提供的声明、证明材料，计算机信息系统安全专用产品销售许可证等。
3．采用国外信息安全产品的，经主管部门批准，并请有关单位对产品进行专门技术检测。
（六）聘请测评机构开展技术测评工作情况
1．按照《管理办法》的要求部署开展技术测评工作。对第三级信息系统每年开展一次技术测评，对第四级信息系统每半年开展一次技术测评。
2．按照《管理办法》规定的条件选择技术测评机构。
3．要求技术测评机构提供相关材料。包括营业执照、声明、证明及资质材料等。
4．与测评机构签订保密协议。
5．要求测评机构制定技术检测方案。
6．对技术检测过程进行监督，采取了哪些监督措施。
7．出具技术检测报告，检测报告是否规范、完整，检查结果是否客观、公正。
8．根据技术检测结果，对不符合安全标准要求的，进一步进行安全整改。
（七）定期自查情况
1．定期对信息系统安全状况、安全保护制度及安全技术措施的落实情况进行自查。第三级信息系统是否每年进行一次自查，第四级信息系统是否每半年进行一次自查。
2．经自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位进一步进行安全建设整改。

第八条各级公安机关按照“谁受理备案，谁负责检查”的原则开展检查工作。具体要求是：

对跨省或者全国联网运行、跨市或者全省联网运行等跨地域的信息系统，由部、省、市级公安机关分别对所受理备案的信息系统进行检查。对辖区内独自运行的信息系统，由受理备案的公安机关独自进行检查。

第九条对跨省或者全国联网运行的信息系统进行检查时，需要会同其主管部门。因故无法会同的，公安机关可以自行开展检查。

第十条公安机关开展检查前，应当提前通知被检查单位，并发送《信息安全等级保护监督检查通知书》。

第十一条检查时，检查民警不得少于两人，并应当向被检查单位负责人或其他有关人员出示工作证件。

第十二条检查中应当填写《信息系统安全等级保护监督检查记录》（以下简称《监督检查记录》）。检查完毕后，《监督检查记录》应当交被检查单位主管人员阅后签字；对记录有异议或者拒绝签名的，监督、检查人员应当注明情况。《监督检查记录》应当存档备查。

第十三条检查时，发现不符合信息安全等级保护有关管理规范和技术标准要求，具有下列情形之一的，应当通知其运营使用单位限期整改，并发送《信息系统安全等级保护限期整改通知书》（以下简称《整改通知》）。逾期不改正的，给予警告，并向其上级主管部门通报：
（一） 未按照《管理办法》开展信息系统定级工作的；
（二） 信息系统安全保护等级定级不准确的；
（三） 未按《管理办法》规定备案的；
（四）备案材料与备案单位、备案系统不符合的；
（五）未按要求及时提交《信息系统安全等级保护备案登记表》表四的有关内容的；
（六）系统发生变化，安全保护等级未及时进行调整并重新备案的；
（七）未按《管理办法》规定落实安全管理制度、技术措施的；
（八）未按《管理办法》规定开展安全建设整改和安全技术测评的；
（九）未按《管理办法》规定选择使用信息安全产品和测评机构的；
（十）未定期开展自查的；
（十一）违反《管理办法》其他规定的。

第十四条检查发现需要限期整改的，应当出具《整改通知》，自检查完毕之日起 10 个工作日内送达被检查单位。

第十五条信息系统运营使用单位整改完成后，应当将整改情况报公安机关，公安机关应当对整改情况进行检查。

第十六条公安机关实施信息安全等级保护监督检查的法律文书和记录，应当统一存档备查。

第十七条受理备案的公安机关应该配备必要的警力，专门负责信息安全等级保护监督、检查和指导。从事检查工作的民警应当经过省级以上公安机关组织的信息安全等级保护监督检查岗位培训。

第十八条公安机关对检查工作中涉及的国家秘密、工作秘密、商业秘密和个人隐私等应当予以保密。

第十九条公安机关进行安全检查时不得收取任何费用。

第二十条本规范所称“以上”包含本数（级）。

第二十一条本规范自发布之日起实施。