长审字〔2022〕19号

**关于印发《长子县审计局审计专网计算机**

**网络与信息安全管理办法（试行）》等制度的通 知**

 各股室、中心：

《长子县审计局审计专网计算机网络与信息安全管理办法（试行）》、《长子县审计局审计业务电子数据管理办法》、《长子县审计局网络安全事件应急预案》已经局党组研究通过。现印发给你们，请遵照执行。

长子县审计局

2022年8月10日

 （此件公开发布）

**长子县审计局**

**审计专网计算机网络与信息安全管理办法**

**（试 行）**

**第一章  总  则**

**第一条**   为确保我局计算机网络与信息系统安全、稳定、高效运行，依据国家保密局、公安部、审计署、审计厅、市审计局有关计算机网络和信息安全的有关规定，结合我局实际，制定本办法。

**第二条**  本办法所称审计专网是指省厅金审工程建设依托国家电子政务外网互联，承载非集中存储处理的审计机关工作秘密、与审计事项有关的被审计单位工作秘密、商业秘密（以下简称工作秘密、商业秘密）和其他审计工作信息的系统。审计专网属于非涉密网络，不运行存储处理涉及国家秘密的信息。

**第三条**  本办法适用于各股室（中心）全体工作人员。

**第二章  管理机构与职能**

**第四条**  成立局网络安全与信息化建设领导小组，以党组书记、局长为组长，分管领导为副组长，各股室负责人为领导小组成员。领导小组办公室设在局办公室，由办公室人员负责运维和日常检查工作。

**第五条**  局办公室具体承担局网络安全与信息化建设日常工作，负责本单位网络信息安全督促、检查、指导等日常工作。

**第三章  人员安全管理**

**第六条** 我局人员不得利用网络从事危害国家安全的活动，不得泄露国家秘密和单位敏感信息，不得侵犯国家、社会、集体的利益和公民的合法权益，不得从事违法犯罪活动。

**第七条** 局各股室（中心）根据审计业务应与各自签约的外聘单位签订保密协议书，相关人员必须进行保密承诺，明确安全保密要求与责任。

**第八条**  我局人员离岗离职时，局办公室应终止其信息系统访问权限，收回各种软硬件设备及电子数字证书等，关键岗位人员须承诺离岗离职后的保密义务。

**第九条** 全局人员应当接受网络信息安全教育或培训。培训内容包括：网络与信息安全策略、安全职责、安全管理规章制度和有关法律法规。

**第四章  账号安全管理**

**第十条**  加强终端计算机账号与密码安全管理，账号密码长度应采用8位以上，由非纯数字或字母组成，每三个月至少更换一次密码。

**第十一条**  加强审计专网中各业务系统和办公系统的账号、密码及权限管理。

（一）各系统的账号及初始密码由局办公室申请后，省厅统一分配。

（二）用户在初次登陆系统后要及时修改密码，密码长度不得小于6位，不得使用生日、电话号码等容易破解的密码，并要定期更换。

**第十二条**  终端计算机以及各系统的账号、密码只授予我局人员使用。我局人员对自己享用的资源有保护责任，口令密码不得泄露给他人，如有泄露应及时改变，由此造成的损失由本人负责。

**第十三条**  未经许可或授权，任何人不得以任何方式使用他人的账号及密码。否则，使用人承担一切后果。

**第五章  网络安全管理**

**第十四条**  各股室（中心）对涉及到网络变更方面的需求（如IP地址申请使用、变更等）、非常规性网络访问（如外来人员临时性访问），需向局办公室提出申请，局办公室对变更申请进行评审通过后，方可进行操作。

**第十五条** 全局人员不得在局机关办公区域内擅自部署无线网络。

**第十六条**  局办公室负责局网络安全防护工作，采取安全措施进行有效隔离防护。

**第十七条**  严禁已接入厅审计专网的计算机通过拨号、无线WIFI、无线上网卡、设置代理服务器等方式接入因特网。

**第十八条**  严禁已接入厅审计专网的计算机使用WIFI类设备。

**第十九条**  在厅审计专网上不得进行任何干扰他人使用、干扰网络服务和网络设备的活动。这些活动具体包括：在厅网络上发布不真实的信息、散布计算机病毒、使用网络进入未经授权使用的计算机、不以真实身份使用网络资源，导致联网计算机系统发生阻塞、溢出、处理机忙、资源异常消耗、死机、瘫痪等运行异常。

**第二十条** 全局人员不得冒用他人名义从事网上活动。不得通过扫描、侦听、破解口令、安置木马、远程接管、利用系统缺陷等手段获取他人信息。

**第二十一条**  全局人员不得利用厅审计专网网络制作、复制、查阅和传播违反宪法和法律法规的信息。

**第六章  终端计算机防护管理**

**第二十二条**  未经批准，全局人员不得擅自改变终端计算机的内部配置、外观和连线。

**第二十三条**  任何连入厅审计专网的计算机均须安装防病毒软件和系统补丁程序，定期对计算机进行查杀毒。一旦发现网络病毒，应立即采取相应措施，避免病毒扩散。

**第二十四条**  禁止在终端计算机安装使用来历不明的软件，并且遵守知识产权有关法律法规。

**第二十五条**  在使用他人计算机软盘、光盘、移动存储等信息存储设备前，必须先进行病毒检查，确信无病毒后，方可使用。

**第七章  信息与数据安全管理**

**第二十六条**  全局人员离开本人座位或在办公区域接待访客时，应将终端计算机退出登录状态。

**第二十七条**  全局人员在使用计算机过程中，要做好审计工作信息的保密工作，确保计算机及其他存储设备中的数据不泄漏。

**第二十八条**  局各股室（中心）应对各自的关键文件、重要数据进行定期备份，并妥善保管，确保数据安全。

**第二十九条**  计算机设备送修时，应确保其中没有存储工作秘密和商业秘密的相关数据，必要时将计算机硬盘拆除后再送修。

**第八章  附  则**

**第三十条** 违反本办法有关规定，视情节分别给予口头批评、通报批评；造成危害后果的，依照有关规定给予行政处分；涉嫌犯罪的，移交司法机关处理。

**第三十一条**  本办法由局网络安全与信息化建设领导小组负责解释。

**长子县审计局**

**审计业务电子数据管理办法**

**第一章    总  则**

**第一条**  为加强审计业务电子数据管理，规范审计业务电子数据采集、存储和使用，保障审计业务电子数据安全，促进数据综合分析利用，根据《中华人民共和国审计法》和《中华人民共和国审计法实施条例》等法律、法规和国家有关规定，制定本办法。

**第二条**  本办法所称的审计业务电子数据，是指为履行审计职责、运用计算机技术进行审计数据分析而采集和使用的电子数据，包括：

（一）从被审计单位采集的财务数据、业务数据、管理数据及相关技术文档。

（二）审计人员对被审计单位原始电子数据经过清洗、转换、审核整理的中间表数据。

（三）从被审计单位以外其他部门和单位取得的与审计业务相关的电子数据。

**第三条**  审计业务电子数据管理应遵循分散采集、集中管理、授权使用、安全保密的原则。

各股室（中心）是审计业务电子数据的采集、使用部门。局数据中心是采集、分析审计业务电子数据的技术支持和数据集中管理内设中心。

**第四条** 审计业务电子数据按不同来源实行等级化保护管理，不同密级的国家秘密或者商业秘密和工作秘密交叉组合的，按最高密级保护管理。

**第二章 电子数据采集、验收、移交和存储**

**第五条**  审计业务电子数据按以下三种方式管理：

（一）定期采集的审计业务电子数据，由各股室（中心）按照职责范围和时间要求组织开展采集、验收、移交和本地恢复工作。

（二）审计项目实施中临时采集的审计业务电子数据，由审计组负责采集、恢复、验证、分析和移交工作。

（三）按照上级部署或局统一组织的重大审计项目，由项目实施牵头股室负责开展采集、报送、恢复、验收、综合分析和移交工作。

局数据中心负责对上述所有数据的集中、复核、备份及向上级审计机关报送定期采集的审计业务电子数据，各部门均需对上述工作中的安全保密工作负责。

**第六条**  从被审计单位和相关部门、单位获取原始电子数据时，应当履行必要的交接手续，对接收的审计业务电子数据进行登记，并验证其真实性和完整性。

**第七条**  定期采集的审计业务电子数据按以下程序采集、整理和移交：

（一）各股室（中心）接收电子数据时，应要求数据提供单位对数据的真实性、完整性做出书面承诺，提交《提供电子数据和资料承诺书》（附件1）。

（二）各股室（中心）在职责范围内，根据上级审计机关下发的审计业务电子数据采集方案组织开展相关审计业务电子数据的采集、验收和本地恢复。填写完成《长子县审计局审计业务电子数据接收单》（附件2）。

（三）各股室（中心）在完成审计业务电子数据采集30日内，将数据移交局数据中心，存入局数据中心，并填写《长子县审计局审计业务电子数据移交单》（附件3）。

**第八条** 审计项目实施中临时采集的审计业务电子数据，按以下程序采集、整理、移交：

（一）审计组应在审计通知书中告知被审计单位需采集的电子数据种类、时间期限等要素。已经列入定期采集清单的数据，应向办公室提出数据使用申请，不再重复采集。

（二）审计组收到被审计单位提交的审计业务电子数据，应对数据的完整性、有效性作初步检查，与数据提供单位履行交接手续，填写《长子县审计局审计业务电子数据接收单》。

（三）审计项目结束后60个工作日内，审计组所在股室（中心）应将审计业务电子数据移交局数据中心，存入局数据中心，填写《长子县审计局审计业务电子数据移交单》。

**第九条**  统一组织的重大审计项目，按以下程序开展审计业务电子数据的采集、整理、报送工作：

（一）按照上级部署统一组织的重大审计项目，由项目实施牵头股室根据上级审计机关下发的采集方案组织开展相关审计业务电子数据的采集；局统一组织的重大审计项目，由项目实施牵头股室制定审计业务电子数据采集、使用方案，根据审计对象范围确定需采集的审计业务电子数据种类、时间期限、地域范围等要素，以及数据分割方式、分发范围，并统一或分别在审计通知书中告知被审计单位。

（二）由项目实施牵头股室负责对统一数据的采集、恢复和验证，填写《长子县审计局审计业务电子数据接收单》。

（三）由项目实施单位负责对非统一数据的采集、恢复和验证，与数据提供单位履行交接手续，填写《长子县审计局审计业务电子数据接收单》。

（四）已经列入定期采集清单的数据，不再重复采集。由项目实施牵头股室向数据中心提出数据使用申请。

（五）项目实施牵头股室对统一采集的审计业务电子数据或者申请获得授权使用的定期采集数据，按数据采集、使用方案切割、分发至项目实施单位。

（六）审计项目结束后60个工作日内，项目实施单位应将按照本条第（三）项规定采集的审计业务电子数据集中至项目实施牵头股室，由项目实施牵头股室统一移交数据中心，存入局数据中心，填写《长子县审计局审计业务电子数据移交单》。

**第十条**  审计组所在股室（中心）或统一组织项目牵头股室移交数据中心的审计业务电子数据应包括从被审计单位采集的原始数据及日志、标准化数据、数据字典、报表数据，数据说明文档等。

**第十一条**  审计业务电子数据全部存放在局办公室集中管理。局数据中心负责存储的审计业务电子数据日常管理，定期制作并向各股室（中心）提供存储的数据目录清单。

**第十二条**  因实施审计项目所获取和留存的电子数据，审计组或审计人员应按本办法第八条、第九条规定的期限移交，不得擅自留存。各股室（中心）应对审计现场数据安全实施检查，检查数据存储、使用是否安全、审计人员有无擅自留存电子数据等，并做好书面记录。

**第十三条**  局数据中心接收各股室（中心）当年移交的审计业务电子数据，应对数据进行查杀病毒等预处理和恢复，并将数据存储至适当位置，第二年3月前交局办公室统一管理。

**第十四条**  局数据中心应当遵循相关国家标准、专业审计数据规划或国家审计数据中心的统一要求整理和加工相关审计业务电子数据，各股室（中心）提供业务支持。

**第十五条** 局数据中心应建立审计业务电子数据存储、备份和恢复策略，及时组织数据备份，保证审计业务电子数据安全、保密和数据库正常运行。

**第十六条**  审计业务电子数据根据时间期限实施不同存储策略：3年以内数据采取在线方式存储；3年以上5年以内的数据采取离线方式存储；5年以上的数据除业务股室特别需要外不再保存。

**第三章 电子数据授权与使用**

**第十七条**  局数据中心存储的审计业务电子数据应经授权程序取得相应使用权限后方可使用，使用完毕后应及时注销授权。

（一）各股室（中心）使用本股室职责范围内采集、加工、移交的数据，由数据使用人填写《长子县审计局审计业务电子数据授权使用审批单》（附件4），经本股室（中心）主要负责人批准后，由数据中心授予使用权限。

（二）各股室（中心）使用其他股室采集、加工、移交的数据，由数据使用人填写《长子县审计局审计业务电子数据授权使用审批单》，经本股室（中心）主要负责人签署意见，报分管本股室（中心）局领导和信息化工作局领导审批同意后，由局数据中心授予使用权限。

（三）统一组织审计项目调用局数据中心存储的审计业务电子数据，由该项目的组织实施单位填写《长子县审计局审计业务电子数据授权使用审批单》，经本股室主要负责人签署意见，报分管本股室局领导和信息化工作局领导审批同意后，由局办公室授予使用权限。

（四）各股室（中心）申请共享省厅、市局数据中心存储的审计业务电子数据，在上述审批程序基础上，报局长审批同意后，由局办公室申请并授予使用权限。

**第十八条**  局办公室和局数据中心存储的电子数据原则上不对我县审计机关以外的其他单位提供调用。确有需要的，使用单位提出书面申请函，经局长批准同意后，在指定的场所和设备上操作使用。

**第十九条**  审计人员使用审计业务电子数据应当严格遵守以下规定：

（一） 在审计机关配备的专用设备上开展数据分析工作。

（二）不得向与审计工作无关人员泄漏数据、数据分析方法和分析结果。

（三） 严格身份、密码管理，不得泄漏和借与他人使用。

（四）不得在局数据中心专用设备上随意加载未经许可的电子数据和分析工具，确保分析数据、数据库资源和数据分析结果的安全。

（五）审计人员不得私自使用和存放原始数据，未经授权，不得私自下载电子数据。

**第二十条**  局各股室人员利用审计业务电子数据进行科研、培训、宣传等活动时，不得违反国家、审计署、省审计厅和局有关保密规定以及本管理办法要求。

**第二十一条**  遇有下列情况时，局办公室应当根据各股室（中心）的书面告知，及时收回分配的审计业务电子数据使用权限，并做好过程记录：

（一）审计项目结束，不再需要使用数据的。

（二）审计人员调离审计机关或变更业务部门、受聘参与审计组的外部聘请人员完成任务离开审计组的。

（三）其他需要收回权限的情形。

审计组发生违规使用审计业务电子数据或失密事件的，局办公室有权收回使用权限，控制损失。

**第二十二条**  审计人员对审计业务电子数据的综合分析和加工工作应在熟悉被审计单位业务流程和数据结构的基础上，围绕审计工作目标进行。各审计组应依据审计工作方案，制定具体的审计业务电子数据综合分析方案或计算机审计实施方案，明确数据来源、分析思路、审计重点、方法、结果利用和相关责任。

**第二十三条**  数据分析人员应当保留数据分析的工作轨迹，为审核和审理工作提供依据。数据分析团队应指定专人负责数据分析结果审核工作，审核内容包括数据分析过程、分析结果、延伸调查结果、取证资料等。数据分析团队负责人对数据分析结果的可利用性负责。

**第二十四条** 对审计业务电子数据分析以及对分析结果进行延伸落实过程中，因分析人员或延伸审计人员不负责发生审计质量问题，造成审计工作受到影响的，参照审计项目质量责任追究的相关办法处理。

**第四章   电子数据分析环境**

**第二十五条** 电子数据分析环境是指开展审计业务电子数据分析的网络、专用场所、虚拟化服务器资源及虚拟桌面等设备环境。

**第二十六条** 数据分析设备使用实行严格的登记制度。使用数据的协审人员应签订保密承诺书（附件5）。

**第二十七条** 审计人员在数据分析室从事数据分析工作时，一律不得擅自对电子数据及分析结果进行拍照、录像、抄录等操作，不得以任何形式泄露电子数据及相关的分析结果。

**第五章   电子数据输出管理**

**第二十八条** 严格控制数据输出。数据输出建立记录台账，输出内容留存至指定区域。原始数据、数据字典和审计方法不允许输出。

**第二十九条** 各股室（中心）需要输出电子数据的，根据需要填写《审计业务电子数据输出审批单》（附件7），由审计项目牵头股室主要负责人审批，由专人负责输出给审计项目主审或组长。

**第六章 责任追究**

**第三十条**  对不按规定程序采集、报送、恢复入库、验收、存储、使用、输出审计业务电子数据的，视情节轻重，追究相关责任人和直接领导的责任。

**第三十一条** 本规定所涉及到的人员存在以下情形的，将按照有关规定进行问责和处理：

（一）遗失存储设备、介质，造成电子数据外泄和损失的。

（二）擅自毁弃、藏匿、删除电子数据，损害信息资产完整性的。

（三）擅自留存或不及时移交应当移交的电子数据并造成不良后果的。

（四）违规使用电子数据的。

（五）违规输出电子数据的。

（六）其它未按规定使用电子数据并造成不良后果的情形。

**第七章 附  则**

**第三十二条**  本办法由局办公室负责解释。

附件：1.提供电子数据和资料承诺书

2.《长子县审计局审计业务电子数据接收单》

3.《长子县审计局审计业务电子数据移交单》

4.《长子县审计局审计业务电子数据授权使用审批单》

5.保密承诺书

6.《审计业务电子数据输出审批单》

附件1

**提供电子数据和资料承诺书**

长子县审计局：

根据《中华人民共和国审计法》第三十四条规定，我单位提供了要求于       年     月报送的                  电子数据和相关资料（提供清单见附件），并作出如下承诺：

我单位对提供的电子数据和资料的真实性和完整性负责。

单位（印章）

年 月 日

附件2

**长子县审计局审计业务电子数据接收单**

编号：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **数据名称** | **数据类型** | **数据****密级** | **数据地域范围** | **数据****时间****范围** | **数据****报送****时间** | **数据****报送人** | **数据****接收人** | **备注** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

数据报送单位：                                  接收部门：

注：1.数据类型是指财务会计数据、业务数据、管理数据、其他

数据等。

2.接收涉密数据，报送单密级按数据最高密级确定。

附件3

**长子县审计局审计业务电子数据移交单**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **数据主要内容** | **区域范围** | **数据****时段** | **数据量（GB）** | **存储介质类型** | **型号及序列号** | **备注** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 电子数据移交确认环节 | 电子数据入库环节 | 存储介质移交环节 |
| 数据移交人签名： |  | 接收人签名： |  | 接收人签名： |  |
| 移交时间： |  | 移交时间： |  | 移交时间： |  |

数据移交部门：

附件4

**长子县审计局**

**审计业务电子数据授权使用审批单**

编号：                 申请日期：     年    月    日

|  |  |  |  |
| --- | --- | --- | --- |
| 申请人 |  | 申请人所在部门 |  |
| 申请理由 |    申请人：                          联系电话： |
| 申请权限 | 申请授权内容：     数据内容起止时段：申请类型：□新增   □变更权限种类：□用户账号 □查询权限 □指定模式下的操作权限授权截至时间： |
| 申请人所在部门主要负责人意  见 |     签名：日期：      年  月  日 | 数据中心主要负责人意见 |     签名：日期：    年   月  日 |
| 分管业务局领导意见 |   签名：日期：      年  月  日 | 分管信息化工作局领导意见 |    签名：日期：     年  月  日 |
| 局长意见 |                   签名：                日期：  年  月    日 |

 附件5

**保密承诺书**

根据《中华人民共和国保守国家秘密法》和相关法律法规，本人作为审计项目人员，了解有关保密法规制度，知悉应当承担的保密义务和法律责任，并庄重承诺：

一、认真遵守国家保密法律、法规和规章制度，履行保密义务，自愿接受保密审查。

二、不违规记录、存储、复制审计项目实施过程中触及的国家秘密、商业秘密和工作秘密，不违规留存涉密信息载体。

三、不以任何方式泄露所接触和知悉的秘密信息。

四、未经审查批准，不擅自发表涉及未公开工作内容的文章、著述。

五、审计项目结束后，自愿接受脱密期管理。

若违反上述承诺，自愿承担法律责任。

本承诺书一式三份，经双方签字后生效。

承诺人签名：          审计组组长（协审负责人）签名：

   年   月   日                     年    月    日

附件6

**审计业务电子数据输出审批单**

编号：

申请股室：         项目名称：           项目主审/组长：

|  |
| --- |
| 我股室需拷贝数据分析结果，具体内容及理由为：    记录条数：                          数据大小：   经办人：                              日期：     年   月   日 |
| 申请股室主要负责人意见：   （签字/签章）                        日期：      年   月    日 |

**长子县审计局**

**网络安全事件应急预案**

**第一章  总  则**

**第一条**  为完善长子县审计网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保证网络安全事件应急处置工作迅速、高效、有序执行，依据中央网信办网络安全事件应急的有关规定，制定本预案。

**第二条**  长子县审计网络安全事件处置由长子县审计局党组统一组织领导，具体工作接受长子县审计局网络安全与信息化建设领导小组（以下简称局网信领导小组）的领导。

**第三条** 坚持统一指挥、密切协同、快速反应、科学处置；坚持以预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责等原则。充分发挥各方面的力量，共同做好长子县审计网络安全事件的预防与处置工作。

**第四条**  本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对长子县审计网络和信息系统或者其中数据造成危害，对社会造成不良影响的事件。

**第五条** 本预案适用于长子县审计网络安全事件的应对工作。

**第二章  组织机构与职责**

**第六条**  长子县审计局成立网络安全应急办公室（以下简称局网络安全应急办），局网络安全应急办在局网信领导小组的领导下开展工作，负责长子县审计网络安全事件应对工作，包括网络安全事件的预防、监测、报告和应急处置工作。

**第七条** 局网络安全应急办设在局办公室，信息化分管领导担任应急办主任，局数据中心主任担任应急办副主任，在局网信领导小组的领导下全面负责处置网络安全事件的组织、指挥、协调工作。下设应急保障组和技术支持组。

（一）网络安全应急办主要职责。

1.向局网信领导小组报告网络安全事件应对工作相关情况，重大事项向局党组报告；

2.贯彻落实局党组决策部署，落实局网信领导小组工作安排，协调和调动各部门应对网络安全事件应急相关工作；

3.局网络安全风险评估控制、隐患排查和整改；

4.制定（完善）局网络安全事件应急预案；

5.局网络安全事件应急预案演练；

6.局网络安全事件应急知识的宣传教育与培训；

7.局网络安全事件应急支撑队伍的组建与调配使用。

（二）应急保障组职责。

应急保障组负责现场应急指挥处置和应急处置期间的综合保障工作。应急保障组在局网络安全应急办负责人授权下，行使现场应急指挥、协调、处置等职责。

1.根据事件性质，迅速调集相关技术专家，组建事件处置工作组，为长子县审计网络安全应急办提供决策支持；

2.根据局网络安全应急办指令，负责现场应急指挥工作，针对网络安全事件发展的事态，制定和调整相应网络安全事件处置、恢复和预防方案；

3.整合调配现场应急资源；

4.核实应急终止条件并向局网络安全应急办请示应急终止；

5.收集、整理应急处置过程资料，编写现场应急工作总结报告。

6.协调相关部门和单位，确保技术支撑专家第一时间到达现场；

7.负责现场处置所需要的计算机、网络等设备设施的到位和畅通。

（三）技术支持组职责。

组建局网络安全事件应急技术支撑队伍并遴选局网络安全事件应急技术支撑单位，从长子县政府网络安全相关技术支撑单位和局协审服务单位中邀请相关专家和技术人员，与长子县审计局有关人员组成局网络安全应急技术支撑队伍。

1.为网络安全事件应急处置方案提供技术支持和建议；

2.为应急预案及管理工作提出建议，参与应急工作重大事项的决策和实施；

3.为重大活动（会议）期间的网络安全保障工作提供现场应急处置。

**第三章  事件分类分级**

**第八条**  网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件等。

（一）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件；

（二）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；

（三）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件；

（四）信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件；

（五）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障；

（六）灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件；

（七）其他事件是指不能归为以上分类的网络安全事件。

**第九条**  长子县审计网络安全事件分为四级：由高到低划分为特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）、一般（Ⅳ级）4个级别，其中特别重大（Ⅰ级）、重大（Ⅱ级）遵循《国家网络安全事件应急预案》分级标准进行分级，较大（Ⅲ级）、一般（Ⅳ级）分级标准由长子县审计局按照严重程度、可控性和影响范围等因素确定。

**第十条**  符合下列情形之一的，为特别重大网络安全事件：

（一）重要网络遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力；

（二）国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁；

（三）其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

**第十一条**  符合下列情形之一的，为重大网络安全事件：

（一）重要网络遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响；

（二）国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁；

（三）其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

**第十二条**  符合下列情形之一的，为较大网络安全事件：

（一）网络配线间火灾或面临火灾威胁；

（二）因中心节点断电、水害、设备失灵等，造成局网络5个工作日以上的中断；

（三）数据丢失或系统故障，影响关键系统正常运行且5个工作日内不能恢复；

（四）病毒或木马入侵导致局网络30%以上的计算机感染。

**第十三条**  符合下列情形之一的，为一般网络安全事件：

（一）因中心节点断电、水害、设备失灵等，造成局网络1个工作日以上的网络中断；

（二）数据丢失或系统故障，影响关键系统正常运行且1个工作日内不能恢复；

（三）病毒或木马入侵导致局网络10%以上的计算机感染。

**第四章  监测与预警**

**第十四条**  长子县审计局建立网络安全事件信息监测机制，通过以下途径获取预报信息：

（一）主管部门向长子县审计局告知的预报信息；

（二）国家通过新闻媒体公开发布的网络安全事件预警信息；

（三）机关网络与信息安全通报机制渠道接收的网络安全预警信息、事件信息；

（四）经风险评估得出的可能发生的网络安全事件。

 **第十五条**  按照“谁主管谁负责、谁运行谁负责”的要求，局办公室负责局机关办公楼审计内网、审计专网的网络安全监测工作。

**第十六条**  局网络安全应急办负责统筹组织单位开展网络和信息系统的网络安全监测工作，网络安全监测工作包括：应用系统、系统软件、网络及网络设备、安全设备、主机、存储、外设、终端、电力、空调等基础环境的可用性和连续性的监测。

**第十七条**  长子县审计局网络安全事件预警等级遵循《国家网络安全事件应急预案》的分级标准，由高到低依次为：红色预警、橙色预警、黄色预警和蓝色预警，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

**第十八条** 局网络安全应急办负责组织对局监测信息进行研判，对需要立即采取防范措施的，立即向局网信领导小组报告，同时组织实施对应的预防工作，并结合事件具体情况在局发布黄色及以下预警。

对可能发生重大及以上网络安全事件的信息，在报经局网信领导小组同意后，及时向地方网信办和上级审计机关报告。

**第十九条**  局网络安全应急办负责组织局网络安全事件应急响应工作。

对国家网络安全应急办公室发布的红色预警，局网络安全应急办及时转发并实行24小时值班，应急保障组、技术支持组全员保持通信联络畅通。局网络安全应急办组织应急支撑队伍开展应急处置或准备、风险评估和控制工作。

对国家网络安全应急办公室发布的橙色预警，局网络安全应急办及时转发并组织开展局应急响应工作，结合局实际情况及时开展风险评估、应急准备和风险控制工作。

对黄色、蓝色预警，局网络安全应急办根据需要转发并组织支撑队伍和有关机构对事态的发展进行跟踪研判，制定防范措施和应急工作方案，协调各部门开展应急处置。

上述工作的有关情况应及时报告局网信领导小组，发现重要情况经局网信领导小组同意后，及时向地方网信办和上级审计机关报告。

**第二十条**  局网络安全应急办根据实际情况，报请局网信领导小组审核后，确定是否解除局网络安全应急办发布的黄色、蓝色预警。

**第五章  应急处置**

**第二十一条**  长子县审计局网络安全事件应急处置工作在局网络安全应急办统一调度下开展工作。

发生较大网络安全事件时，现场负责人必须在半小时内向局网络安全应急办主任报告；局网络安全应急办主任必须在1小时内向局网信领导小组报告。

发生一般网络安全事件时，现场负责人必须在1小时内向局网络安全应急办主任报告；局网络安全应急办主任必须在4小时内向局网信领导小组报告。

发生上述情况，局网络安全应急办负责人及相关人员进入应急状态，组织开展勘察、研判，处置、恢复、信息通报和管理应急状态，必要时组织技术支撑单位专家参与。

**第二十二条**  较大网络安全事件、一般网络安全事件处置完毕后，局网络安全应急办应当组织编制网络安全事件处置报告，提交局网信领导小组，并视情况向地方网信办和上级审计机关报告。

网络安全事件处置报告应结合分析系统日志、运行记录、值班记录等资料，评估事件造成的后果、产生的影响，统计处置所发生的费用和造成损失，分析事件产生的原因，提出应当采取规避措施的意见。

**第二十三条** 有害程序事件的紧急处置措施。

（一）危害系统运行的病毒暴发。

1.数据中心得到多个病毒事件报告后，应当指导计算机使用者将染毒计算机从网络上隔离，启用反病毒软件杀毒；

2.启用反病毒软件杀毒无效时，立即升级最新版本后查杀，仍无效时，通知反病毒软件公司、技术支撑专家队伍，提供病毒样本，寻求支持解决；

3.确认反病毒软件有效时，局办公室组织审计机关全网计算机统一清查杀毒；

4.局数据中心分析查明病毒暴发原因。必要时可请技术支撑单位参与分析研究。原因查明后，将有关情况报告局网信领导小组，并视需要向本地安全主管部门和上级审计机关报告。

（二）重要系统被植入木马或间谍程序。

1.抓取能够证明被植入木马或间谍程序的界面，注意保存好相关系统日志；

2.分析研判，慎重确定重要系统确实被植入木马或间谍程序；

3.局数据中心负责分析研究系统运行或者存储的信息性质、一旦被泄露后的危害，评估风险；

4.分析追查木马或间谍程序，必要时可请信息安全机构和技术支撑单位参与分析研究。查明后，将有关情况报告局网信领导小组，并视需要向国家相关机构报告或向公安部门报警。

**第二十四条**  网络攻击事件的紧急处置措施。

（一）数据中心发现网络攻击后，抓取能够证明被网络攻击的界面，注意保存好相关系统日志；

（二）将被攻击计算机从网络上隔离开来。采取查杀病毒或者升级漏洞补丁方式，避免再次遭受攻击；

（三）分析研究攻击性质，评估风险。必要时可请信息安全机构和技术支撑单位参与分析研究。查明后，将有关情况报告局网信领导小组，并视需要向国家相关机构报告或向公安部门报警。

**第二十五条**  信息破坏事件的紧急处置措施。

（一）因硬盘故障造成数据丢失。

1.因硬盘故障造成数据丢失时，操作人员或者首先发现数据丢失的人员应立即停止操作，并向对数据负有责任的股室领导报告，股室领导要及时向局网络安全应急办负责人报告，涉及审计业务数据的同时要及时向信息化分管局领导报告；

2.拔出故障硬盘，检查数据是否完整、RAID机制是否起作用。如数据完整，更换硬盘，监视系统至运行正常；

3.查看备份系统中是否有备份数据，其他介质中是否有可使用的备份数据。如有备份数据，对数据负有责任的股室恢复数据，恢复完成后调试系统至运行正常；

4.局网络安全应急办负责人组织相关单位研究评估数据丢失的影响程度；

5.数据无法从备份系统中或其他介质中恢复且人工恢复工作量可以接受的，组织人工恢复；无法人工恢复的，寻求具备资质的专业数据恢复公司恢复。

**第二十六条** 审计专网或审计内网有恶意信息的紧急处置措施。

（一）接到有关审计专网或审计内网存在恶意信息要求采取措施的情况通报后，或者数据中心发现审计专网或审计内网有恶意信息，应联系相关股室立即撤下恶意信息，同时报告局网络安全应急办负责人；

（二）抓取保存恶意信息的全部网页页面，编制抓取过程记录，注意保存好系统日志；

（三）分析追查非法信息来源，必要时可请信息安全机构参与分析研究。查明后，将有关情况报告局网信领导小组，并视需要向国家相关机构报告或向公安部门报警。

**第二十七条**  设备设施故障的紧急处置措施。

（一）系统软件故障。

1.审计管理系统等应用软件所使用的操作系统、数据库管理系统、中间件等系统软件发生故障影响系统运行时，局办公室查明故障原因，判断故障模块；

2.如属于配置的原因，应备份原配置文件，保存好系统日志，重新配置，调试至系统正常；

3.不能判断故障原因时，联系金审工程山西审计厅、应用软件开发集成商、系统软件开发商，提出解决方案。

（二）应用软件故障。

1.审计管理系统等应用软件系统发生影响运行的故障时，局办公室会同相关处查明故障原因，判断故障模块；

2.检查系统数据保存、备份情况是否正常，必要时采取补救措施；

3.先行停用部分功能，维持系统其他功能正常运行；

4.联系金审工程山西省审计厅、应用软件开发集成商，提出解决方案。

（三）公共通信设备故障或线路中断。

路由器等公共通信设备发生故障，或者中国联通、中国电信等的公共通信线路中断，造成网络中断运行时，局办公室应立即通知长子县政府办信息中心。

（四）网络设备故障。

1.防火墙、交换机等网络设备发生故障造成网络中断运行时，局办公室应立即着手确认故障节点，尽快排除故障；

2.确认属于设备硬件故障后，应立即与相关单位联系维修；

3.确认属于设备配置文件破坏后，应备份原配置文件，保存好系统日志，重新配置，调试联通。

**第二十八条**  灾害性事件的紧急处置措施。

（一）发生火灾时的紧急处置措施。

1.首先发现办公场所起火、或身置起火现场的人员应使用灭火器等扑救初期火灾，及时联系周边人员协助，现场人员应立即通知长子县政府办信息中心；

2.初期火灾不能扑灭时，现场人员迅速撤出火灾现场。能够判定义务消防员和专业消防队员即将到达的，撤出火灾现场时不关闭房门；能够判定义务消防员和专业消防队员不能及时到达，而火灾可能蔓延至其他部位时，撤出火灾现场时关闭房门；

3.现场人员应配合义务消防员和专业消防队员的工作；

4.火灾扑灭后，协助专业消防部门保护现场，配合调查起火原因，清理现场，尽可能保全设备资产和信息资源；

**第二十九条**  其他事件的紧急处置措施。

（一）人身触电。

1.发现人身触电，应立即切断电源或者采取安全方式使触电人脱离电源；

2.触电人身体遭遇伤害的，立即拨打112进行救治；

3.局网络安全应急办负责人组织查明触电原因，属于设备漏电的要采取措施。

（二）由各类紧急情况次生、衍生的紧急情况。

1.局网络安全应急办负责人召集会议，研究次生、衍生紧急情况的原因，找出主要矛盾，部署处置顺序。必要时可以局部或者全部停止系统运行；

2.相关股室根据商定的处置顺序，分头解决问题；

3.联合调试至系统恢复正常。

**第三十条** 日常工作中遇到与本预案相似情形但不能判定是否属于紧急情况的，先行按照一般网络安全事件处置。

**第六章  调查与评估**

**第三十一条**  网络安全事件处置完毕，局网络安全应急办应组织对应急响应工作进行分析和回顾，形成总结报告，总结经验并部署采取适当的后续措施。

**第三十二条**  对应急响应工作进行分析和回顾包括：

（一）应急响应工作的充分性和针对性；

（二）应急事件发生的原因、数量及频率；

（三）应急事件处置的经验和教训；

（四）应急事件的趋势信息；

（五）网络信息系统中潜在的类似隐患。

**第三十三条**  网络安全事件处置完毕，局网络安全应急办应组织对应急响应工作有效性和实效性进行评估，提出改进目标、改进的具体工作内容。

**第七章  预防工作**

**第三十四条** 局办公室负责局网络安全事件日常预防工作，定期检测排查网络安全隐患，开展风险评估和容灾备份工作，不断完善网络安全信息通报机制，提高网络安全应对能力，减少和避免网络安全事件的发生与危害。

**第三十五条** 局网络安全应急办负责局网络安全应急预案的演练工作，定期开展应急演练，根据演练结果评估应急预案并进一步完善。

**第三十六条**  局网络安全应急办负责局网络安全事件预防和处置有关法律、法规和政策的宣传，在审计专网网站加载网络安全基本知识和技能，开展网络安全事件应急知识培训，提高网络安全防范意识及技能。

**第三十七条**  在国家重要活动、会议等敏感时期，局网络安全应急办加强网络安全的检测和分析研判，及时预警可能造成的重大影响的风险和隐患。

局网络安全应急办负责在国家重要活动和会议前，按照相关主管部门的要求，委托安全部门对局网络开展渗透测试，组织局网络防护演练。按照有关部门预警要求，及时组织相关部门实行24小时值班制度，及时发现和处置网络安全事件隐患。

**第八章  保障措施**

**第三十八条** 局网络安全应急办每年根据工作需要对网络安全应急技术支撑队伍的人员进行调整和培训。

**第三十九条**局办公室每年将网络安全事件应急经费列入计算机网络运行维护项目。

**第四十条**  实行网络安全事件处置责任追究制。对人为原因引发网络安全事件的，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依据相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

**第九章  附  则**

**第四十一条**  本预案由局网信领导小组负责解释。

**第四十二条**  本预案由局网信领导小组组织制定和实施，办公室具体承担每年对预案进行评估，根据实际情况进行修订等工作。

**第四十三条**  本预案自公布之日起执行。

 长子县审计局办公室 2022年8月10日印发