通辽市人民政府办公室
关于印发《通辽市政府网站及政务新媒体信息安全管理办法》的通知

各旗县市区人民政府、开发区管委会，市政府各委办局：

经市人民政府同意，现将《通辽市政府网站及政务新媒体信息安全管理办法》印发给你们，请结合实际，认真贯彻落实。

2023 年 4 月 27 日

（此件公开发布）

通辽市政府网站及政务新媒体信息安全管理办法

第一章　总则

第一条 为切实加强通辽市政府网站及政务新媒体信息安全管理，保障我市政府网站及政务新媒体安全、稳定、高效运行。依据《政府网站发展指引》（国办发〔2017〕47号）、《国务院办公厅关于推进政务新媒体健康有序发展的意见》（国办发〔2018〕123号）、《信息安全等级保护管理办法》（公通字〔2007〕43号）等文件精神以及有关政策法规文件，结合本市实际情况，制定本办法。

第二条 通辽市政府网站及政务新媒体信息安全管理坚持“信息安全与业务并重，安全管理与技术并重”的总体方针，实现信息系统安全可查、可视、可控。按照“分区、分级、分域”总体安全防护策略，执行信息系统安全等级保护制度。

第三条 信息安全管理工作总体目标是：保护全市政府网站及政务新媒体系统的硬件、软件、业务信息和数据、通信网络设备等资源的安全，有效防范各类安全事故，深入推进政府网站创新发展，确保为社会提供高效稳定的政务服务。

第四条 本办法适用于指导全市政府网站及政务新媒体信息系统资产和信息技术人员的安全管理，适用于指导全市政府网站

及政务新媒体系统安全策略的制定、安全方案的规划和安全建设的实施。

第五条 本办法的编制参照了以下国家标准:

《信息安全技术信息系统安全等级保护体系框架》（GA/T 708-2007）

《信息安全技术信息系统安全管理要求》（GB/T 20269-2006 ）

《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2008）

第二章　信息安全组织管理

第六条 政府网站信息系统安全人员包括信息系统安全责任人和维护人。

安全责任人职责: 负责管理网络设备、服务器以及安全设备，作为底层系统的安全责任人。信息部门可指派网络管理员、服务器管理员、安全设备管理员负责相应的资产；负责管理具体业务系统的运行和数据资源的安全性，作为业务系统数据资产的安全负责人；负责基于业务使用需要，分配必要的访问权限；每年需要审查资产的访问权限。

安全维护人职责: 负责支持和维护网络与信息资产安全运行；根据所保管信息的保密类别来确定相应实物资产的安全管理流

程，包括物理保护及程序性保护，以确保网络与信息资产责任人所要求的机密性、完整性和可用性；确保适当的安全措施到位，并可以适度向下委派。如若需要，可以确定备用联络人；负责妥善保管责任人的名单，并应通知责任人其所应承担的安全职责。

第七条 政府网站信息系统工作人员设立以下岗位角色，分别负责不同的工作内容，确保信息系统的安全运行，具体岗位和安全职责如下：

1. 安全主管。其安全职责包括：建设信息安全管理体系和技术保障体系；制定或修订现有信息安全管理政策、制度与流程，规范信息技术应用的安全规格和标准；监督并控制信息安全风险，预防并处理信息安全事件，杜绝重大信息安全事故的发生；负责信息安全技术及相关产品及项目的引入实施和运营维护；负责对整体信息架构安全隐患地挖掘、追踪与消除，对信息安全问题导致的紧急与突发事件制定应急预案，并做好预防性措施及定期演练；定期进行安全审计，并协助安全事件的调查，定期组织信息安全技术培训，完善信息安全知识库、工具建设；敏锐感知行业信息安全最新动态，了解前沿信息安全管理政策，定期发出信息安全公告。

2. 安全管理员。其安全职责包括：负责信息安全工作的具体实施和有关信息安全问题的处理，根据信息安全事件的处理情况和对网络系统安全检测的结果，提交事件处理报告；根据网络系统安全需求，定期提出网络系统安全整改意见，上报信息安全

领导小组；组织定期的信息安全巡检，并在其他管理员的协助下建立完整的安全巡检报告，及时向信息安全工作组提交报告，汇报网络的信息安全现状；指导和监督其他管理员和普通用户与安全相关的工作，为他们的安全改进提供建议；监控信息系统的安全需求变化，及时获取来自其他管理员和普通用户的安全意见，进行必要的安全策略体系修订；处理信息安全领导小组核准的其它事务。

3. 网络管理员。其安全职责包括：负责对所管理网络设备的日常运行、管理和维护，保持系统处于良好的运行状态；接受安全管理员的安全整改建议，对网络设备进行必要的安全性增强；参加定期的信息安全巡检，并记录巡检结果，在巡检结束后提交给安全管理员，配合安全管理员完成信息安全巡检报告；在每个网络系统工程验收后，应对工程所涉及的网络设备、网络服务作相应的安全设置，删除设备的测试账号，对需要保留的账号口令重新进行设置，并且在口令的设置上要符合保密性要求；编制网络设备的维修、报损、报废计划，报上级相关部门审核；监控信息系统的安全需求变化，及时获取来自其他管理员和普通用户的安全意见，进行必要的安全策略体系修订；处理信息安全领导小组核准的其它事务。

4. 系统管理员。其安全职责包括：负责对所管理的主机系统的日常运行、管理和维护，保持系统处于良好的运行状态；接受安全管理员的安全整改建议，对主机系统进行必要的安全性增

强；参加定期的信息安全巡检，并记录巡检结果，在巡检结束后提交给安全管理员，配合安全管理员完成信息安全巡检报告；在每个网络系统工程验收后，对工程所涉及的主机系统作相应的安全设置，删除系统的测试账号，对需要保留的账号口令重新进行设置，并且在口令的设置上要符合保密性要求；编制计算机设备的维修、报损、报废计划，报相关部门审核；监控信息系统的安全需求变化，及时获取来自其他管理员和普通用户的安全意见，进行必要的安全策略体系修订；处理信息安全领导小组核准的其它事务。

5. 数据库管理员。其安全职责包括：数据库管理员全面负责数据库系统的管理工作，保证其安全、可靠、正常运行；负责数据库服务器的管理工作，做好服务器的运行记录，当服务器出现故障时，迅速会同相关人员一同解决；负责数据库系统的建设，做好服务器的维护、数据库软件的安装、数据库的建立工作，定期对数据进行备份；负责数据库服务器的安全防范管理工作；协助软件开发人员完成数据库软件开发所需的各类数据库的信息。

6. 审计员。其安全职责包括：监督信息部门对各项信息安全规章制度的执行，并对关键文件进行备份，及时查处安全隐患；负责对整个信息系统进行安全审计，对安全管理员做的安全评估报告进行审计；负责做好有关审计资料原始调查的收集、整理、建档工作，按规定保守秘密和保护当事人合法权益；在安全审计过程中，详细记载发生异常时的现象、时间和处理方式，并及时

上报；负责对所有涉及的审计事项，编写内部审计报告，及时报主管领导审核，并提交处理意见和建议；负责参与网络安全事故调查，对于由于安全审计员工作疏忽或失误而产生的安全事故，应追究其相应责任。

7. 应用管理员。其安全职责包括：负责对所管理业务应用系统的日常运行、管理和维护，保持系统处于良好的运行状态；接受安全管理员的安全整改建议，对应用系统进行必要的安全性增强；参加定期的信息安全巡检，并记录巡检结果，在巡检结束后提交给安全管理员，配合安全管理员完成信息安全巡检报告；在每个业务应用系统工程验收后，对工程所涉及的业务应用系统作相应的安全设置，删除系统的测试账号，对需要保留的账号口令重新进行设置，并且在口令的设置上要符合保密性要求；监控信息系统的安全需求变化，及时获取来自其他管理员和普通用户的安全意见，进行必要的安全策略体系修订；处理信息安全领导小组核准的其它事务。

8. 资料管理员。其安全职责包括：存放收藏每天运营生产系统的数据备份资料载体及产生的相关书面文档；信息系统方案文档（施工规划、网络设计、软件设计、硬件设计、安全设计、网络拓扑、网络布线、技术参数等）的整理收藏工作；每月进行计算机软件载体（光盘、软盘等）以及软件（自行开发的软件源代码、软件设计书、使用说明书等）资料清点工作；机房的软硬件系统、设备的技术资料（产品手册、使用手册、相关单据）整

理汇总保管；其他有关的文档管理（各种工作规章制度、个人工作日志、培训计划、办公文件归档等）；处理信息安全领导小组核准的其它事务。

9. 终端人员。其安全职责包括：配合安全管理员进行终端的安全检查和安全加固工作；严格遵循各项信息安全管理制度的相关安全要求；配合信息安全巡检，完成信息安全检查工作。

第三章　日常信息安全管理

第八条 信息安全管理人员和信息安全技术人员上岗前必须经单位人事部门进行政治素质审查，应当政治可靠、业务素质高、遵纪守法、恪尽职守，技术部门进行业务技能考核，工作经历和工作经验考查等，合格者方可上岗。违反国家法律、法规和行业规章受到处罚的人员，不得从事信息安全管理与技术工作。

第九条 信息安全管理人员和信息安全技术人员接受外部邀请进行演讲、交流或授课，应事先征得单位批准，并就可能涉及的有关单位业务的重要内容征求领导意见。

第十条 网站信息安全人员的配备和变更情况，应向上一级单位报告、备案。信息安全人员调离岗位，也必须严格办理调离备案手续，承诺其调离后的保密义务。涉及单位业务核心技术的信息安全人员调离单位，必须进行离岗审核，并在规定的脱密期后，方可调离。

第十一条 信息资产包括：硬件、软件、数据（电子数据）、文档（纸质文件）、人员、服务设施、其他。 软件、硬件设施、服务性设施等的获得主要以采购的方式获得，采购按照有关规定进行采购和验收。数据信息资产的获得来源主要为外包供应商、市场信息、其他信息。所有软、硬件资产必须明确使用人员、管理人员，明确职责。建立严格完整的购置、移交、使用、维护、维修和报废等记录，认真做好资产登记和管理工作，保证资产管理的正规化。

第十二条 各地各部门要根据业务流程列出信息资产清单，并将每项资产的资产类别、信息资产编号、资产现有编号、资产名称、所属部门（组别）、管理者、使用者、地点等相关信息记录在资产清单上。

第十三条 按照信息资产的公开和敏感程度，将信息资产化分为不同的保护等级，并对不同等级的信息资产进行保护，确保信息安全。各单位要将所有的移动介质和电子文件按照敏感性和重要程度分为不同的保护等级、保密级别与保密期限。

第十四条 硬件资产处置和存储设备销毁前，必须确保所有存储的敏感数据或授权软件已经被移除或安全重写；服务器、主要网络设备的处置要进行安全处理；台式机、打印机、传真机、扫描仪等 IT 设备的处置要做登记；如需报废时，应向主管部门提出报废申请，经批准后报废。

第十五条 软件资产安装软件时要规定使用权限，防止非授

权访问；工作人员离职或岗位变动，需要回收有关的软件，必要时由技术人员对离职人员使用的软件进行卸载删除。对过时或确认无效的软件资产，定期进行清除。

第十六条 设备的选址应采取控制措施以减小潜在物理威胁的风险，例如偷窃、火灾、爆炸、烟雾、水（或供水故障）、温度、湿度、尘埃、振动、化学影响、电源干扰、通信干扰、电磁辐射和故意破坏。

第十七条 数据库服务器所放置的场所应在电源、空调、温度、空气湿度、通风条件、防水防尘防雷防震防静电等方面均满足计算机机房的规范要求以及服务器本身的场所要求，置于单独的服务器区域。数据库服务器所在的服务器区域边界应部署防火墙或其它逻辑隔离。设备储存环境要符合出厂标准要求，安全产品及保密设备必须单独储存并有相应的保护措施。

第十八条 由责任人负责进行设备的日常清洗及定期保养维护，做好维护记录，保证设备处于最佳状态。一旦设备出现故障，管理员如实填写故障报告，通知有关人员处理。设备由专人负责维修，并建立满足正常运行最低要求的易损件备件库。

第十九条 根据每台设备的使用情况及系统的可靠性等级，制定预防性维修计划。对系统进行维修时必须采取数据保护措施，安全设备维修时应有安全管理员在场。设备进行维修时必须记录维修对象、故障原因、排除方法、主要维修过程及维修有关情况等。

第二十条 应优先选用我国自主研发的信息安全技术和设备。如需采用境外信息安全产品时，必须确保产品获得我国权威机构的认证测试和销售许可证。使用经国家密码管理部门批准和认可的国内密码技术及相关产品。终端物理隔离必须使用国家保密局认可的隔离卡或采用国家保密局认可的其他方式。

第二十一条 严格按照相关规定，规范政府网站相关信息系统建设项目规划、立项、审批、外包、实施、验收全流程，由专人负责项目全过程中的管理，并留存相关文档。

第四章　信息安全防护管理

第二十二条 网络维护人员至少每天 1 次对所有网络设备进行检查，确保各设备都能正常工作。

第二十三条 网络维护人员应尽可能减少网络设备的远程管理方式，例如 Telnet、web、SNMP 等；如果的确需要进行远程管理，应使用 SSH 代替 Telnet，使用 HTTPS 代替 HTTP，并且限定远程登录的超时时间，远程管理的用户数量，远程管理的终端 IP 地址，同时按照“网络安全配置管理策略”中的规定进行严格的身份认证和访问权限的授予，并在配置完后，立刻关闭此类远程连接；应尽可能避免使用 SNMP 协议进行管理，如果的确需要，应使用 V3 版本替代 V1、V2 版本，并启用 MD5 等验证功能；进行远程管理时，应设置控制口和远程登录口的超时时

间，让控制口和远程登录口在空闲一定时间后自动断开。

第二十四条 软件更新或者补丁安装应尽量安排在非业务繁忙时段进行。操作必须由两人以上完成，由一人监督，另一人进行实际操作，并在升级（或修补）前后做好数据和软件的备份工作，同时将整个过程记录备案。软件更新或者补丁安装后网络维护人员应重新对系统进行安全设置，并进行系统的安全检查。

第二十五条 网络维护人员应及时报告任何已知的或可疑的信息安全问题、违规行为或紧急安全事件，并在采取适当措施的同时，向信息管理处领导报告细节；不得试图干扰、防止、阻碍或劝阻其他员工报告此类事件；同时禁止以任何形式报复或调查此类事件的个人。

第二十六条 网络维护人员应制订网络设备日志的管理制度，对于日志功能的启用，日志记录的内容，日志的管理形式，日志的审查分析做明确的规定。对于重要网络设备，应建立集中的日志管理服务器，实现对重要网络设备日志的统一管理，以利于对网络设备日志的审查分析。网络维护人员应至少每年 1 次对整个网络进行灾难影响分析，并进行灾难恢复演习。

第二十七条 对服务器系统进行升级维护时，要首先备份操作系统和数据库，避免由于升级失败导致系统无法恢复，影响业务系统的正常运行。

第二十八条 依据最小权限原则，对服务器进行安全优化与配置。应保持服务器应用系统正常运行所需的最小服务，以及客

户端对服务正常访问所需的最小网络及系统权限。

第二十九条 对服务器应定期进行安全评估，及时发现最新安全漏洞与异常。根据安全评估结果，定期对服务器进行安全加固和优化配置。任何新的服务器系统投入运行前，首先进行安全评估及优化，以保证其安全性。

第三十条 系统维护人员应禁止不被系统明确使用的服务、协议和设备的特性，避免使用不安全的服务，例如: SNMP、RPC、Telnet、Finger、Echo、Chargen、Remote Registry、Time、NIS、NFS、R 系列服务等。

第三十一条 系统维护人员应严格控制重要文件的许可权和拥有权，重要的数据应当加密存放在主机上，取消匿名 FTP 访问，并合理使用信任关系。

第三十二条 系统维护人员应及时报告任何已知的或可疑的信息安全问题、违规行为或紧急安全事件，并在采取适当措施的同时，向主管领导报告细节；不得试图干扰、防止、阻碍或劝阻其他员工报告此类事件；同时禁止以任何形式报复或调查此类事件的个人。

第三十三条 系统维护人员应保证各主机设备的系统日志处于运行状态，并每两周对日志做一次全面的分析，对登录的用户、登录时间、所做的配置和操作做检查，在发现有异常的现象时应及时向信息安全领导小组报告。

第三十四条 系统维护人员应通过各种手段监控主机系统的

CPU 利用率、进程、内存和启动脚本等的使用状况，在发现异常系统进程或者系统进程数量异常变化时，或者 CPU 利用率、内存占用量等突然异常时，应立即上报主管领导，并同时采取适当控制措施，并记录备案。

第三十五条 当主机系统出现以下现象之一时，系统维护人员必须进行安全问题的报告和诊断:

1. 系统中出现异常系统进程或者系统进程数量有异常变化;

2. 系统突然不明原因的性能下降;

3. 系统不明原因的重新启动;

4. 系统崩溃，不能正常启动;

5. 系统中出现异常的系统账号;

6. 系统账号口令突然失控;

7. 系统账号权限发生不明变化;

8. 系统出现来源不明的文件;

9. 系统中文件出现不明原因的改动;

10. 系统时钟出现不明原因的改变;

11. 系统日志中出现非正常时间系统登录,或有不明 IP 地址的系统登录;

12. 发现系统不明原因的在扫描网络上其它主机。

第三十六条 系统服务器至少每月做一次系统备份，每周做一次增量备份; 每个服务器至少保持最近三个月的系统和数据备份，以确保信息安全。

第三十七条 计算机必须设置开机密码、管理员密码，开机密码由计算机安全员设置，管理员密码由计算机信息系统管理员设置，密码不得少于8位，并定期进行变更，密码不得告诉他人，不得窃取或擅自使用他人的密码查阅相关的信息。

第三十八条 口令设置权限要求：口令必须符合复杂性要求，禁止使用名字、姓氏、电话号码、生日等容易猜测的字符作为口令，也不要使用单个单词或命令作为口令，组成口令的字符应包含大小写英文字母、数字、标点、控制字符等，口令长度要求在8位以上；不应将口令存放在个人计算机文件中，或写到容易被其它人获取的地方。口令文件（如：系统中的/etc/shadow）及其所有拷贝的访问权限应该严格限制为超级用户可读，并且定期检查；对于重要的主机系统，要求至少每个月修改一次口令，或者使用一次性口令设备；对于管理用的工作站和个人计算机，要求至少每两个月修改一次口令；若掌握口令的管理人员调离本职工作时，必须立即更改所有相关口令；应用系统、邮箱的用户名和密码由系统管理员统一设定，由系统管理员登记并请用户确认（书面或电话通知），并保存用户档案；当用户忘记口令时，需本人向有关部门提交申请单，按照所规定的手续，对该用户口令进行重置；如发现口令泄漏，系统管理员要立刻更换密码并报告部门负责人，由部门负责人报告上级领导，同时要保护好现场并记录。

第三十九条 基于不同业务的需求对访问政府网站信息系统

资源的用户分别建立用户账户的授予与撤销的管理措施和执行过程；授予用户的身份是唯一的，不允许多人共享一个账户；对重要资源的访问保证有足够的口令强度和防攻击能力，用户必须使用符合安全要求的口令，并妥善保护口令；数据库服务器要实现操作系统和数据库系统管理员的权限分离，由不同人员分别担任数据库系统管理员和操作系统管理员，避免直接管理的情况；依据权限最小原则，对系统当前用户进行权限限制。

第四十条 安全策略要周期性的有更新，并且有更新记录，如服务器修补补丁和漏洞的情况，linux 服务器每周至少升级一次，windows 服务器每周至少升级 2 次；安全策略至少应该包括使用服务器服务的方式、服务器数据备份策略、口令策略，入侵者检测和系统防止攻击的策略等。

第四十一条 各地区各部门应按照计算机信息系统安全保护等级标准，盟市级政府门户网站定为三级并每年进行一次系统安全等级保护测评备案，旗县市区和市政府各委办局网站定为二级并每两年进行一次系统安全等级保护测评备案。

第四十二条 各级政务新媒体应严格执行网络安全法等法律法规和有关政策规定，认真履行信息安全主体责任和数据安全保护义务，建立健全安全管理、保密审查和应急预案，落实安全管理责任，做好平台运维操作权限管理设置、日志记录和安全审计、数据加密、数据脱敏、访问控制、数据容灾备份等措施，落

实数据备案管理、事件通报、溯源核查、技术检测和安全认证等工作，提高安全防护能力。

第四十三条 政务新媒体工作应当配置专用设备，做到专机专用、专人专用，严禁安装与工作无关的软件，严禁接入不明网络。强化账号密码管理，每 3 个月变更一次政务新媒体密码。密码设置须具备一定的复杂性和强度，至少包含数字、小写字母、大写字母、特殊符号中的 3 种，管理人员变动后应及时变更密码，收回权限及所配设备。不得在网吧等公共场所或没有安全保障的设备上登录账号，不得使用自动登录模式，不使用账号时必须及时退出登录，防止账号被盗用或被恶意攻击等安全事故发生。

第四十四条 各级政务新媒体应定期开展平台应用程序、操作系统以及数据库的安全检查，实时监测软硬件环境、应用系统等运行状态以及政务新媒体挂马、内容篡改等受攻击情况，及时处置安全风险，做好备份、恢复、容灾和安全认证管理工作。

第四十五条 政务新媒体服务器不得放在境外，禁止使用境外机构提供的物理服务器和虚拟主机。涉及本地本部门数据服务的政务移动客户端等应用系统类政务新媒体服务器，原则上设置在本自治区内，实行本地化管理。

第四十六条 介质的使用和管理：

1. 涉密存储介质应根据所存储信息的最高密级划定密级，并在明显位置粘贴密级标识，禁止使用无标识的存储介质。涉密存储介质严禁在联接互联网的计算机和非涉密计算机上使用；

2. 在涉密信息系统内使用的涉密存储介质采取绑定或有效的技术接入控制措施，使涉密存储介质只能在授权的涉密计算机上使用。未采用绑定技术的涉密计算机，须采取关闭和监控数据端口（USB 口）的物理防护措施进行控制;

3. 严格控制其它存储介质的使用，对光盘、软盘等移动存储介质应采用关闭数据接口或禁止驱动设备使用等方式加以控制;

4. 禁止在低密级计算机上使用高密级存储介质，禁止在低密级存储介质上存储高密级信息;

5. 高密级存储介质用于存储低密级信息时，应当按照存储介质原标识的高密级进行管理;

6. 存放涉密存储介质的场所、部位和设备应符合安全保密要求，集中统一管理;

7. 发现存储介质丢失，应立即报告本部门、单位和相关部门，并及时组织查处。

第四十七条 电子数据的使用和处置:

1. 对所有电子数据进行分类、分级，标识未授权人员的访问限制，不同安全级别的数据应存储在不同的区域，按类按级传达;

2. 不同类型的电子文件按照统一规律存放在个人电脑或服务器中，并定期进行备份;

3. 对于存于服务器上的电子数据的访问，根据服务器提供

服务的不同，设置不同的访问权限，避免非授权访问;

4. 对于内部公开级别的电子信息，其使用要控制在内部，禁止带出;

5. 对于秘密级别以上的电子文件的处理过程，必须保障数据的完整性、机密性和可用性;

6. 对于秘密级别以上的电子文件的使用，系统应进行审计;

7. 对于秘密级别以上的电子文件的传输，必须采取适当的安全措施加以保护，如加密传输、分散传输等;

8. 在整理电脑中的电子数据时，要小心操作，确认后再进行处理，避免由于误操作将有用的电子数据删除。

第四十八条 对计算机病毒与黑客的防范应以预防为主，事后处理为辅。工作中应贯彻“谁主管、谁负责，谁使用、谁负责”的安全责任制。

第四十九条 各地各部门分管领导担任本单位防病毒工作的第一责任人，制定本单位计算机病毒防治工作策略，并指定专人担任安全专员，负责计算机病毒防治工作的具体实施；计算机使用者应负责其所使用、管理的计算机的病毒防范工作。

第五十条 所有上网的计算机（含服务器）都必须安装使用通过国家公安部认证的正版防病毒软件，并且保证在开机状态下防病毒软件处于监控运行状态。

第五十一条 防病毒软件的升级频率不得低于每周 1 次；设置防病毒软件定时扫描功能，至少每周 1 次对计算机全部磁盘进

行病毒扫描。

第五十二条 及时更新操作系统安全补丁，执行相关操作系统的安装规范，设置系统安全策略，关闭不需要的服务，并开启安全审计功能。

第五十三条 经远程通讯传送、从互联网下载及其它外来的数据、程序，必须经过防病毒软件检测确认无病毒后方可使用。

第五十四条 如果发现计算机感染病毒，应将受感染的计算机与计算机网络隔离，防止病毒扩散，同时迅速对网络和所有计算机进行查毒。

第五章　信息安全教育培训

第五十五条 人员安全教育培训分为新员工培训和在职培训两大类。新员工培训是专门对新进员工举办，旨在帮助新进员工了解单位信息安全情况和信息安全规章制度，尽快适应工作要求的培训，并将制度掌握及执行情况纳入试用期考核。在职培训指不脱离工作岗位，在工作中接受的培训。旨在提高员工信息安全技能和综合素质，满足单位信息安全不断发展的需求。

第五十六条 信息安全教育培训可根据实际情况组织实施，所涉及的地区和部门必须予以配合并执行。全市政府网站信息安全工作人员均有接受相关培训的权利和义务，必须按规定参加培训活动，严格遵守培训规范。全市政府网站信息安全教育培训每

年至少 1 次。

第六章　信息安全检查

第五十七条 信息安全检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况和单位、部门自查结果等。安全检查至少每年组织 1 次。

第五十八条 信息安全自查内容包括系统的安全状态检查、安全管理制度及措施的落实情况检查等，自查工作应保留自查结果。自查至少每年组织 1 次。

第五十九条 信息安全检查和自查均应在检查之前形成检查表，严格按照检查表实施检查，检查完毕记录下所有检查结果，检查记录需经受检单位签字认可；检查记录要进行归档，只有授权人员可以访问阅读；检查结果要进行汇总分析，形成安全检查报告，报告应对问题进行分析，提出解决建议。安全检查报告至少每年组织 1 次。

第六十条 检查结果汇总后，应指派专人对检查情况进行记录、整理、分类情况进行审核，并对安全检查结果进行通报，限期整改。只对经过授权的人员通报安全检查结果。凡是查出的事故隐患，必须立即解决，防止事故发生。凡是已经发现的事故隐患，由于解决不及时而发生事故的，要追究负责人的责任并按规定处理。

第七章　附则

第六十一条 市政府办公室根据国家和自治区有关要求及工作推进需要，适时对政府网站信息安全管理办法的内容进行修改。

第六十二条 各旗县市区人民政府和市政府各部门在认真执行本办法的同时，可根据实际情况，进一步建立和完善本地区、本部门的各项安全管理制度。

第六十三条 本办法由市政府办公室负责解释，自印发之日起施行。《通辽市政府信息安全管理办法》（通政办字〔2018〕219号）同时废止。