**衡阳市政务信息资源安全管理规定**

**第一章 总则**

**第一条** 为加强对全市各级行政机关、事业单位和群团组织（以下统称各单位）政务信息资源的安全管理，确保网络数据信息的安全，根据《衡阳市政务信息资源共享管理暂行办法》等有关规定，结合我市实际，制定本规定。

**第二条** 加强政务信息资源安全保护工作，目的是确定各单位信息系统正常运行，维护数据信息应用工作的正常开展，预防、打击利用或针对各单位信息系统数据进行违法犯罪活动的行为，提高各单位信息系统数据整体安全水平，降低数据被非法生成、变更、泄露、丢失及破坏的风险。

**第三条** 本规定中所指政务信息资源是各单位在工作过程中收集、整理、更新和维护的各种业务数据的集合。包括各单位为履行政务职能而采集、加工、使用的数据，各单位在办理业务和事项过程中产生和生成的数据，以及各单位直接管理的数据等。

**第四条** 各单位政务信息资源安全保护工作应按照“谁主管、谁负责、预防为主、综合治理、制度防范与技术防范相结合”的原则，逐级建立数据安全管理领导问责制和岗位责任制，加强制度建设，逐步实现数据安全管理的科学化、规范化。

**第五条** 各单位政务信息资源实行安全等级保护，信息系统数据的建设和存储应符合相应的安全等级标准，使用的安全产品必须具有《计算机信息系统安全专用产品销售许可证》，其登记应与信息系统数据确定的安全等级相适应。

**第二章 组织管理**

**第六条** 各单位“一把手”是政务信息资源安全第一责任人。成立以分管领导为组长的政务信息资源安全管理小组，全面负责本单位信息系统数据安全管理工作。

**第七条** 政务信息资源安全管理小组负责确定本单位数据安全等级，并组织有关人员制定、评审本单位信息系统数据安全策略、安全标准、安全工作流程和各项规章制度。

**第八条** 政务信息资源安全管理小组依据本规定，定期对本单位信息系统数据安全情况进行检查、考核。对于存在数据安全隐患部门，协助提出整改方案，限期整改。因不及时整改而发生重大案件和事故的，由该部门的有关责任人承担责任；对违反国家相关法律法规的，由公安机关进行处罚；构成犯罪的，由司法机关依法追究刑事责任。

**第九条** 各单位要设立专职政务信息资源安全管理人员，数据安全管理人职责是按照安全管理工作流程和规范，执行各项数据安全管理操作任务，保障本单位各项数据的安全。

**第三章 信息系统安全管理**

**第十条** 各单位的信息系统上线使用前，要向政务信息资源安全管理小组申请安全检查与系统备案登记，确定系统安全登记，指定政务信息资源安全责任人。

**第十一条** 信息系统必须使用正版软件，并及时进行系统升级或更新补丁；信息系统必须装了防毒杀毒软件，并定期进行病毒检查；与互联网相连的信息系统要有防止非法入侵防护及措施。

**第十二条** 信息系统必须有全面、规范、严格的用户管理策略或办法。重要的信息系统必须有双人互备作为系统管理员。系统管理员必须对信息系统的各种服务器加设口令，严禁采用系统默认超级管理员用户名和口令；由系统管理员对用户实行集中管理，对用户按职能分组管理，设定用户访问权限，严禁跨岗位越权操作；严防非法用户或非授权用户对非授权服务、数据及文件的访问、使用和修改等。对信息系统的用户身份、主机身份等进行安全审计，并留存审计日志，审计日志应进行妥善保存。

**第十三条** 信息系统的主要软件、数据等要有完整可靠的备份机制和手段。并具有在要求时间内恢复系统功能以及重要数据的能力。对重要信息系统及设备要有应急处理预案，政务信息资源安全管理小组要对应急预案备案登记，并定期或不定期举行数据安全应急演习。

**第十四条** 信息系统主机或存储设备发生故障时，要尽量现场维修，系统管理员要在现场监督；确实需要送出维修时，注意去掉存储部件或删除数据。

**第十五条** 严格信息系统客户机接入管理。只有经过系统管理员批准并进行安全登记备案的计算机才能接入信息系统。严禁未经批准接入外来笔记本电脑、计算机系统或其他配件。

**第四章 网络安全管理**

**第十六条** 坚持“涉密计算机不上互联网，非涉密计算机不处理涉密信息”的原则。涉及国家秘密的信息系统，不得直接或间接地与互联网或其他公共信息网络相连接，也不得与业务内网相连接，必须实行物理隔离。

**第十七条** 对重要或涉密数据的存储和传输应进行加密处理。对重要或涉密数据的存储介质，应采取必要的安全保护措施，并建立相应的登记管理制度。对保密信息不得遗失、泄露。

**第十八条** 需接入互联网的计算机按正常程序申请，由本单位信息化主管部门分配相应的上网权限。杜绝以各种形式违规外连互联网。接入互联网的计算机应具备必要的防黑客攻击、防病毒以及过滤有害信息等安全技术措施。

**第十九条** 建立政务外网信息的监视、保存和备份制度，要有专人进行监视，并做好记录。

**第二十条** 任何单位和个人不得利用互联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

**第五章 数据维护及备份管理**

**第二十一条** 建立信息系统管理员制度，系统管理员承担系统的运行维护和数据的安全管理工作。并将数据安全管理方案、数据备份策略、管理流程和人员组织情况向本单位数据安全管理小组登记备案。

**第二十二条** 系统管理员要严格遵守数据备份策略，及时做好数据的备份工作。严格数据库管理员口令管理，要定期更换数据库管理员口令。系统每天应作数据库的增量备份，每周应作数据库的完全备份。重要数据读入系统后应及时备份。

**第二十三条** 数据备份采用在线存储与脱机介质两种形式进行双备份。一方面要将数据备份到非本机的存储设备上；另一方面备份到脱机介质上，脱机备份要实行本地与异地双存储。数据备份后要认真填写数据管理日志。

**第二十四条** 重要数据必须定期、完整、真实、准确地备份到不可更改的介质上，并要求做到集中和异地双备份保存。对长期保存的数据光盘等备份介质，应每年进行一次以上检查，以防止存储介质损坏造成损失。

**第二十五条** 系统出现故障和遭到破坏时，由系统管理员负责完成数据恢复工作，系统管理员必须保证备份数据能够及时、准确、完整地恢复。确因特殊原因不能恢复的，应及时向分管领导汇报，妥善处理。对数据的各项操作实行日志管理，严格监控操作过程，对发现的数据安全问题，要及时处理和上报。

**第二十六条** 未经批准，系统管理员不得直接对后台数据库进行数据更改操作。确实需要后台操作的，必须上报分管领导批准，并事先对数据库进行备份后进行，同时详细记录操作过程及数据更改情况以存档备查。

**第六章 人员管理**

**第二十七条** 建立政务信息资源安全管理人员的录用、考核制度，不能胜任工作的人员必须及时调离。政务信息资源管理人员应严格遵守软件的操作规范，离开操作岗位时，必须退出操作界面或锁定计算机，以防他人进行未经授权的操作。

**第二十八条** 政务信息资源安全管理员调离时，必须按规定移交全部技术资料和有关数据，设有口令密钥的要及时进行更换。涉及重要人员调离时，应确认对业务不会造成危害后方可调离。

**第二十九条** 政务信息资源安全管理人员必须遵守有关安全保密法律法规，应注意自己的用户名和口令的保密，并定期或不定期修改口令。如出现他人借用或盗用本人账号引起不良后果的，要按规定追究有关责任人的责任。

**第三十条** 发生重大事故，应当立即报告政务信息资源安全管理小组，发现相关违法、犯罪案件，须立即向公安机关报案。

**第七章 附则**

**第三十一条** 本规定由市电子政务管理办公室负责解释。

**第三十二条** 本规定自下发之日起执行。