附件

韶关市数字政府网络和数据安全体系建设总体规划（2023-2025年）

2023年10月

目　录

引　言

《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》明确提出：“提高数字政府建设水平。将数字技术广泛应用于政府管理服务，推动政府治理流程再造和模式优化，不断提高决策科学性和服务效率”。“十四五”时期是我国开启全面建设社会主义现代化国家新征程的重要开端，也是内外部环境继续发生深刻变化，机遇与挑战并存的时期。电子政务发展将进入“数据赋能、协同联动、服务优化、安全可控”的新阶段，引领国家治理体系和治理能力现代化迈上新征程。

数字政府必须安全、可靠、平稳的运行，才能有效的保障社会安稳，赢得民众的信任，促进数字经济的发展。为全面贯彻党的二十大关于“坚持以新安全格局保障新发展格局”的战略部署，深入贯彻落实习近平总书记对网络安全和信息化工作提出的“网络强国”“数字中国”的安全理念，按照《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》、《广东省电子政务外网网络安全管理办法》等法律法规的规定，结合《国务院关于加强数字政府建设的指导意见》、《广东“数字政府”改革建设方案》、《全国一体化政务大数据体系建设指南》、《广东省数字政府改革建设“十四五”规划》、《广东省数字政府省域治理“一网统管”三年行动计划》、

《广东省电子政务外网网络发展行动计划（2022-2023年）》，以及《韶关市“数字政府”改革建设方案》、《韶关市数字政府建设“十四五”规划》等政策文件要求，从安全管理、安全技术、安全运行、安全监督四大体系出发，厘清安全责任、制定总体架构、明确建设内容，构建全要素、多层次“安全可信、合规可控”的网络空间安全防护体系，充分保障韶关市数字政府在制度、业务、数据、运营、维护等各方面安全运行，制定本总体规划。

总体规划以韶关市数字政府安全体系建设需求为抓手，夯实数字政府建设安全基础，持续创新安全机制和管理体制，整合业内优势力量，推动多领域、多技术交叉融合，以“统筹、集约、动态、科学、可控”为理念，构建贯穿设计、建设、运营、管理、监督等不同阶段，覆盖基础设施、网络、系统、数据和平台等全要素空间的多层次、多维度、主被动相结合的网络空间安全体系，为韶关市数字政府网络和数据安全提供顶层设计，推动韶关市数字政府网络安全体系建设工作，为韶关市数字政府建设构建一个“更有效、更安全、更可持续”的未来。

一、 发展现状与挑战

（一）发展现状

1.数字政府基础设施不断夯实

（1）四级政务外网体系纵向到底、横向到边。

2018 年，我市根据国家和省关于做大做强政务外网的要求，进一步扩容提速和拓展延伸政务外网。目前，全市非涉密电子政务外网已经建成，统一了市县两级互联网出口；电子政务外网实现了上连省，横向连接党政机关、群团、党政直属事业单位等部门，下连 10 个县（市、区）和镇（街）村（居），基本形成了市县镇村四级电子政务外网网络体系，为各地各部门政务信息系统运行提供了可靠的网络基础条件。

目前，市级互联网出口带宽 2 G，接入市级部门 120 多个，接入计算机终端超 6000 台；市级骨干网带宽 10000M，市县骨干网带宽 100M，县镇村带宽不低于 40M，10 个县（市、区）、109 个镇（街道）、 935 个县（市、区）直属单位、1428 个村（居）全部接入电子政务外网，接入计算机终端超过 2 万台。

（2）数字政府政务云平台基本建成。

在政务云平台建设方面，2019 年，我市在省的大力支持下，建成了省数字政府政务云平台韶关节点，截至 2023 年 7 月 31 日，广东省数字政府政务云平台韶关节点共建设了 vCPU21504 核，内存 60.46TB，存储 3386TB，依托政务云平台，大力推动各地各单位政务信息系统迁移上云，迁移上云率超 85%。

（3）政务大数据中心初步建成。

2021年8月，我市积极争取省试点政策和资金支撑，在全省率先部署上线省市一体化政务大数据中心韶关节点，依托政务外网、政务云平台等基础资源，建成上连省、横向到部门，纵向到县（市、区）的数据交换共享高速公路，为全市各地各部门数据采集、传输、存储、交换提供便捷、高效、安全的基础支撑。自省政务大数据中心韶关分节点上线以来，共编制发布数据目录7342个，支撑全市620个用数申请单共4579个数据目录的交换共享，累计配置数据共享交换任务8000多个，汇聚视频数据12000多路。

2.数字政府安全管理不断完善

（1）安全制度体系建设持续完善。陆续出台了《韶关市电子政务外网网络安全管理办法》、《韶关市政务信息化服务项目管理办法》、《韶关市“数字政府”政务云管理办法（试行）》、《韶关市工程建设项目审批管理系统运行管理办法》等多项管理制度和指引，围绕政务云平台、政务外网、数字政府应用平台的安全管理，明确了各单位的安全职责，梳理了网络和数据安全防护基本要求、常见安全漏洞预防及处置方法，为各单位安全建设、安全管理、安全运营工作中提供参考；

（2）网络和数据安全情况纳入到绩效考核。将县（市、区）、市直各部门数字政府安全管理情况分别纳入年度数字政府落实情况考核指标、政务服务改革和数字政府建设情况逆向扣分指标，

督促各地各单位加强数字政府网络和数据安全建设管理。

3.数字政府安全体系初步建立

政务外网安全方面：基本建立政务外网边界防护体系。电子政务外网上部署有防火墙、入侵防御、堡垒机、上网行为管理、负载均衡器、VPN 等设备，构建了电子政务外网分区分域防护能力，降低了电子政务外网网络和数据安全风险。

政务云安全方面：初步建立政务云安全防护能力。广东数字政府政务云平台韶关节点按要求开展网络安全等级保护建设，通过了网络安全等级保护三级测评，为云上电子政务系统提供了基础云平台安全环境；建设了政务云平台韶关节点安全资源池，为各地各单位政务信息系统提供虚拟安全资源，满足了云上信息系统等级保护的要求，降低了云上业务系统安全风险。

数据安全方面：全面推进数据安全防护体系建设。构建数字政府政务云平台密码资源池，为各地各单位政务信息系统开展密码应用建设提供可靠的密码资源。依托数字政府政务云平台密码资源池，省政务大数据中心韶关分节点和韶关市大数据分析平台进行商用密码改造，通过了第三方商用密码应用评估。

4.数字政府安全运营初步构建

依托省市一体化安全运营平台，初步建立了韶关市数字政府网络数据安全运营体系。组建数字政府网络安全运营团队，团队成员多厂商融合，对数字政府政务云平台韶关节点进行安全事件监测及处置，常态化开展网络安全检查，督促各单位自行开展风

险评估（含等保测评、密码测评等）、基线核查、漏洞扫描、渗透测试，不断完善数字政府安全运营工作。

5.数字政府安全效果初现成效

经过各县（市、区）、市直各部门的共同努力，韶关市数字政府网络和数据安全水平有了明显改善，监测预警和应急处置能力得到进一步提升，安全效果工作初现成效。2022年，市委网络安全和信息化委员会办公室、市公安局及市政务服务数据管理局联合举办了“丹霞杯”网络安全攻防演练活动，2023年，东莞、韶关两市开展了网络安全联合攻防演练，有效检验了韶关市网络安全监测预警和应急处置机制，提升了网络安全日常监测和风险防范能力，锻炼了各地各单位的安全防护队伍，为有效地应对突发网络攻击事件积累了宝贵经验。

（二）主要问题及挑战

我市数字政府网络和数据安全建设取得了一定成绩，但综合当前数字政府网络和数据安全形式来看，仍面临着不少问题和挑战。

1.安全管理权责边界需厘清

一是数字政府建设采用“政企合作、管运分离”的建设模式，受人员和技术等方面限制，存在对建设运营单位安全防护方案设计细则、实施细节和安全风险把控不足的问题。二是对于云上托管业务和云下自运维业务的责任主体和权责不清晰，导致安全事件响应慢、难闭环的问题。三是部分单位履行网络和数据安全主

体责任不到位，错误认为信息系统迁到政务云平台后就安全了，出现安全问题由政数部门负责，从而对系统的安全不闻不问。四是各政府单位存在安全管理制度更新不及时、执行不到位、责任不明确等的安全管理问题。

2.安全防护技术体系待完善

数字政府建设前期工作主要集中于政务基础设施建设、政务服务建设等方面，网络和数据安全建设缺乏机构建立、力量配备、管理机制、监督机制等方面的顶层设计。集约化建设和系统上云所带来的新的安全问题如政务外网接入单位边界隔离、IP 和端口开放范围过大、云租户隔离、云上数据备份和容灾、数据共享难控制、政务终端安全事件难定位等问题，尚未有完整的解决方案，建设运营单位人员安全意识和安全管理能力还需进一步加强。

3.安全运营监管机制待建设

已初步构建了云、网、端的安全能力，但技术架构成熟度和整体安全防护能力有待加强，安全治理体系有待进一步完善，安全责任边界、安全机构协同联动、实战安全培训等方面还需进一步调整优化。一是政务外网信息资产采集、更新不及时。当前未形成有效的电子政务网信息资产动态更新机制，资产信息无法有效关联到责任人，仍存在部分僵尸及无人监管的资产，出现安全隐患处理效率低、难以快速定责。二是网络和数据安全风险监测能力待加强。已建安全运营平台只能对广东省数字政府政务云韶关节点进行监测，对自建电子政务云、政务外网出口、互联网出

口等未形成有效安全风险监测，网络和数据安全风险整体感知能力亟需加强。三是云网端未形成有效联动，常规安全风险需要大量时间进行分析处置，各安全设备之间存在“信息孤岛”，无法集中分析来自各层面的安全风险进行自动化决策处理。四是缺乏统一的安全监管体系，数字政府网络和数据安全主要依托建设运营单位，安全力量过于单一，过于依赖原有安全防护系统，对安全团队提出的安全方案,缺乏有效的第三方机构进行评审和监督。

4.安全监管运营水平仍需优化

一是安全运营覆盖面有待扩大。依托省市一体化安全运营平台，初步建立了数字政府政务云平台安全运营体系，开展了安全事件检查监测及处置，但暂未形成韶关市、县（市、区）一体化“云、网、数、端、应用”全流程安全运营机制，缺乏科学高效的网络和数据安全突发事件应急措施，应急响应相关规章制度不完备，应对突发事件相关保障准备工作不到位。二是缺乏统一的安全监管体系,数字政府网络和数据安全主要依托建设运营单位,安全力量单一，过于依赖原有安全防护系统，缺乏第三方机构对安全团队提出的安全方案进行评审和监督。

5.供应链安全管理机制待建立

供应链安全管理的重视程度不足，对数字政府咨询、设计、集成、运维、测评、改进等各环节供应商及采购的产品或服务的安全管理情况未能定期开展供应链风险评估及安全效果评价。一是全市未发布统一的供应链管理制度及评价办法，各单位缺少供

应链管理体系建设指引。二是未建立有效供应商服务安全监控和审计机制，主要依靠运维安全规范、人员保密协议进行约束，供应链风险无法有效溯源。三是未建立完善的供应商安全评价机制，供应商信息档案无法及时同步，潜在的供应商安全风险无法有效规避。

6.数据安全管理尚处起步阶段

我市已初步建成了省政务大数据中心韶关节点，根据省统一标准规范管理我市数据目录编制发布、数据申请、数据审批、数据交换等流程，制定省政务大数据中心韶关分节点角色申请、数据编目、数据申请等操作指引。全市公共数据开发共享工作已稳步推进，但数据安全防护体系建设处于起步阶段。一是本市各数源单位的数据梳理和数据编目挂接不充分，对数据分级分类不准确。二是共享数据的唯一性、真实性和可靠性缺乏完整的保障机制。三是缺乏数据脱敏、传输加密和加密存储等数据安全技术手段，易造成数据篡改和数据泄露等数据安全问题。四是数据使用安全监管还不到位，对数据使用单位、人员以及第三方公司针对获取的数据使用范围、用途、存储等行为的监管有所欠缺。

7.安全建设管理队伍待增强

数字政府改革建设专业性强、任务重，网络和数据安全建设管理尤其突出，市、县政务服务数据管理部门普遍存在专业网络安全人员缺乏、技术力量不足，专业支撑能力欠缺等问题，难以满足数字政府网络和数据安全建设管理需求，数字政府网络和数

据安全建设管理队伍不强与工作任务繁重的矛盾十分突出。

二、 总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想和党的二十大会议精神为指导，全面贯彻落实习近平总书记关于切实保障国家网络安全的重要批示指示精神，结合《广东省数字政府改革建设“十四五”规划》、《广东省“数字政府2.0”建设服务“百县千镇万村高质量发展工程”若干措施》、《韶关市数字政府改革建设“十四五”规划》等文件关于网络和数据安全建设要求，立足韶关市数字政府网络和数据安全工作实际，严格落实党委（党组）意识形态和网络安全工作责任制，全面提升韶关市数字政府网络和数据安全保障能力，助力韶关高质量发展。

（二）主要原则

1.统建统管、共建共治

落实数字政府网络和数据安全全市统筹的工作目标，坚持“一盘棋”机制，持续强化管理统筹、资金统筹、项目统筹、使用统筹等工作机制，强化顶层设计，统一规划部署，增强各地各单位的网络和数据安全责任意识。

2.系统布局、整体谋划

从数字政府网络和数据安全工作全局视角出发，充分分析总结网络和数据安全管理、建设、运行、监督等关键领域的深层次问题，积极引导和推动信创工作，整体谋划网络和数据安全工作，

全面落实数字政府网络和数据安全工作行动方向和重点任务。

3.协同实战、技管并重

提升网络和数据安全管理水平，强化网络和数据安全技术措施，建设网络和数据安全运营体系，明确网络和数据安全监管体系，重点突出网络和数据安全保障体系的实战能力与保障能力，实现网络和数据安全管理体系、技术体系、运营体系、监管体系的有效融合，有效保障网络和数据安全的可持续发展。

4.创新驱动、夯实基础

加强基础性、通用性、前瞻性网络和数据安全技术研究，加快关键核心技术攻关，激发网络数据安全技术创新动力，提升全市网络数据安全发展水平。

（三）参考依据

1.《中华人民共和国网络安全法》

2.《中华人民共和国数据安全法》

3.《中华人民共和国个人信息保护法》

4.《中华人民共和国密码法》

5.《关键信息基础设施安全保护条例》

6.《中共中央国务院关于加强网络安全和信息化工作的意见》（中发〔2017〕18号）

7.《关于加强数字政府建设的指导意见》

8.《全国一体化政务大数据体系建设指南》

9.《广东省公共数据管理办法》

10.《广东省国民经济和社会发展第十四个五年规划和2035年远景目标纲要》

11.《广东省数字政府改革建设“十四五”规划》

12.《广东省数字政府省域治理“一网统管”三年行动计划》

13.《广东省电子政务外网网络发展行动计划（2022-2023年）》

14.《2022广东省数字政府网络安全指数评估报告》

15.《韶关市数字政府建设“十四五”规划》

16.《2022年韶关市数字政府网络安全指数分析报告》

17.GB/T 37988-2019 《信息安全技术 数据安全能力成熟度模型》

18.GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

19.GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

20、GB/T 20273-2019 《信息安全技术 数据库管理系统通用安全技术要求》

21.GB/T28448—2019《信息安全技术 网络安全等级保护测评要求》

22.GB/T 37044-2018《信息安全技术 物联网安全参考模型及通用要求》

23.GB/T 36951-2018《信息安全技术 物联网感知终端应用安

全技术要求》

24.GB/T 35273-2017 《信息安全技术 个人信息安全规范》

25.GB/T 35274-2017 《信息安全技术 大数据服务安全能力要求》

26.《广东省数字政府网络安全指数指标体系》

27.《广东省数字政府电子政务外网管理办法》

（四）规划思路

构建覆盖“云、网、数、端、应用”等全要素空间的多层次、多维度、主被动相结合的网络和数据安全体系，促进网络和数据安全管理制度和标准规范建设，明晰网络和数据安全责任机制、责任主体、安全责任指标考核，提升韶关市数字政府安全运营能力，围绕以下四个体系，为稳步推进我市数字政府建设保驾护航。

1.巩固安全技术体系

近年来，韶关市数字政府政务云平台、政务应用和政务网络得到不断优化和完善，面临的网络和数据安全挑战也日益复杂，网络和数据安全技术体系仍待完善，依据韶关市网络和数据安全战略和规划，从基础设施安全、公共服务组件、终端安全、边界安全、数据安全、应用安全、云平台安全等维度深化网络和数据安全设计。

（1）基础设施安全

根据国家要求，采用国产化的服务器、操作系统等搭建国产化政务云，为业务系统国产化改造提供基础支撑，完善国产商用

密码在数字政府中的应用，保障数字政府安全自主可控。

（2）公共服务组件

面向韶关市政务外网终端接入认证、政务云平台用户的虚拟安全需求、政务外网各接入单位之间的安全隔离问题等共性安全问题，建立统一的公共安全服务中心，为终端访问、应用授权提供基础安全能力。

（3）终端安全

针对韶关市政务外网终端身份鉴别、访问控制、安全审计、恶意代码防范、统一管控平台、准入控制、终端安全管理、终端安全检测与响应和终端非法外联等问题，搭建完善的终端防护体系。

（4）边界安全

通过逻辑隔离、访问控制、安全检测、安全审计等手段保障各政务外网接入单位的边界安全。

（5）数据安全

在满足国家法律的同时以业务为出发点，通过数据资产梳理、数据安全风险评估、数据分级分类、数据全生命周期安全防护、数据隐私保护、数据安全治理等方面进行数据安全建设，保障数据的安全性。

（6）应用安全

针对政务外网的应用服务，提供漏洞发现、WEB 应用防护、网站安全监控防篡改等防护能力，重点解决 WEB 应用层攻击的检

测和防护问题。

（7）云租户安全

建设云平台安全资源池，为云租户提供相应的云平台安全服务，落实“安全管理责任不变，数据归属关系不变，安全管理标准不变”原则，实现云服务方和云租户在网络和数据安全责任的权责分离。

2.完善安全管理体系

加强网络和数据安全管理制度和标准规范建设，形成网络和数据安全管理制度和标准规范体系。制订电子政务外网网络安全管理办法、数字政府网络和数据安全指引、网络和数据安全总体策略、网络和数据安全风险评估管理等制度，制定网络和数据安全管理组织框架、网络和数据安全教育培训、第三方机构和人员安全管理、网络和数据安全检查及审核管理等制度，制定移动应用、云计算、数据安全、外部互联等安全管理标准规范，为我市数字政府建设提供安全制度保障。

3.构建安全运营体系

构建韶关市数字政府安全运营体系，构建云、网、数、端一体化的安全运营中心,结合省市一体化安全运营平台韶关分平台，实现自适应安全、智慧化安全体系的建设，持续检测网络内部安全威胁，构建“云网数端”协同联动机制，落实“谁主管谁负责、谁运行谁负责、属地管理”的要求，突出运营和监管两个职责。以风险管理为导向，以内控体系建设为核心，制定运营管理计划，

规范运营管理流程，推行可记录、可持续、可考核的运营管理方法，切实加强网络和数据安全运营。

4.加强安全监管体系

强化数字政府安全态势监管、保密监管、安全通报等机制建设，建立健全“事前、事中、事后”全程安全态势监管的联动机制，制定网络突发安全事件紧急处理预案，提高网络突发安全事件的应急处理能力；建立健全保密监管体系，加强对失窃泄密行为的监管，确保政府内部敏感信息不被扩散，保障数字政府运作的安全性和稳定性。

5.构建数据安全防护体系

随着“互联网+政务”的发展，政务数据种类和数目累计增加，相应的数据安全问题也变得日趋复杂化，单一的技术已难以应对。按照“自上而下”的数据安全治理体系以及数据安全能力成熟度模型；通过提升数据安全管理能力、数据安全技术能力、数据安全运营能力来提升整体数据安全能力成熟度，建立一套科学的数据安全实践体系。

（五）建设理念

统筹。强化数字政府安全顶层设计，将网络和数据安全纳入数字政府发展总体战略，与数字政府建设统一谋划、统一部署、统一推进、统一实施。突出重点，分步实施，积极稳妥推动规划落实。

集约。加强网络和数据安全需求分析和整体规划，充分利用、

合理整合现有韶关市数字政府网络和数据安全建设成果与资源，统一网络和数据安全基础设施建设，实现集约化、一体化建设。

动态。针对动态的数据资产与安全风险变化进行持续有效的监控与分析，建立健全“事前分析预警、事中响应防控、事后溯源取证”的全程安全监管机制。

科学。以数据安全为核心，科学规划云平台、数据、应用安全、终端安全策略和措施，采用先进的安全分析和方法论，明确韶关市数字政府安全建设中的重点方向，优先解决关键性的安全问题。

可控。加强数据安全和个人信息保护，增强互联网内容安全和政务数据安全，提高各重点领域的安全可控水平，加强要害信息系统和关键信息基础设施安全保障，确保安全可控。在信息安全技术和产品选型上坚持“安全自主可控”原则，实现核心安全技术和安全设备国产化，构建安全可控的网络和数据安全技术能力。

（六）发展目标

统一规划部署韶关市数字政府网络和数据安全体系总体架构，通过安全技术体系、安全管理体系、安全运营体系、安全监管体系建设，形成有效的安全防护能力、隐患发现能力、安全风险管理能力、应急响应能力，安全风险管理能力、应急响应能力和系统恢复能力，提高全天候、全方位安全保障能力，扎实筑牢数字政府安全防线。

1.全面提升安全运营能力

加强安全运营管理，构建全市业务链条网络和数据安全责任模型，将网络和数据安全责任、监督和激励等工作融入数字政府的业务体系；建立健全政务网络信息安全应急处置机制。

2.全面提升安全监管能力

建立健全保密监管体系，加强对失窃泄密行为的监管，确保政府内部敏感信息不被扩散，保障政府运作的安全性和稳定性；建立健全网络和数据安全监管体系，提高对网络犯罪行为的监管和打击能力，建立“事前、事中、事后”全程安全监督联动机制，提高网络和数据安全突发公共事件处置能力；建立健全内容安全监管体系，加强对全市政府网站和政务新媒体的检查监测，防止出现不当言论和有害信息。

3.全面提升安全管理能力

按照“边界明确、权责清晰”的安全管理要求，明确各参与方在数字政府安全工作中的责任分工，做到事事有章可循、件件有人负责，全面提升安全管理能力。

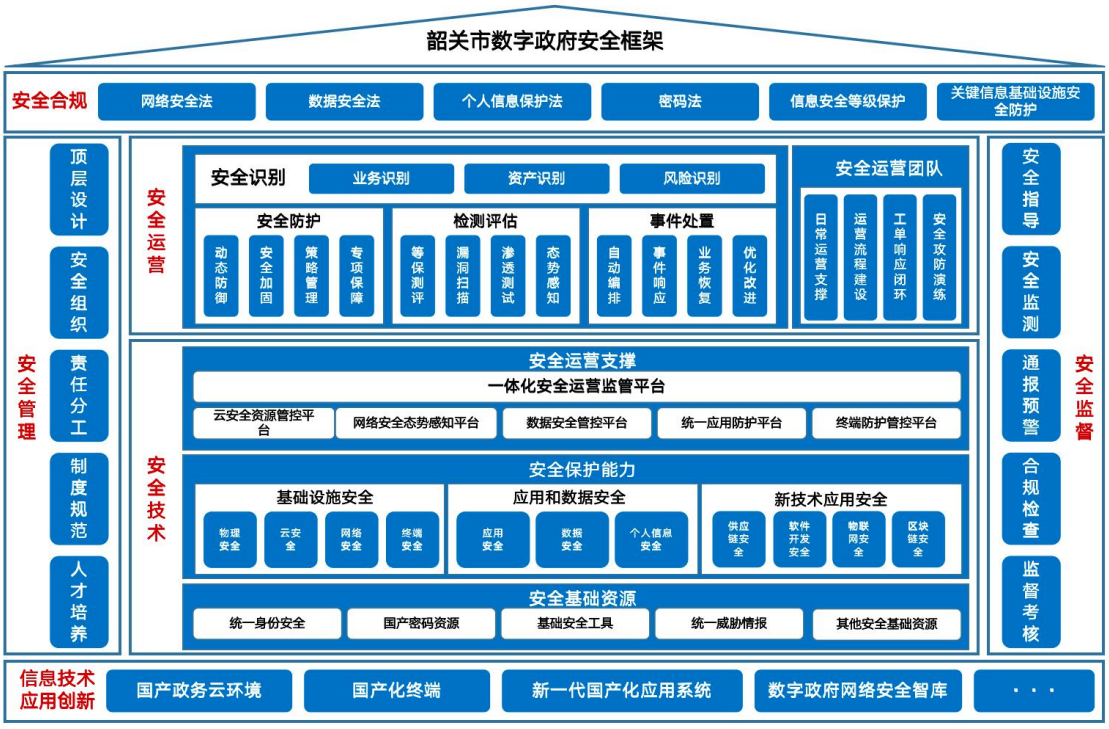
4.全面提升数据安全能力

保障政务数据的整体安全，确保政务数据能够为国家安全、社会稳定提供长效支撑,持续推动对政务数据安全风险进行分析，并在此基础上针对性地开展政务数据安全治理工作，全面提升政务数据安全能力。

三、我市数字政府网络和数据安全架构

（一）总体架构

为全面落实市委、市政府要求深入推进数字政府改革建设，发展数字经济，建设智慧城市的工作部署要求，充分依托市安全技术保障能力，以数字政府政务云平台和政务外网为底座，统一安全管理机制，以安全技术体系为支撑，以安全运营和安全监管为保障，打造覆盖“事前、事中、事后”的全周期防护，构建“安全可信、合规可控”的数字政府网络和数据安全支撑体系，保障我市数字政府安全高效的运行。



韶关市数字政府安全总体架构

（二）“四大体系”是核心

四大体系是数字政府安全建设的核心，包括“安全技术体系”、“安全管理体系”、“安全运营体系”、“安全监管体系”

四大安全体系，为韶关数字政府提供立体化安全保障。

安全技术体系：根据“立体防护、自主可控”的安全防护要求，强化数字政府安全的关键技术支撑，建立一套公共安全服务组件，构建覆盖基础设施安全、应用和数据安全、新技术应用安全的安全技术防护体系，提升数字政府的安全防护能力。

安全管理体系：承接“边界明确、权责清晰”的安全管理要求，完善安全组织架构，明确各参与方在数字政府安全工作中的责任分工，强化安全人员管理和培训，建立健全安全制度流程，提高安全管理水平，做到事事有章可循、件件有人负责。

安全运营体系：建设全面贯彻“安全运营闭环管理并基于数据分析为核心”的安全运营理念，面向“主动防御、实时预警”的安全要求，基于安全技术体系，提升安全识别、安全防护、事件响应与处置、安全分析与监测等安全服务水平，提供覆盖安全全生命周期的服务能力，形成预测预防、实时防护、持续监测、快速响应的闭环安全运营，保障数字政府稳定持续运行。

安全监管体系：对应“标准合规、强化红线”的安全保密要求，建立“业务监管与行业监管有机结合”的安全监管机制，加强安全指导、安全监测、通报预警和监督考核，建立技术平台提升安全监管的效率与能力，保障数字政府满足网络安全法、数据安全法、网络安全等级保护等标准法规要求。

（三）“应用业务、基础设施”是核心保护对象

基础设施层包含政务云、终端、应用系统、密码系统等，主

要提供底层云计算、云存储、云网络等基础设施以及基础服务，是数字政府的关键基础，是其他业务应用系统运行的根基。应用业务系统提供覆盖、汇聚和整合各县（市、区）的基础数据，包括人口库、法人库、社会信用信息库、自然资源和地理空间库等4大类公共基础数据库和各类主题数据库、专题库、分析库的基础数据，是数字政府核心政务数据的集合。政务应用覆盖民生、营商、政务等相关业务场景，是数字政府便利民生事项、优化营商环境、提升政府行政效率的关键载体。

四、建立网络和数据安全责任机制

（一）工作目标

严格落实党委（党组）意识形态和网络安全工作责任制及网络安全法的规定，按照“谁主管谁负责、属地管理”的原则，明确各级党委（党组）对本单位在数字政府中主管的政务网站、应用系统、网络、云平台、终端等的网络和数据安全主体责任。

（二）建设内容

市政务服务数据管理局对市级数字政府政务云平台、公共应用支撑平台、市电子政务办公业务系统集约化平台、市“一门式一网式”政务信息系统等统建系统负网络和数据安全主体责任；市直各部门对本部门的专业应用信息系统、政务网站、政务网络、政务终端等负网络和数据安全主体责任。各县（市、区）参照市级数字政府网络和数据安全工作责任制要求，落实本级主体责任。

市政务服务数据管理局统筹协调韶关市数字政府网络和数

据安全工作，加强纵向工作指导和横向工作协调，健全与县（市、区）和市直部门的工作统筹协调机制；负责制定网络和数据安全制度及规划，指导各县（市、区）和市直各部门制定具体要求和相关规划；负责建立健全网络和数据安全监管制度，自行或者委托网络安全服务机构对建设运营单位落实网络和数据安全保障措施情况进行监督；与市委网信办、市委机要和保密局、市公安局等部门建立安全管理联动和应急响应机制。

市直各部门负责制定、落实本部门网络和数据安全管理规范的具体细则，承担本部门专有业务系统及接入系统的网络终端、政务网站的网络和数据安全主体责任，参与制定安全管理规范。

市委网信办、市委机要和保密局、市公安局等部门在各自职责范围内负责相关网络和数据安全保护和监督管理工作。

数字政府建设运营单位负责对政务云平台以及在政务云上运行的信息系统等提供网络和数据安全保障服务，配备网络、系统、应用、大数据、云平台、管理等领域的专业人才队伍，负责日常安全保障、监测预警和应急响应。

1.建立数字政府关键信息基础设施安全保护机制

依照《关键信息基础设施安全保护条例》，在网络安全等级保护制度基础上，在识别认定、安全防护、检测评估、监测预警、应急处置五个环节做好关键信息基础设施安全保护工作。

市委网信办牵头统筹协调数字政府关键信息基础设施安全保护工作。市公安局、市通建办在各自职责范围内负责数字政府

关键信息基础设施安全保护和监督管理工作。市政务服务数据管理局会同市网信办、市公安局定期抽查各地各部门数字政府关键信息基础设施安全保护工作，指导督促问题整改，协调组织开展常态化网络安全攻防演练。

各县（市、区）和市直各部门对本地本部门主管的关键信息基础设施安全负主体责任，履行网络和数据安全保护义务。

各县（市、区）和市直各部门会同建设运营单位对本单位主管的关键信息基础设施开展识别和认定活动，围绕关键信息基础设施承载的关键业务，开展风险识别；根据已识别的安全风险，在规划、人员、数据、供应链等方面制定和实施适当的安全防护措施，确保关键信息基础设施的运行安全；制定相应的检测评估制度，根据检测评估、监测预警环节发现的问题，制定并实施适当的应对措施。

2.建立网络和数据安全工作应急响应机制

按照“统一领导、分级负责”“谁主管谁负责、谁运行谁负责”的原则，建立健全数字政府网络安全应急协调工作机制和网络安全信息通报工作制度，压实数字政府建设中的网络和数据安全主体责任，实现应急响应工作“统一指挥、密切协同、快速反应、科学处置”，切实提高数字政府网络和数据安全应急保障能力。

一是建立数字政府网络安全应急协调工作机制。建立市委网信办、市委机要和保密局、市公安局、市政务服务数据管理局等

部门的跨部门网络和数据安全应急联动处置机制，负责组织协调市级数字政府网络和数据安全应急响应工作。各县（市、区）参照建立相应的数字政府网络和数据安全应急指挥协调机构和跨部门联动处置机制。

二是建立数字政府网络和数据安全信息通报工作制度。建立市、县（市、区）数字政府网络和数据安全信息通报工作制度，各级政府部门要分别确定网络和数据安全分管领导与网络和数据安全具体负责人，明确本部门网络和数据安全责任，制定网络和数据安全应急预案，做好网络和数据安全事件的预防、监测、报告和应急处置工作，建立 24 小时通畅、可靠的网络和数据安全信息通报联络渠道。

五、健全网络和数据安全管理体系

（一）工作目标

通过构建涵盖设计、执行、监督三个维度的数字政府安全组织架构，强化安全人员管理和培训，明确各主体的责任分工，加强对人员的背景调查和安全保密管理，建立行之有效和及时响应的合规管理机制，建立确保网络和数据安全总体方针和安全策略实施的安全管理制度，完善我市数字政府网络和数据安全管理体系，提高安全管理水平。

（二）建设内容

1.加强网络和数据安全组织管理

数字政府安全组织由市“数字政府”暨“智慧城市”建设领

导小组、市“数字政府”暨智慧城市建设领导小组办公室、市直各部门安全管理部门、专家委员会、建设运营单位、第三方安全服务机构组成。

“数字政府”暨“智慧城市”建设领导小组为领导层，由市政府领导任组长，成员包括市直各部门领导;

“数字政府”暨“智慧城市”建设领导小组办公室为管理层，设在市政务服务数据管理局;

市直各部门、专家委员会、建设运营单位和第三方安全服务机构组成执行层。其中，“数字政府”暨“智慧城市”建设领导小组负责批准数字政府网络安全政策以及对重大事项进行决策。

“数字政府”暨“智慧城市”建设领导小组办公室负责统筹协调数字政府网络和数据安全工作，与市委网信办、市委机要和保密局、市公安局等部门建立安全管理联动和应急响应机制。

市直各部门安全管理部门负责本单位政务服务范畴的相关网络和数据安全保障工作。

专家委员会负责参与网络和数据安全政策及重要安全工作的审议，并提供专业咨询意见建议。

建设运营单位负责落实“数字政府”暨“智慧城市”建设领导小组办公室安全管理要求，接受监督管理。

第三方安全服务机构负责监督、评估、审计建设运营单位网络和数据安全工作落实情况。

2.加强网络和数据安全人员管理

划分人员工作岗位职能，明确安全职责义务，建立问责审查机制，设置人员管理流程，完善人员安全意识和教育制度，提升全员安全意识，落实人员背景调查和安全保密管理，签订安全保密协议，做好人员岗位管理和培训，承担网络和数据安全人员管理责任实现背景“干净”上岗、行为“干净”在岗、权限“干净”离岗。

3.加强网络和数据安全合规管理

建立一套及时响应的合规管理机制，在相关业务环节和内部运营流程中开展关键信息基础设施、网络安全等级保护等工作，以实现对云平台、大数据中心、业务应用的全生命周期安全防护。使数字政府的运作既符合网络和数据安全相关法律法规要求，又保证数字政府建立的安全管理制度得到有效执行。

4.健全网络和数据安全管理制度

依照网络安全相关法律法规要求，参考《国家电子政务外网信息安全标准体系框架》、《广东省电子政务外网网络安全管理办法》、《广东省数字政府电子政务外网管理办法》、《韶关市电子政务外网网络安全管理办法》等文件，结合我市网络和数据安全管理现状，建立健全韶关市数字政府网络和数据安全管理制度体系，为市直各部门、各县（市、区）在政务云、政务外网、业务应用、政务数据等方面的安全管理工作提供依据。

5.加强网络和数据安全风险管理

制定规划阶段风险处置方案，做好风险评估、风险处置计划

制定和风险接受的方案。做好实施阶段风险有效控制措施，要依据风险处置计划，实施将风险降低到可接受水平所需的行动和控制措施。修订检查阶段风险评估和方案，在“检查”阶段要根据事件和环境变化来确定风险评估和风险处置实施的效果做好处置风险阶段应对行动，在“处置”阶段要执行好应对风险所需的任何行动，包括风险管理过程的再次应用。

六、建设网络和数据安全技术体系

（一）工作目标

以保障韶关市数字政府快速、稳定的提供便捷服务为核心目的，构建韶关市数字政府网络和数据安全技术支撑体系，打造纵涵盖物理安全、终端安全、网络安全、平台安全、数据安全、应用安全的数字政府纵深安全防护体系，为数字政府共性安全需求提供能力支撑。

（二）建设内容

韶关市数字政府安全技术架构遵循“立体防护、纵深防御”的理念，采用自主、先进、成熟、可控的安全防护技术，通过物理安全、终端安全、网络安全、平台安全、数据安全、应用安全六个层次建立纵深防御体系。

1.建设公共安全服务中心

面向韶关市数字政府政务外网终端接入认证、政务云平台用户的虚拟安全、政务外网各接入单位之间的安全隔离、政务信息系统的商用密码等共性安全需求，建立一套统一的公共安全服务

组件，统筹规密码服务、云安全资源池、技术支撑等方面的公共服务安全能力。

（1）提供统一身份管理与认证服务

依托省统一身份平台，为数字政府应用系统提供基于安全措施的用户管理服务、身份认证服务、单点登录服务、数字证书服务、会话管理服务等接口服务，建立跨部门、跨系统、跨应用的统一身份标识，接入、整合多种认证方式和认证源，提供安全可靠、方便使用的多种身份认证方式，实现“一次注册、全网通行”。

（2）完善密码应用支撑体系

完善韶关市数字政府密码应用支撑体系，包括国产密码基础设施建设、国产密码应用安全性评估。建设数字政府云平台密码应用服务资源池，形成和完善密码应用支撑能力，推动政务信息系统密码应用改造，降低信息系统遭受攻击导致敏感信息泄露的风险，积极推动国产密码在数字政府中的应用，从自主可控的角度发展数字政府密码服务。

密码服务的建设，主要分三个方面，一是建设完善国产商用密码算法基础设施，如公钥、加密机、数字证书、数据加密等；二是基于密码服务的基础设施，提供密码应用服务，如数字证书统一管理，密钥统一管理等服务，三是建立健全密码应用安全性评估审查制度，在系统规划、建设和运行阶段，全面开展国产商用密码应用安全性评估工作。

（3）建立政务云安全资源池

面向韶关市数字政府政务云虚拟资源安全、各上云单位的业务安全需要，结合云的特性，建立政务云安全资源池，提供安全能力的虚化交付能力，核心要解决 2 个方面的问题:

一是要解决用户之间的隔离和用户自身业务的安全防护需要问题: 对于上云的用户，首先要实现云内不同用户之间的安全隔离，保障各用户之间互不影响，即使有云内用户出现了网络和数据安全问题，也不会影响其他用户；其次是要根据上云用户自身业务的业务特性，如网站类业务、OA 类业务，其安全防护需求不同，要能够要云上用户根据自身业务的需要选择合适的虚拟安全能力。

二是要解决业务上云的合规性问题，业务上云不等于安全托管、不等于责任主体发生变化，按照“谁主管谁负责、谁使用谁负责”的原则，业务上云后，用户也应当对自身业务的网络和数据安全问题负主体责任，云平台运营方应当建立满足用户合规安全的技术手段，以服务的形式供上云用户选择，满足上云用户的合规需求，保障用户的上云安全。

（4）做好安全专家技术支撑

建立长效安全咨询服务机制，聘请安全专家，提供涵盖规划、立项、开发、建设、运营等系统建设全周期的安全评估咨询及服务，提升数字政府网络和数据安全建设和管理水平；建立安全培训演练机制，组织不同层次的安全培训，强化数字政府建设各参与方的安全意识；开展安全体系核查，从网站安全检查、渗透测

试、等级保护测评、上线前风险评估、攻防演练等方面组织第三方安全机构，对数字政府进行安全测评，及时发现安全隐患，督促抓好落实整改，全面提升数字政府安全防御能力。

2.建立纵深安全防御体系

（1）物理安全

安全物理环境是云平台安全的基石，参照《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》，安全物理环境包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等安全措施。

（2）终端安全

按照国家电子政务外网标准要求，持续完善终端安全防护，强化准入控制，系统安全管理、设备管控、安全审计、任意代码防范、数据防泄漏等防护措施，保证终端接入安全。面向政务外网接入终端，根据终端的资产相似性、业务访问流程相似性、终端使用情况的相似性，构建一套涵盖终端入网前、入网中、入网后的终端安全体系：

入网前：在接入政务外网进行办公之前，首先要对终端的安全性进行安全基线核查，设置安全基线，只有满足安全基线的终端才能入网。避免有重大安全问题的终端入网，如终端存在高危漏洞、高危端口未封堵、安装恶意流氓软件、未安装杀毒软件等，对于不满足安全基线要求的终端，必须进行整改后，才能入网，

保障终端的入网安全。

入网中：针对满足基线要求，允许接入数字政府平台的终端，在已经入网后，要持续监测终端的安全情况，一旦发现终端异常，采取必要措施判断终端安全性，若终端处于不安全的状态，强制断开终端连接。

入网后：定期开展高危端口扫描、漏洞扫描、病毒扫描、终端操作系统密码复杂度检查等，定期集中发现终端问题，并采取相关处置措施，修复终端脆弱性问题。同时结合安全运营体系对终端的安全问题做持续监测，及时做好系统更新、补丁升级、病毒库更新等操作。

（3）云平台安全

基于等级保护 2.0 云计算安全扩展三级要求持续优化、完善政务云平台安全建设，在此基础上结合政务云平台安全技术要求、可信云安全技术要求，建立可信、可靠、安全的政务云平台。建设省市一体化安全运营平台韶关分平台，通过安全管理中心进行集中管控、调度和管理，通过虚拟网络隔离、边界防护、身份鉴别、访问控制、安全审计、入侵防御、恶意代码防范、数据完整性、数据保密性、数据备份恢复等安全防护技术手段构建动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控的防护架构，为云平台提供安全保障，为各单位云租户尽快业务上云提供安全基础；丰富政务云安全管理中心、安全资源池及通用安全能力组件，统一管控安全策略，统一监测安全态势，统一调度

管理安全资源，为各单位统一提供安全能力服务。各单位可根据自身业务重要性对安全防护等级的不同需求，选择相应的安全服务，满足等保合规要求以及自身的安全防护需求。

（4）网络安全

网络安全即市电子政务外网、数字政府政务云韶关节点以及各单位网络环境安全，包括网络访问控制、入侵防御/检测、抗DDOS、高级威胁检测、安全接入、安全审计等。

网络访问控制主要指在政务云、政务外网及各单位网络边界部署防火墙，以权限最小化原则设置合理的访问控制规则，防止非授权访问;

入侵防御/检测是指对在网络边界对网络流量进行实时检测，及时发现异常流量和攻击行为并及时告警，阻止更多威胁并应对攻击，保障网络安全;

抗 DDOS 指部署抗 DDOS 防护设备，增加政务外网和云平台网络抗 DDOS 能力;

高级威胁检测指对接入政务外网、政务云及各单位的流量进行实时监测，运用数据模型、安全模型识别网络攻击及高级威胁（APT）并告警;

安全接入指部署专用的安全接入设备采用安全可靠的方式接入政务外网、政务云平台，访问政务外网、云平台的资源;

安全审计指是采集部署在政务云及各单位的安全设备的安全日志，并对安全日志进行分析及溯源。

（5）数据安全

韶关市数字政府数据安全防护体系建设以数据安全治理为前提、以零信任体系为基础、以数据安全防护为核心、以数据安全运营为保障，以数据“进不来、拿不走、看不懂”的原则，构建数据安全防护体系。

采用“全方位、规范化、细粒度”的防护思想，建立数字政府数据安全防护体系，围绕数据创建与采集、存储与传输、发布与使用、销毁、边界安全等数据生命周期的各个阶段，建立数据全生命周期的 安全防护技术措施。

一是基于零信任理念构建数据安全访问，政务外网部署零信任网关，提供统一的身份管理、身份认证、动态访问控制等核心能力。采用多因素认证方式，对数据访问用户的身份唯一性进行可信校验，确保仅有合法用户允许数据访问，同时可基于用户、设备、应用、等细粒度访问控制，实现最小权限管理。对权限进行细粒化分割，保障访问控制的精准。提供数据传输的安全加密，保证数据的完整性和保密性。

二是构建数据安全纵深防护，数据加密技术实现数据安全存储；通过部署数据库防火墙构筑数据的最后一道防线，灵活配置访问控制规则，提供对数据库的入侵防护；部署数据库审计对数据访问行为进行审计，保证数据访问行为可追溯；通过数据脱敏和去标识化实现数据的安全发布和共享；部署数据共享访问风险监测，提供通过 API 接口数据共享访问的风险监测分析，实时发

现安全风险并告警。

三是制定数据备份和恢复机制，制定数据备份、恢复管理制度和规范，定期对数据进行备份，保障数据的可用性。

（6）应用安全

针对 WEB 扫描、WEB 探测、网页篡改、DDOS 攻击、SQL 注入、XSS 跨站脚本攻击等应用层安全攻击手段，为数字政府应用提供统一的安全云防护服务。依托数字政府政务云平台，建设云平台安全资源池，提供漏洞扫描、WAF 应用防火墙、网页防篡改、数据库审计等服务。结合线下应用漏洞扫描、渗透测试、攻防演练等形式，做到应用层的安全问题早发现、早处置，同时结合安全运营体系，对应用安全状态进行 7*24 小时监测，降低应用安全风险。

七、完善网络和数据安全运营体系

（一）工作目标

基于安全技术体系，提升安全识别、安全防护、事件响应与处置、安全分析与监测等安全服务水平，利用大数据分析、自动化编排等技术，开展集中化、自动化、智能化的安全运营，提供覆盖安全全生命周期的服务能力。面向韶关市数字政府的安全防护需要，结合业内先进的安全运营理念，将专业的安全技术队伍和本地安全技术手段相融合，建立规范化、流程化、智能化的动态安全运营体系。基于安全技术体系，提升安全识别、安全防护、事件响应与处置、安全分析与监测等安全服务水平，利用大数据

分析、自动化编排等技术，开展集中化、自动化、智能化的安全运营，提供覆盖安全全生命周期的服务能力。

（二）建设内容

1.数字政府运营体系框架

韶关市数字政府网络和数据安全运营体系由三个部分组成，分别是安全运营平台、安全运营组织、安全运营流程，其中：

安全运营平台是安全运营工作开展的统一承载平台，负责整合技术、工具、服务、流程、人员等全要素，打通网络安全监测、分析、处置、应急等全流程。安全运营平台共分为四层：即采集层、大数据分析层、应用层、展示层。其中采集层主要通过探针实现对全网的流量采集，并对各类网络设备运行日志、资产信息、威胁情报等进行采集；大数据分析层主要是对已采集的元数据进行深度的采集和挖掘，识别当前安全风险、威胁、事件；应用层则构建集中管理能力，提供资产管理、风险识别与预警、安全事件通报与处置闭环、应急指挥、应急演练等安全工作业务模块；展示层主要通过监控中心大屏进行全网安全态势、网络攻击态势、安全事件态势等综合展现，为安全管理决策提供整体数据支撑。

安全运营组织：指根据不同类型的安全运营工作设立决策组、检测组、处置组、审核组、安全专家组等安全运营岗位与角色，为安全运营工作的落地提供专业的人员保障。

安全运营流程：基于通报、日常运维、重保等日常运营场景，建立符合实际情况的安全运营流程，并将这些线下的运营流程通

过安全运营平台实现电子化的线上流程，将安全运营平台和安全运营组织通过安全运营流程打通，基于安全运营流程进行分工协作，实现高效安全运营。

2.建立统一协同安全运营机制

建立覆盖网络和数据的安全运营团队，建立“管、监、察”分离的岗位职责，明确分工，加强沟通协作，以完整而规范的组织体系架构保障每个环节的安全管理工作；以省市一体化安全运营平台为基础，打造全市统一的数字政府网络安全运营平台，建设集安全大数据、攻防演练、流程闭环、态势感知于一体的安全运营支撑平台，完成上下级平台的对接工作，加强安全告警、安全事件、威胁情报、预警信息、知识案例、工单报表等安全数据的交互能力，完善安全编排与自动化响应能力，持续赋能安全运营工作，提升实战化安全运营水平，整体性提升内外部风险感知能力、安全管理闭环能力、协同安全防护能力、攻击检测分析能力、违规行为发现能力、应急事件响应能力和态势感知预警能力。

3.全面梳理信息资产

通过主动梳理+被动识别的方式，全面梳理韶关市数字政府相关信息资产，对于政务信息系统，采用人工梳理的方式，通过各地各单位排查核对，在省数据资源“一网共享”平台录入政务信息系统。对于终端、服务器、一般应用系统、中间件等，可采用被动识别的方式,通过基于流量的分析对这部分资产进行识别;对于重要资产和未被识别的资产,可通过主动识别的方式， 由相

关安全运营人员进行手工输入，并明确资产 IP、MAC、物理位置、责任人等相关信息,通过资产管理实现资产全流程生命周期管理。

4.安全监控与预警

依托数字政府网络安全运营平台，通过终端监控、网络流量监控、网络安全威胁情报分析、应用风险监控、APT 监测预警、操作日志分析、入侵检测联动等，开展全链路端到端监控，实现数字政府全网安全监测，监测的安全问题包括僵木蠕主机监测、异常流量监控、APT 威胁监测、非法外联监测、失陷终端监测等。

5.数据采集与分析

对韶关市数字政府网络关键节点和边界流量进行采集，对关键网络设备、核心安全设备、核心业务系统的日志进行采集，通过大数据分析和建模的技术，对数据中的有用信息，为后续的网络安全威胁、事件的分析提供支撑。

6.事件响应及处置

建立健全韶关市数字政府网络和数据安全应急预案，针对网络访问流量异常、非授权访问行为、网络相关的风险情报等网络安全场景，分别制定对应的网络安全预案，定期进行场景演练，检验预案的可行性，根据演练情况不断完善预案；组建数字政府网络安全运营团队和应急支撑技术队伍，当出现安全事件时，协助有关单位进行网络和数据安全突发事件应急处置工作，包括系统恢复和安全件事件入侵追踪和溯源，同时收集网络和数据安全突发事件相关信息，做好安全事件的分析总结。

7.安全检查监测与整改

常态化开展韶关市数字政府相关业务的网络和数据安全检查监测，定期开展安全巡检。通过安全基线检测完成安全配置检查；通过漏洞扫描发现设备和系统中存在的各种漏洞，并及时修补完善系统漏洞；通过渗透测试，从攻击角度了解系统存在的隐藏漏洞和安全风险，并督促整改。加强政务网络基础设施和应用系统定期安全巡检，定期发布数字政府网络安全运营简报、威胁情报通告。

8.开展网络安全攻防演练

常态化举办数字政府网络安全攻防演练，坚持以保障全市党政机关、重点企事业单位网络和数据安全为目标，以实兵、实网、实战的方式,针对事先设置的突发事件情景及其后续的发展情景，在现有安全应急响应设备和资源条件下，通过实际决策、行动和操作，排查发现各单位网络安全漏洞和风险隐患，完成真实应急响应的过程，从而检验和提高各单位网络安全意识，加强网络和数据安全能力建设，建立完善网络和数据安全制度和应急响应机制，落实网络安全主体责任，锻炼网络安全队伍。

八、构建网络和数据安全监管体系

（一）工作目标

在韶关市“数字政府”暨“智慧城市”建设领导小组统一领导下，建立健全“事前、事中、事后”全程安全监管的联动机制，建立长效的监管对接机制，加强跨行业网络安全通报和事件反馈

工作，配合好国家和省有关部门处置各类信息安全事件；提高处置网络与信息安全突发公共事件能力，实现有机整合，满足集中监管、独立运营、全面覆盖的信息安全监管能力建设要求，为我市数字政府网络和数据安全从内部控制和外部监管两个层面提供保障，实现“层层监管、层层把控、层层防护”，为数字政府政务云、政务外网及数字政府应用的稳定运行提供高效能、高可靠、灵敏快速的信息安全支撑保障能力。

（二）建设内容

1.建立有效的网络和数据安全监管体系

依托数字政府网络安全运营平台，对海量日志数据和业务数据的采集和治理，包括协议审计数据、系统日志、应用日志以及安全日志等，结合特征匹配、关联分析、聚合统计、机器学习、深度学习等技术，配合云端威胁情报，充分感知识别威胁，构建数字政府安全态势监管平台。实现细粒度的安全监管，做到安全风险早发现、早解决。在外部监管层面，实现出入口的安全态势监管，建设外部数据接口，建立对接机制，为监管单位履行安全态势监管职能提供抓手。

脆弱性态势感知。通过安全基线监测等技术手段对系统进行监测和分析，主动地对系统、应用层、中间件、数据库等漏洞检测，及时发现系统漏洞，规避系统安全风险，提高系统整体安全性，确保脆弱性态势处于可控范围内。

高级威胁态势感知。基于人工智能、大数据、机器学习、建

模分析、威胁情报、威胁检测等技术对外部威胁、内部威胁进行全方位监测，精准检测各类高级威胁，有效发现外部攻击行为、内网潜伏威胁等高级威胁。

异常行为态势感知。异常行为检测引擎，实时匹配流量，实现对全网流量的实时监控,对网络流量中重要协议进行解码还原，当发现存在异常行为时会将流量片段在采集的流量数据中进行标记，传给安全运营平台，由平台进行深度关联分析，挖掘潜在的威胁。通过网络异常流量检测模型，提高发现异常行为的能力和效率。

未知威胁态势感知。利用机器学习、关联分析、UEBA 等新技术，发现最新未知威胁，同时支持自定义部署 AI 机器学习模型，通过输入任意指标类数据进行模型训练，实现发现未知安全威胁和安全事件，进而有效解决传统网络安全措施无法解决的网络和数据安全问题。

僵木蠕毒态势感知。通过脆弱性态势感知、高级威胁态势感知、异常行为态势的感知和监测分析结果，快速确认僵木蠕毒的感染情况，统计僵木蠕毒感染量和感染类型，并依据感染情况进行分布态势分析，可视化展示僵木蠕态势数据。

2.建立内容安全监管体系。

建立全市政府网站和政务新媒体内容安全监管机制，严格对上网内容进行审核把关，加强对各单位政府网站和政务新媒体的监管，常态化开展政府网站和政务新媒体的内容监测和检查，避

免政府网站和政务新媒体上出现涉黄、涉毒等违规、违禁、敏感、不良内容，保障政府网站和政务新媒体的内容安全。

3.建立网络安全指标体系

根据《广东省数字政府网络安全指数指标体系》、《信息安全保障指标体系框架》、《等级保护评价考核体系》、《国家电子政务外网网络安全风险排查工作方案》等规范要求，结合韶关实际，建立科学、客观、实用，覆盖“云、网、数、用、端、行为”的韶关市数字政府网络安全指标体系，主要围绕网络安全管理、安全建设、安全运营、安全效果等维度进行基本指标构建，及重保、通告预警、专项检查、综合评价、网络安全工作责任制考核等场景化的评价体系实现。

九、云平台安全建设

（一）工作目标

根据政务云平台虚拟化、资源池化、弹性扩容等特点，结合《GB/T22239-2019信息安全技术网络安全等级保护基本要求》关于云计算扩展要求的相关标准，通过政务云权责划分、政务云平台安全、政务云租户安全、政务云安全运营、政务云安全监管五方面建设，明确数字政府政务云平台韶关节点管理使用中各方的权责，强化租户安全责任划分、虚拟化安全工具及公共组件防护，优化政务云平台安全运营和安全监管体系，建设安全资源池，为各租户提供个性化安全服务，为我市数字政府建设提供安全、高效的云安全服务。

（二）建设内容

1.政务云权责划分

市政务服务数据管理局：统筹协调数字政府政务云平台韶关节点安全管理工作，参考省数字政府政务云制定数字政府政务云平台韶关节点安全管理规范，承担数字政府政务云平台基础设施和云边界的安全管理主要责任。

政务云平台使用部门：负责数字政府政务云平台云上应用系统等保测评及整改等合规性安全工作，承担数字政府政务云平台云上系统的运行管理安全、信息内容安全以及接入数字政府政务云平台云上系统网络终端的安全管理责任，参与制定安全管理规范实施细节，参与安全考核。

政务云平台建设运营单位：负责落实各项安全管理制度规范，执行数字政府政务云平台安全技术措施，接受市政务服务数据管理局的安全考核。

第三方安全服务机构：受市政务服务数据管理局委托，负责监督、评估、审计建设运营单位数字政府政务云平台安全运营工作落实情况，定期上报云平台安全风险分析报告，对发现的重大安全风险要第一时间报告并提出整改意见。

安全监管部门（网信、公安、保密）：负责数字政府政务云平台出口的安全态势监管、失泄密监管，以及内容安全管理。

2.政务云平台安全

数字政府政务云平台韶关节点总体安全建设应按照《网络安

全法》、《关键信息基础设施安全保护条例》的相关要求，在满足等保三级的基础之上，实行重点保护，完善安全物理环境、安全区域边界、安全通信网络、安全计算环境、安全管理中心、安全管理人员、安全管理机构、安全管理制度、安全建设管理、安全运维管理以及等级保护 2.0 中关于云计算扩展要求的相关建设内容，同时完善关于关键基础设施的态势感知能力、安全运营能力、安全监管能力的相关建设。

2.政务云租户安全

根据各单位上云系统的实际需求，提供租户安全服务，解决租户自身的业务安全防护、租户与租户之间的安全隔离、租户的远程数据传输安全等相关安全问题，使得上云的租户可以根据自身的业务需求，获取不同的安全能力，同时满足上云业务系统等级保护合规建设的相关要求，助力租户安全、合规上云。

3.政务云平台安全运营

数字政府政务云平台采用安全技术团队与态势感系统相互配合，结合人工安全研判与自动态势分析来确保平台获得稳固的防护体系与及时的安全预警，同时结合网络和数据安全事件应急预案，进行政务云平台网络安全事件的识别与研判，通过集中安全监控与分析工作，将网络和数据安全事件集中管控、统一处理。

4.云平台安全监管

在政务云平台运营团队内部建立自我监管的流程、制度和技术手段，及时发现安全风险及不规范操作，确保平台安全；建立第三方安全

审查制度，从外部视角发现安全盲区，修补监管漏洞；利用云平台内部自身机制开展监管的同时。结合第三方安全服务机构的能力，对云平台开展安全测试和问题审查。

十、大数据安全建设

（一）工作目标

坚持安全和发展并重的理念，以保障韶关市数字政府数据安全为核心，围绕数据采集、传输、存储、处理、交换、销毁等数据生命周期全过程，从安全管理、安全技术、安全运营、安全监管四个维度制定数据安全体系规划，建设数字政府数据安全保障体系，保证政务数据的使用和开发处于有效保护、合法使用的状态。

（二）建设内容

1.大数据安全权责划分

大数据安全管理组织由市政务服务数据管理局、市直各部门、建设运营单位、第三方安全服务机构、安全监管部门等组成。

市政务服务数据管理局：统筹协调政务数据安全管理工作，负责制定政务数据安全管理规范，落实安全考核工作，承担省数据资源“一网统管”平台韶关分平台的安全管理主体责任；

市直各部门：参与制定安全管理规范，参与安全考核工作，承担牵头开展的业务主题数据的安全管理主体责任；

建设运营单位：负责落实执行各项安全管理制度规范，执行数据安全监管技术措施，接受市政务服务数据管理局的安全考核；

第三方安全服务机构：受市政务服务数据管理局委托，负责监督、评估、审计建设运营单位数据安全运营工作落实情况，定期上报数据安全风险分析报告，对发现的重大数据安全风险问题要第一时间报告并提出整改意见；

安全监管部门：负责承载省数据资源“一网统管”平台韶关分平台接入和输出边界的安全态势监管、内容安全监管、失泄密监管。

2.大数据安全管理

（1）数据安全管理组织

建立健全覆盖全市的数据安全管理组织架构，明确部门职责及部门内部数据安全管理岗位的职责。通过进一步完善政务部门的数据安全管理组织，确定数据安全第一负责人（首席数据官CDO），建立协作机制，压实数据安全管理责任，准确理解数据流转环节的管理要求。依照组织监督考核机制，落实对政务大数据安全的监督检查/考核制度，定期对数据安全管理机构、职能部门和安全岗位进行工作绩效评估。

（2）数据安全人员管理

明确重要岗位人员能力要求，确定相应的考核内容与考核指标，定期对重要岗位人员能力进行评估和考核，依据评估、考核结果确定任职资格。制定人员招聘、录用、培训、上岗、调岗、离岗、考核、选拔等大数据服务人员安全管理的操作规程，确保重要岗位人员上岗前的背景调查与保密协议签署全覆盖。

（3）数据资产管理

面向政务信息系统、政务数据，建立数据资产登记制度，编制数据资产清单,明确政务大数据服务相关数据资产的基础属性、分类属性、安全级别及相关方的权限和责任。制定韶关市政务数据分类分级标准，明确数据分类分级方法和操作指南，以及明确数据分类分级的变更审批流程。依据数据主体分级要求建立相应的标记策略、访问控制、数据加解密、数据脱敏等安全机制和管控措施。

（4）供应链管理

建立供应链安全管理制度，将对供应链中的公司和人员的管理纳入整体的数据安全管理体系中，明确供应链中公司和人员的资质要求，规范供应链公司和人员的职责、权限、服务内容和服务流程。对于能接触到业务数据的供应链人员签订保密协议，对于能接触到大量个人信息、核心数据、重要数据的供应链人员进行背景调查。

（5）数据安全评估

落实数据安全法律法规、合规要求，对政务数据处理活动定期开展数据安全评估，明确政务数据处理活动面临的数据安全风险及其应对措施等，形成数据安全风险评估报告，及时整改数据安全风险评估中发现的问题。

（6）数据安全应急处置

建立数据安全应急处置机制，制定政务数据安全事件应急处

置预案，发生数据安全事件时及时启动数据安全应急预案，采取相应的应急处置措施，消除安全隐患，防止危害扩大。根据数据安全事件应急处置预案制定演练计划，定期组织应急演练，保存演练记录，针对演练中发现的问题立即整改。

3.大数据安全技术

（1）数据采集安全

政务部门通过应用系统人工录入或数据接口调用的方式实现政务数据采集，并明确政务数据的采集目的、采集用途、采集渠道、采集流程、采集内容和数据格式，建立数据采集台账，保证政务数据采集的合法性、正当性、必要性和业务关联性，定期执行政务数据采集合规性审查。对政务数据采集涉及的采集环境、采集设施和采集技术采取必要的管控措施，提高政务数据的科学性、准确性和时效性，保证政务数据在采集过程中的安全。

（2）数据传输安全

政务部门制定并执行政务数据安全传输策略和规程，采用安全可信通道或数据加密等安全控制措施，确保政务数据传输过程完全可控。对关键网络传输链路、网络设备节点实行冗余建设，保障数据传输可靠性和网络传输服务可用性。

（3）数据存储安全

通过技术手段保障存储数据的机密性、完整性和可用性。建立数据加密存储机制，采用加密技术保证个人信息和各类重要政务数据在存储过程中的保密性。建立数据备份与恢复机制，通过

在本地和异地建立数据副本保障数据存储的可靠性，防止数据丢失。

（4）数据处理安全

政务部门需建立数据处理活动相关平台系统的访问控制措施，为平台系统访问方分配完成职责所需的最小数据使用权限；涉及授权特定人员超权限处理数据的，由首席数据官审批和记录；及时清除与数据处理相关系统中无用账号、默认账号，杜绝多人共用同一系统账号的情况；采取技术手段实施数据脱敏，对数据脱敏处理过程相应的操作进行记录，满足数据脱敏处理安全审计要求；采用技术手段对违规使用数据的行为进行有效的识别、监控和预警。

（5）数据交换安全

完善数据共享交换平台的安全防护措施，建立边界安全防护机制，完善访问控制、数据加密、数据脱敏、日志记录等技术防护手段。建立数据交换过程的监控工具，对共享数据及数据交换服务过程进行监控，确保共享的数据未超出授权使用范围。

（6）数据销毁安全

建立数据删除操作规范，建立法规要求的重要数据或个人信息多人和多级的操作模式，明确大数据服务停止运营、用户账户注销、数据保存期到期、用户申请数据删除等场景的删除数据对象和操作规程。确保各部门在政务数据使用和交换过程中产生的临时数据，在市各部门完成履行法定职责的范围内工作且不再符

合法律、行政法规规定的使用政务数据条件和程序时合规销毁。

4.大数据安全运营

（1）数据处理监测

建立数据处理活动及其服务接口安全监管措施，具备对数据服务接口访问进行自动化监控和应急处置的能力。建立数据处理活动的监测规则和行为基线，能根据设定的规则和基准对数据处理活动异常行为进行告警，并定位数据处理活动发生的位置、操作以及数据处理活动的风险及威胁等信息。

（2）数据安全追溯

依据国家相关法律法规和地方规章制度等要求，建立跨部门的长效化政务数据安全调查机制，对造成安全事件发生的相关责任人按照相关法律法规的要求进行责任追究。跟踪和记录数据处理活动，确保能对数据处理活动进行追踪溯源，能对存储数据使用、提供和公开等进行细粒度安全审计。

（3）数据灾难恢复

制定数据备份、归档与恢复计划，定期对备份和归档数据的可用性、完整性和一致性进行检测，对数据恢复的安全风险进行分析，建立异地容灾备份措施，确保具备备份和归档数据的恢复重建能力。

5.数据安全监管

利用建设运营单位内部自身监管机制，定期或不定期开展各类数据安全审计和检查活动，发现内部潜在安全隐患。委托第三

方安全服务机构对大数据平台开展安全测试和问题审查，发现平台存在的安全问题和薄弱点，查漏补缺，优化现有防护体系，与市委网信办、市机要和保密局、市公安厅等部门建立联动机制，满足大数据平台漏洞检测、违规信息检测、失泄密检测等监管要求。

十一、应用安全建设

（一）工作目标

围绕软件研发生命周期，将安全管理、安全技术、安全运营、安全监管四大安全支柱贯穿于整个应用开发阶段，构建应用安全管理架构、应用安全技术架构、应用安全运营架构和应用安全监管架构；将“安全基因”嵌入到政务应用的全生命周期，强化数字政府政务应用安全防护能力。

（二）建设内容

1.应用安全权责划分

应用安全管理组织由市政务服务数据管理局、市直各部门、建设运营单位、第三方安全服务机构、安全监管部门等组成。

市政务服务数据管理局：统筹协调政务应用安全管理工作，负责制定政务应用安全管理规范，落实安全考核工作，承担统建应用如韶关市电子政务办公业务系统集约化平台、韶关市“一门式一网式”政务信息系统等的安全管理主体责任；

市直各部门：参与制定安全管理规范，参与安全考核工作，承担牵头开展的业务应用的安全管理主体责任；

建设运营单位：负责落实执行各项安全管理制度规范，执行应用安全监管技术措施,接受市政务服务数据管理局的安全考核;

第三方安全服务机构：受市政务服务数据管理局委托，负责监督、评估、审计建设运营单位应用安全运营工作落实情况，定期上报应用安全风险分析报告，对发现的重大数据安全风险问题要第一时间报告并提出整改意见;

安全监管部门：负责承载应用的网络出入口的安全态势监管、内容安全监管、失泄密监管。

2.应用安全管理

在整体的网络和数据安全管理体系人员管理的基础上，加强应用开发和运营人员的管理，对安全设计、安全编码、安全验收、安全部署、安全运营、源代码保管和交接等工作流程进行严格规范，编写相关的安全操作指南，对人员行为进行约束，同时建立奖惩机制、问责机制，将安全责任落实到应用开发人员，提高安全开发意识。

按照国家网络安全、数据安全相关法律法规，开展应用系统网络安全等级保护和密码应用建设等工作。通过合规管理，进行差距分析和安全整改，加强应用系统的安全防护能力。

建立应用安全开发运营管理体系，制定相应安全管理制度、安全开发规范等，规范编码的安全性，规范上线流程的安全管控，加强应用开发的安全考核。应用安全管理制度主要包括：研发安全管理制度、安全开发编码规范、应用上线审核制度、应用日常

运营安全管理制度等。

3.应用安全技术

应用安全技术围绕安全开发生命周期进行建设，将四大安全体系融会贯通于整个应用开发的各个阶段，将安全工作前置并介入到开发的需求、设计、开发、测试、发布等5个阶段。

需求阶段要把握安全需求分析和关键目的识别，设计阶段要考虑受攻击面分析、安全方案设计，开发阶段要考虑安全编码规范、代码审计，测试阶段要上线渗透测试等相关手段，应用发布阶段要进行集成测试和最终安全评审。

4.应用安全运营

通过安全评估、安全审计、安全运营分析，提高应用安全漏洞主动发现能力，为应用安全整体保障输出有价值的预警信息。通过安全监控进行脆弱性检测、完整性检测、可用性检测、认证检测等。通过内容安全监控技术进行不良信息监测，及时发现色情、暴恐、涉政等违规信息。通过安全加固，提高数字政府应用基础防护能力。

5.应用安全监管

利用建设运营单位内部自身监管机制，定期或不定期开展各类应用安全审计和检查活动，发现内部潜在安全隐患。委托第三方安全服务机构对应用系统开展安全测试和问题审查，发现应用系统存在的问题和漏洞。与市委网信办、市委机要和保密局、市公安厅等部门建立联动机制，满足应用系统漏洞检测、违规信息

检测、失泄密检测等监管要求。

6.应用国产化改造

推动成立韶关市信息技术应用信创适配中心，开展软硬件产品信创适配测试验证，为全市数字政府政务信息系统建设提供方案技术审核和项目验收前信创适配测试验证服务，助力全市信创设备替代和本地信创产业发展；按照“信创为常态，非信创为例外”的原则，加大政务信息化项目信创技术审核力度，新建和升级改造的政务信息系统必须符合信创技术要求。

十二、实施步骤

（一）2023年重点实施内容

1.安全规划和标准规范建设

以国家政策文件及广东省数字政府安全体系建设总体规划为指导，以韶关市数字政府网络和数据安全实际需求为出发点，以保障韶关市数字政府建设成果为目标，编制韶关市数字政府网络和数据安全体系建设总体规划和实施方案，为韶关市数字政府网络和数据安全建设做战略部署。

建立健全韶关市数字政府网络和数据安全体系建设的管理制度及规范,依据《广东省数字政府网络安全指数指标体系标准》,编制韶关市数字政府网络和数据安全指引，为各县（市、区）、市各有关单位网络和数据安全建设提供指导。

加强网络和数据安全意识的宣贯和培训，提高全员安全意识和各单位的安全防范能力。

依据《中华人民共和国数据安全法》及《信息安全技术 政务信息共享数据安全技术要求》的相关要求，开展数据资源分类、数据开放共享、数据监管、数据加密、数据安全等重点标准规范的制定，明确数据分级分类原则、数据开放共享要求、数据监督管理、数据责任主体等核心要点，形成长效的数据安全规章制度保障。

制定韶关市数字政府应用安全体系建设的管理制度及规范，包括应用开发、测试、上线、运行等流程的管理制度，制定与供应链、第三方服务机构相关的标准规范。

围绕“政务应用大集中”、“集约化”等业务发展趋势，保障各项安全措施的持续有效及政务系统安全可靠运行，建立安全集中运营管理机制，开展资产管理、流量监测、大数据分析、通报预警、响应处置等相关管理办法的梳理，明确重点资产、采集对象、分析方法、预警机制、处置流程等核心要点，并出台相关管理规章制度，形成长效的安全运营规章制度保障。

2.平台安全服务建设

完善韶关市数字政府政务云平台安全保障体系，从安全物理环境、安全区域边界、安全通信网络、安全计算环境、安全管理中心五大方面进行建设，保障政务云平台基础设施和应用系统安全，满足合规要求。建立政务云安全资源池，为政务云租户按需提供服务。

开展国产政务云平台建设，逐步进行国产化生态的适配，充

分发挥生态上下游产业的优势，打造自主可控、稳定可靠的云平台基础设施，为保障运行于云平台之上的应用做长远规划。

开展数字政府安全运营中心和安全运营平台建设，在数字政府政务云平台已有安全能力的基础上，整合电子政务外网等安全能力，打造数字政府安全运营中心，组建数字政府安全运营团队，初步构建基于安全运营的监测预警手段。

推进国产商用密码资源平台应用，加强密码计算资源池、密码服务资源池、密码接口资源池、密码服务管理的建设，对于已建设但未完成国产商用密码改造的系统，持续推动改造；对于新建的业务系统，必须满足国产商用密码的要求，才能允许上线。

开展数字政府信创适配测试中心建设，组织电信企业、高校和信创软硬件企业，联合共建韶关市信息技术应用创新适配中心，为全市数字政府政务信息系统建设提供方案技术审核和项目验收前信创适配测试验证服务；按照“信创为常态，非信创为例外”的原则，持续推进政务信息化系统信创适配改造。

升级改造市级电子政务外网，打造一网多平面的政务外网，为不同接入单位专网整合至电子政务外网提供专属平面。

3.终端安全服务建设

基于《政务外网终端一机两用安全管控技术指南》，构建零信任管理平台、零信任安全网关，对接入政务外网的终端准入进行安全控制，保障终端网络接入安全。构建一体化终端安全管理平台，涵盖终端资产管理、脆弱性管理、防病毒建设等方面，摸

清终端家底、加强终端安全防范。

4.数据安全服务建设

基于零信任架构，建设大数据中心韶关分节点权限管理平台，按照统一的权限管理模块，进行大数据中心内的统一认证和授权管理。做好数据安全需求调研分析、数据资源目录梳理、数据分级授权管理等数据安全工作。

5.安全监管服务建设

常态化开展网络和数据安全检查监测，开展网络安全攻防演练，不断加强网络安全和数据安全宣传教育，进一步强化全市网络安全和数据安全风险意识和责任意识，提升网络安全和数据安全保障能力和防护水平，有效筑牢网络安全和数据安全防线。

（二）2024年重点实施内容

1.安全规划和标准规范建设

完善韶关市数字政府网络和数据安全实施方案，在前期已制订安全管理办法和规章制度的基础上，不断完善数字政府安全管理制度、安全评价体系、数据安全规范、应用安全标准、安全运营制度等安全标准规范。

2.平台安全服务建设

基于最新的网络和数据安全法律法规防护要求，持续加强韶关市数字政府政务云平台安全的合规建设。

开展国产政务云平台物理资源扩容，加强国产化政务云平台的平台安全建设。发挥信创适配测试中心作用，持续推动全市政

务信息化系统信创改造，并迁移到国产化政务云平台。

完善安全运营平台建设，将数字政府各单位的安全情况纳入运营范畴，初步形成纵向体系系统能力，加强安全运营团队的队伍建设并进行培训赋能，形成较为完善的运营机制流程，开展网络安全攻防演练、应急对抗等工作，沉淀安全运营经验。

完善政务云密码资源池，根据实际使用需求，适时对密码资源池进行扩容。持续推动应用系统的国产商用密码改造，并推广国产商用密码在物理环境、网络、数据等维度的应用。

推进各县（市、区）电子政务外网升级改造，构建一网多平面的政务外网，并按需向接入单位延伸。

3.边界安全服务建设

在政务办公一张网的大环境下，建设各接入单位接入政务外网的边界隔离、访问控制、防火墙、防病毒、入侵防御等技术措施，实现各接入单位之间的安全隔离，避免各接入单位之间横向感染、攻击，同时保障各接入单位办公环境安全。

4.数据安全服务建设

持续开展数据安全分类分级，在完成数据安全需求调研和数据安全建设方案编制基础上持续开展数据安全分类分级工作；开展数据安全评估工作，形成数据安全风险评估报告；建设大数据中心数据监测审计、数据加密、数据脱敏等数据安全防护手段，从数据产生、传输、使用、存储、销毁全流程保障数据全生命周期安全。

5.安全监管服务建设

持续开展网络和数据安全检查监测，开展网络安全攻防演练，持续加强网络安全和数据安全宣传教育，进一步强化全市网络安全和数据安全风险意识和责任意识，提升网络安全和数据安全保障能力和防护水平，有效筑牢网络安全和数据安全防线。

（三）2025年重点实施内容

1.安全规划和标准规范建设

持续优化韶关市数字政府网络和数据安全实施方案，在前期已制订安全管理办法和规章制度的基础上，持续优化数字政府安全管理制度、安全评价体系、数据安全规范、应用安全标准、安全运营制度等安全标准规范。

2.平台安全服务建设

丰富国产政务云平台服务目录，打造满足合规要求的国产化政务云平台，持续适配国产化政务云生态，持续推进业务系统国产化改造，并迁移至国产化政务云平台。

总结安全运营经验，标准化整体安全运营流程，基于人机共治，初步形成自动化响应处置能力，提高安全时间的处置效率。

持续推广国产商用密码在物理环境、网络、数据等维度的应用，推进政务信息系统商用密码应用改造。

3.数据安全服务建设

建设数据安全运营平台，持续发现数据安全风险，如API接口安全问题，建立数据安全应急处置机制，并通过技术演练、策

略优化，不断完善优化安全运营体系，提升数据安全运营能力。

4.安全监管服务建设

基本实现可视化、一体化的运营管理体系，采用机器学习、深度学习等算法，结合人工核查，及时检测发现各类安全事件，提高安全事件处置能力；完善安全专家技术服务，基本形成完善的安全培训、安全咨询、安全测评服务体系；

5.终端和边界安全服务建设

强化一体化终端安全管理，集中识别终端安全威胁、监测终端安全事件，保障终端的入网安全；形成完善的边界安全防护体系，做到接入单位与政务外网安全隔离、单位与单位之间的安全隔离，最大限度保护韶关市数字政府网络和数据安全。

十三、实施保障

（一）组织保障

充分发挥韶关市“数字政府”暨“智慧城市”改革建设工作领导小组的作用，加强宏观指导，统筹规划、统一部署、协调推进韶关市数字政府网络和数据安全体系建设。各县（市、区）各部门建立本单位、本部门、本系统的组织领导管理机构，明确领导及工作人员责任，制定管理岗位责任制及有关措施，严格内部安全管理机制。充分发挥韶关市数字政府专家库专家作用，吸收国内知名网络安全企业经验，对数字政府网络和数据安全发展战略和网络和数据安全规划提出意见和建议，参与制订网络和数据安全实施计划和解决方案，为我市数字政府网络信息安全技术层

面提供规划设计、论证、指导和评估等咨询建议。

（二）资金保障

加大韶关市数字政府网络和数据安全体系建设支持力度，积极争取国家、省、市的资金，多渠道强化资金保障。将韶关市数字政府网络和数据安全体系建设资金纳入均衡化发展资金和市财政预算，根据每年数字政府网络和数据安全体系建设实际需求，保障网络和数据安全重点领域和重大项目的投入。规范政务信息化项目中涉及网络和数据安全经费的预算编制和资金使用管理，保障政务信息化项目中的网络和数据安全资金，确保网络和数据安全体系可持续的运营和发展。

（三）人才保障

加强数字政府网络和数据安全培训，全面提升各级领导干部数字政府网络安全意识，加强专业人才培养，重视业务骨干培训，建设一支既具备网络安全技术又精通政府工作的复合型人才队伍，并通过政策支持吸引、留住网络安全专业人才。常态化开展网络安全攻防演练，持续推动利用社会网络安全机构的力量提升数字政府网络安全体系的健壮性，吸引高水平人才以不同形式参与韶关市数字政府网络安全体系建设。优化人才培养机制，通过内部挖潜、技能培训、外部引起或政企合作等方式，挖掘网络和数据安全领域高水平研究型人才和具有工匠精神的高技能人才。持续开展各类专项技能教育与培训计划，健全完善职称制度、职业资格制度、职业技能等级制度等体系，提高人才评价的针对性

和有效性。加强领导干部网络和数据安全教育培训，提升领导干部安全意识和安全技能，不断提高对快速变化的安全形势的驾驭能力。

（四）技术保障

确保提供数字政府运行所需的政务网络、政务云平台运行环境保障和安全技术支撑，满足政务服务应用的可用性、完整性、保密性需求。吸纳优秀网络信息安全企业共同参与韶关市数字政府网络和数据安全体系建设，为韶关市数字政府安全体系建设、运营、测评和监管提供长期稳定的服务和支撑。

（五）宣传保障

创新宣传方式，丰富宣传手段，加强网络和数据安全相关政策及概念解读，总结推广一批做法经验、典型模式和先进案例。举办网络安全大会、网络安全宣传周、安全技术沙龙等多种形式，积极宣传相关法律法规。定期组织网络和数据安全培训交流，推广使用网络安全新产品新技术和新解决方案，提升网络安全、数据安全保护意识和防范能力，营造全社会共同关注、积极参与、协力支持、共同推进数字政府安全建设的良好氛围。