数字时代城市数据安全管理经验

齐同军　　杭州市数据资源管理局数据资源处处长

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

数据安全背景

数据安全存在着多个层次，如：

制度安全、技术安全、运算安全、存储安全、传输安全、产品和服务安全等。

对于计算机数据安全来说：制度安全治标，技术安全治本，其他安全也是必不可少的环节。

数据安全是计算机以及网络等学科的重要研究课题之一。它不仅关系到个人隐私、企业商业隐私；而且数据安全技术直接影响国家安全。

数据安全背景

中国最著名“照片泄密案”

由1964年《中国画报》封面刊出的一张照片引起的。

在这张照片中，大庆油田的"铁人"王进喜头戴大狗皮帽，身穿厚棉袄，顶着鹅毛大雪，握着钻机手柄眺望远方，在他身后散布着星星点点的高大井架。

数据安全背景

自今年3月中旬英国政治咨询公司“剑桥分析”被曝以不当手段获取海量Facebook用户数据，Facebook公司就成为“众矢之的”。4月10日至11日，扎克伯格先后出席美国国会参议院和众议院听证会，总计接受了两院议员十余个小时的“拷问”。 Facebook公司通报“剑桥分析”总计获取8700万名Facebook用户数据，其中欧盟计有270万名用户受到影响，为此欧洲议会、欧盟委员会高层多次向Facebook公司“喊话”，呼吁扎克伯格赴欧出席听证会接受质询。

数据安全背景

各行业所需要加密保护的数据

1、制造业设计图纸、价格体系、商业计划、客户资料、财务预算、市场宣传计划、采购成本、合同定单、物流信息、管理制度等；

2、政府和军队公文，统计数据，机要文件，会议机要，军事情报、军事地图、作战方案等；

3、金融、电信机构交易数据、账目信息、融资投资信息、董事会决议、大客户信息、上市公司中报/年报等；

4、咨询型企业调查报告、咨询报告、招投标文件、专利、客户资料、价格等；

5、设计类机构设计图、设计方案、策划文案、客户信息、软件程序等。

数据安全背景

如何实现数据安全？

1、早实施。数据安全相关的措施如果完全没有，那么企业应该立即实施起来，从而确保各个数据体系的安全，绝不能再任意其处于极脆弱的状态。

2、数据分类。对于数据进行一定的分类，让所有的员工知道什么样的数据属于绝密的，什么样的数据属于公开的，我们在进行任何有关于数据的工作中一定要注意到这种严格的界定。

3、分析系统。对于数据进行一定的分析，看看自己的体系之内有没有机密的数据处于不安全的状态之下，如果有，一定要立即实施措施来保护。

4、加密。对于数据有一套自己的加密措施，通过加密措施来设置屏障，从而彻底保障一些数据的安全。加密方式也要实行多种并举。

5、完善管理。对于数据的管理也要不断的完善，从而形成一个合理的流程，让数据的使用更加的合理。

6、备份。相关的网上数据有一个长期的备份策略，从而让数据可以在遭受攻击的时候能够快速的恢复。

目录

第一部分

《杭州市政务数据安全管理办法》解读

（一）综述

1.总体框架（6章60条）

第一章 总 则

第二章 职责与分工

第三章 数据安全

第一节 一般规定

第二节 应急管理

第三节 信息保护

第四章 政务数据安全监督检查

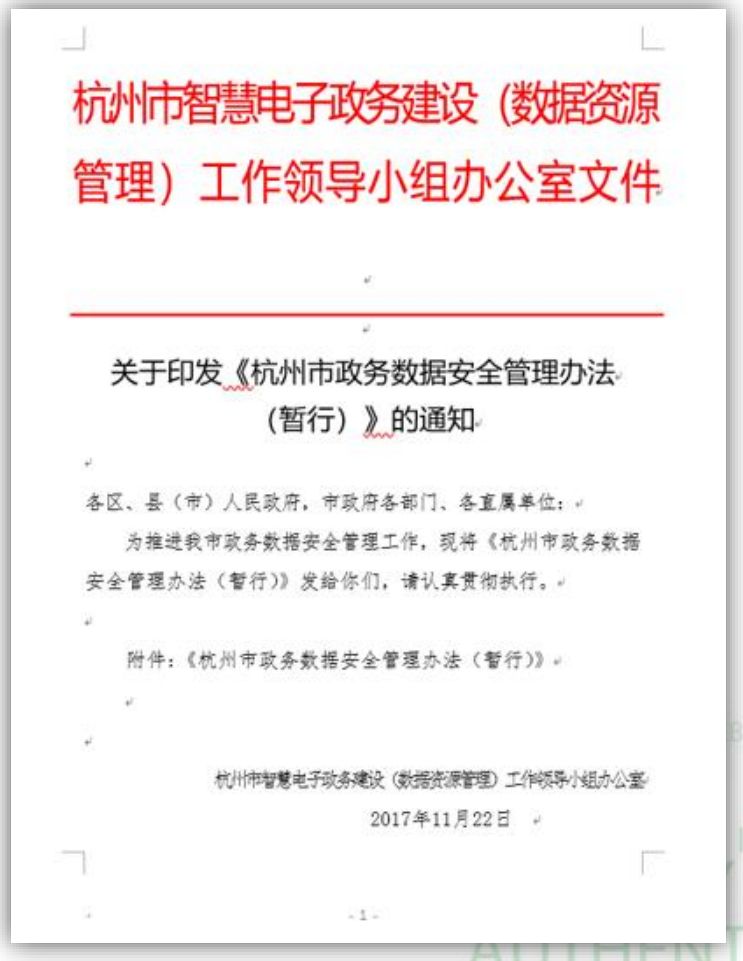
第一节 政务数据安全监察员

第二节 政务数据安全检查

第三节 政务数据安全事件调查

第五章 责任追求

第六章 附则



杭州市智慧电子政务建设（数据资源管理）工作领导小组办公室文件

关于印发《杭州市政务数据安全管理办法（暂行）》的通知

各区、县（市）人民政府，市政府各部门、各直属单位：

为推进我市政务数据安全管理工作，现将《杭州市政务数据安全管理办法（暂行）》发给你们，请认真贯彻执行。

附件：《杭州市政务数据安全管理办法（暂行）》

杭州市智慧电子政务建设（数据资源管理）工作领导小组办公室

2017年11月22日

- 1 -

（一）综述

2.目标和依据

- 目标：为加强政务数据安全管理，建立健全政务数据安全保障体系，预防政务数据安全事件发生
- 依据：《中华人民共和国网络安全法》、《浙江省公共数据和电子政务管理办法》等

3.适用范围

适用于杭州市域范围内的非涉密政务数据安全管理工作。

（一）综述

2.目标和依据

- 目标：为加强政务数据安全管理，建立健全政务数据安全保障体系，预防政务数据安全事件发生
- 依据：《中华人民共和国网络安全法》、《浙江省公共数据和电子政务管理办法》等

3.适用范围

适用于杭州市域范围内的非涉密政务数据安全管理工作。

4.方针与原则

- 方针：积极防御、综合防范
- 原则：政务数据安全与促进信息化发展相协调、管理与技术统筹兼顾原则。政务数据安全和信息化工作应当同步规划、同步建设、同步实施、同步发展。

5.责任追究制度

政务数据安全管理工作实行安全事件责任追究制度，依照有关法律、法规和规章，追究政务数据安全事件责任人的责任。

6.相关概念

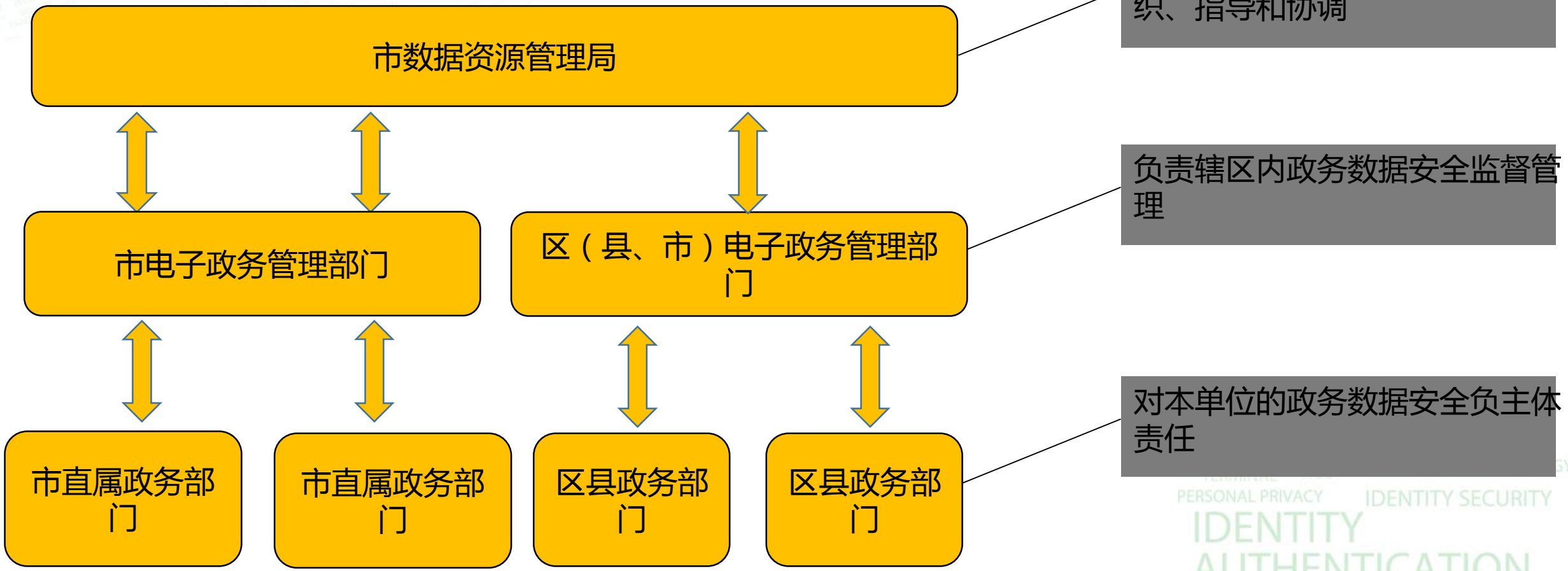
- 政务信息系统：各级政府组成部门（含国有企事业单位、下级部门和单位）所建设的，由计算机及其相关和配套设备、设施（含网络）构成的，按照一定的应用目标和规则对相关信息和数据进行采集、加工、存储、传输、检索等处理的人机系统。
- 政务数据：各级政府组成部门在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等。

6.相关概念

- 政务数据安全：通过采取必要措施，防范对网络（系统、数据）的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络（系统）处于稳定可靠运行的状态，以及保障政务数据的完整性、保密性、可用性的能力。
- 政务数据安全管理：在政务数据系统规划建设、运行维护、使用及废止等过程中，保障政务数据（含个人、企业信息）、信息系统、网络与机房基础设施安全的一系列活动。

（二）重要条款解读

1.职责与分工



（二）重要条款解读

1.职责与分工——市数据资源局（第六条）

1. 编制政务数据安全发展战略和总体规划，制定政务数据安全规章、政策和标准，指导各单位开展政务数据安全工作；（指导职能）
2. 组织杭州市重大政务数据安全基础设施建设，研究解决涉及政务数据安全的重大事项；（组织职能）
3. 组织开展政务数据安全检查、风险评估和等级保护工作，开展政务数据安全培训；（组织职能）
4. 会通相关主管部门建立政务数据安全监测预警、信息通报和应急处置机制，制定政务数据安全应急预案，通报政务数据安全信息，调查处理重大政务数据安全事件；（协调、组织职能）
5. 建立政务数据安全管理与测评机构和专家队伍。

（二）重要条款解读

1.职责与分工——电子政务管理部门（第七条）

1. 制定辖区内政务数据安全工作制度，指导辖区内各单位开展政务数据安全工作；
2. 监督辖区内各单位政务数据安全规划和建设；（监督职能）
3. 实施政务数据安全年度检查以及重要保障时期的专项检查，组织开展辖区内的政务数据安全专项培训；（监督检查职能）
4. 建立辖区内政务数据安全事件应急机制和通报制度，向市数据资源局通报辖区内各单位的政务数据安全信息，协助市数据资源局调查处理辖区内的政务数据安全事件；（信息通报职责）
5. 配合辖区保密行政管理部门对政务数据开展保密安全检查工作；
6. 对辖区内政务数据安全工作进行年度总结和讲评，对在政务数据安全保障工作中成绩显著和有突出贡献的单位和个人给予表彰；

（二）重要条款解读

1.职责与分工——各单位（第八条）

1. 编制政务数据安全规划，制定人员、资产、采购、外包、系统建设与运维、备份、应急等方面的政务数据安全管理制度；
2. 建立本单位政务数据安全管理部门，设置政务数据安全员专职岗位，落实政务数据安全责任制；
3. 采取技术措施和其他必要措施，保障政务数据安全，有效应对政务数据安全事件，防范违法犯罪活动；
4. 落实政务数据安全经费，建设和完善政务数据安全保障基础设施，开展政务数据安全等级保护、风险评估、安全自查、安全培训等工作，保护政务数据安全，制定信息安全应急预案，定期开展应急演练；
5. 建立政务数据安全信息通报制度，配合市数据资源局进行政务数据安全检查和事件调查，对发现问题进行整改；

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——一般规定

第九条:安全教育培训

各单位应当建立政务数据安全培训制度，定期开展政务数据安全意识教育与政务数据设备安全操作基础培训，对系统建设、运维人员和政务数据安全从业人员进行专项技能培训。

第十条:等级保护与整改

各单位应当按照国家等级保护制度要求和技术标准，建立等级保护制度，组织开展信息系统定级工作，将定级结果和备案证明材料报送所在地电子政务管理部门等数据安全管理部门。（《网络安全法》的要求）

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——一般规定

第十一条:风险评估和等级测评

各单位应当定期对政务信息系统安全状况开展风险评估。安全保护等级为第三级（含）以上的政务信息系统应当按照国家和行业有关规定进行等级保护测评；未达到安全保护等级要求的，应当进行整改。（三级以上系统每年都需进行等保测评工作）

第十二条：安全信息通报

各单位应当建立政务数据安全信息通报制度，开展信息通报工作，按照规定通报程序向电子政务管理部门报告有关情况，不得瞒报、缓报、谎报、迟报和推诿责任。（《网络安全法》的要求）

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——一般规定

第十四条: 采购管理

各单位应当选用符合国家有关规定、安全可控的信息技术产品和服务，采购的数据安全产品和服务应当经过国家认证。对数据做安全评估，并把评估结果作为项目立项的必备材料。（安全专用产品销售许可证制度、网络安全审查制度）

第十五条：外包服务和远程技术服务管理

各单位应当建立政务数据技术外包服务和远程技术服务安全管理制度，需要外包服务或远程技术服务的，应当与提供者签订安全保密协议。

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——一般规定

第三十条：政务数据共享安全管理

各单位应当建立政务数据共享管理制度，对于法律法规、规章和政策要求共享的政务数据予以安全保护。政务数据提供单位应当与政务数据获取单位签订政务数据使用和政务数据安全保护协议，明确政务数据共享内容、使用期限以及双方的权利、义务和责任。政务数据获取单位对于共享的政务数据具有相同的安全管理责任，政务数据提供单位应承担保密审查职责。

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——一般规定

- 其他应该履行的安全管理责任，与传统安全相似（第十七条至二十九条）

  - 物理环境安全
  - 网络边界安全防护
  - 外部系统接入管理
  - 网络接入内控管理要求
  - 对公共场所互联网服务管理要求
  - 系统安全管理
  - 系统变更管理
  - 网站和网上运行业务系统技术防护要求
  - 门户网站管理要求
  - 终端计算机安全防护
  - 移动存储介质管理
  - 系统和数据备份
  - 电子信息安全管理

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——对应急管理的要求

第三十一条:应急管理制度与管理机构

各单位应当建立政务数据安全应急管理制度，设立或者指定应急工作管理机构，负责应急管理工作。

第三十二条：应急预案与应急演练

各单位应当制定政务数据安全事件应急处置预案，定期开展应急演练，并对演练情况进行评估，针对演练中发现的问题，补充修订应急预案。

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——对应急管理的要求

第三十一条:应急管理制度与管理机构

各单位应当建立政务数据安全应急管理制度，设立或者指定应急工作管理机构，负责应急管理工作。

第三十二条：应急预案与应急演练

各单位应当制定政务数据安全事件应急处置预案，定期开展应急演练，并对演练情况进行评估，针对演练中发现的问题，补充修订应急预案。

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——对信息保护的要求

第三十五条:信息保护制度

各单位应当制定公民、企业信息保护制度，对在提供服务过程中收集、使用的公民、企业信息，应当采取相应措施严格保护，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第三十六条：收集使用信息的要求

各单位收集、使用公民、企业信息，应当遵循合法、正当、必要的原则，不得收集与其提供的服务无关的公民、企业信息，不得违反法律、法规的规定收集、使用和向第三方提供公民、企业信息。（收集数据需要目的明确、最少够用、公开透明）

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——对信息保护的要求

第三十五条:信息保护制度

各单位应当制定公民、企业信息保护制度，对在提供服务过程中收集、使用的公民、企业信息，应当采取相应措施严格保护，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第三十六条：收集使用信息的要求

各单位收集、使用公民、企业信息，应当遵循合法、正当、必要的原则，不得收集与其提供的服务无关的公民、企业信息，不得违反法律、法规的规定收集、使用和向第三方提供公民、企业信息。（收集数据需要目的明确、最少够用、公开透明）

（二）重要条款解读

2. 各单位政务数据安全管理的具体要求——对信息保护的要求

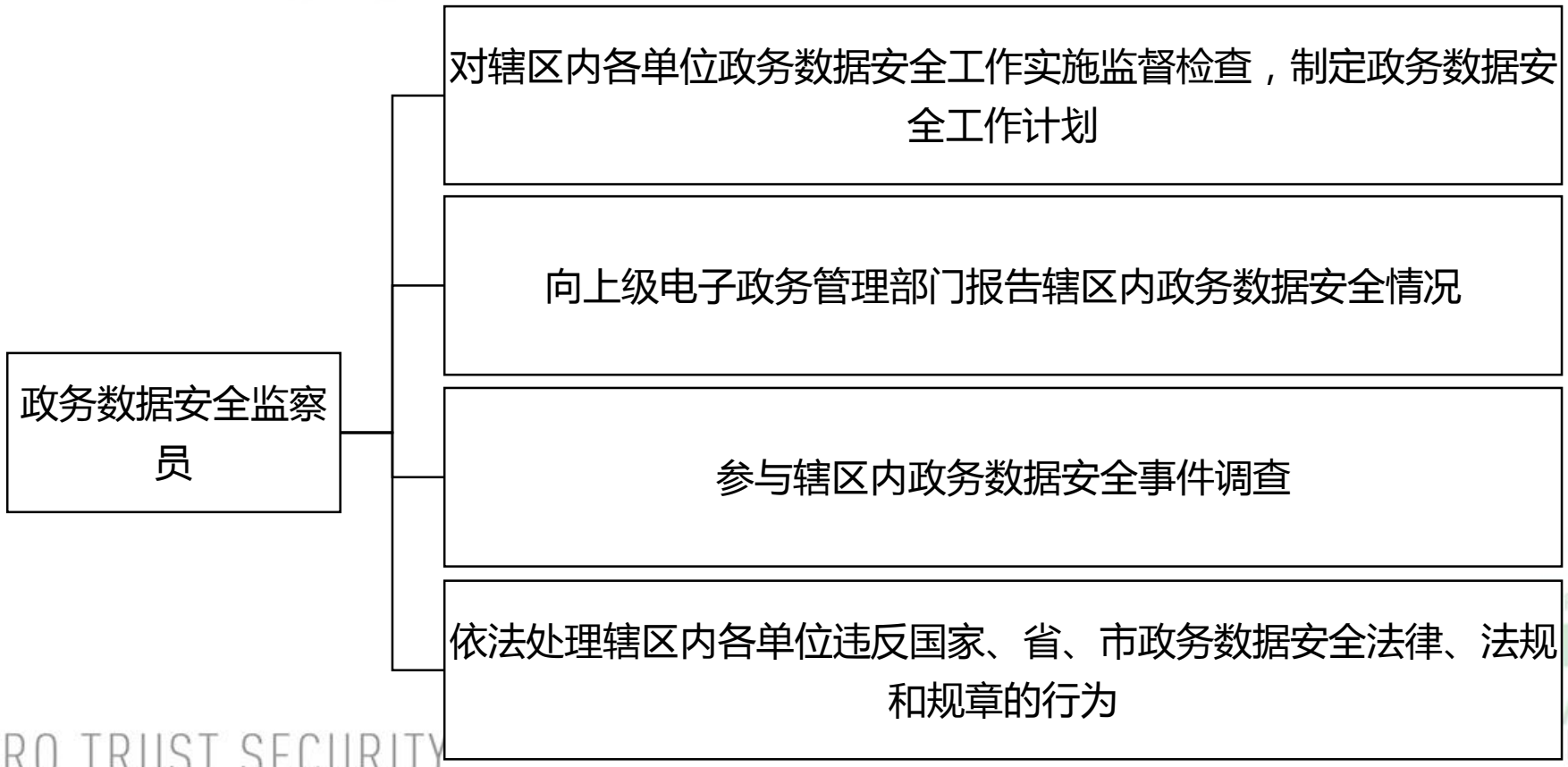
第三十七条:信息转移或委托的要求

各单位将公民、企业信息转移或委托给其他组织或机构使用的，应当与该组织或机构签订公民、企业信息保护协议，明确公民、企业信息使用范围和保护责任。（不得向不具备数据安全保护能力的机构转移数据）

特别是对个人信息的收集和使用，应遵照《网络安全法》、《个人信息安全规范》（GB/T 35273-2017）等要求执行。

3. 电子政务管理部门安全监督检查的具体要求

- 设立政务数据安全监察员角色



培训上岗

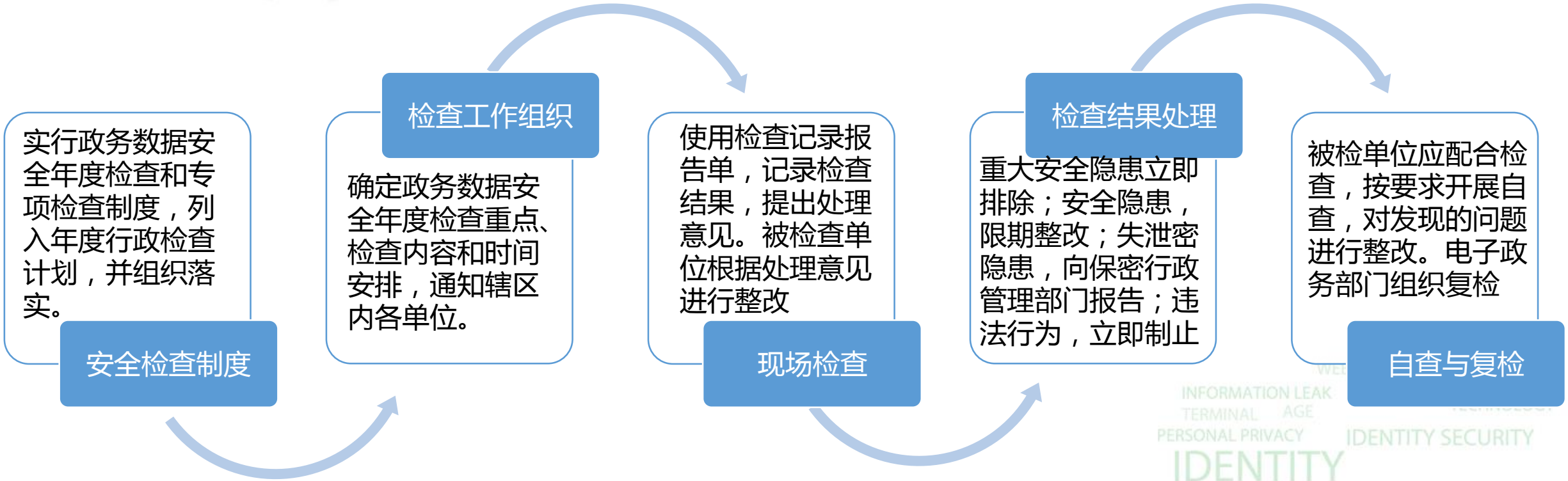
定期复训

年度考核

（二）重要条款解读

3. 电子政务管理部门安全监督检查的具体要求

- 参照管理办法第四十一到四十五条，进行辖区内政务数据安全检查



（二）重要条款解读

4. 政务数据安全事件调查的具体要求

◆ 参照管理办法第四十六到四十九条，对政务数据安全事件进行调查

启动条件

- 重大网络安全隐患、漏洞或基础网络、重要系统受到外部攻击遭到破坏的
- 重大政务数据安全事件
- 公民、企业信息或重要政务数据泄露，造成重大影响或经济损失
- 电子政务管理部门和重要单位的网站被篡改
- 国家、省、市政务数据安全主管部门通报的事件

调查组织

- 由市数据资源局或者由市数据资源局授权地方电子政务管理部门组织，被调查单位应当予以协助。

调查实施

- 调查组织部门成立事件调查组，开展调查工作。调查组可以调阅、摘抄、复制与政务数据安全事件有关的资料，封存有关设备，进行调查取证。

调查结果

- 调查组向调查组织部门提交调查报告。事件调查组织部门应当根据调查报告提出处理意见，并将事件调查资料归档。

（二）重要条款解读

5. 责任追究

- 各单位未履行职责，或者违法本管理办法相关要求的，由电子政务管理部门责令限期改正，逾期未改正的，将进行通报并在相关考核中扣分；造成安全隐患或者导致政务数据安全事件发生的，对责任单位主要负责人约谈；造成重大损失或者社会影响的，责令暂停相关业务，涉及违法犯罪的由公安机关依法查处。（第五十条）
- 电子政务管理部门工作人员不依法履行监督检查职责，或者有玩忽职守、滥用职权、徇私舞弊行为，尚不构成犯罪的，由有关部门依法予以行政处分。（五十三条）
- 使公民、法人或者其他组织的合法利益受到侵害的，依法承担民事责任。构成犯罪的，由公安机关依法追究刑事责任。（第五十四条）

第二部分

《杭州市政务数据安全保障体系规划》解读

ZERO TRUST SECURITY

规划出台的必要性和意义

规划出台的必要性

- 履行《网络安全法》的需要
- 落实国家大数据发展战略的需要
- 保护公民合法权益不受侵害的需要
- 满足新技术快速应用所带来的新要求的需要
- 推进杭州市“最多跑一次”改革的需要

规划出台的意义

提出了未来三年杭州市政务数据安全保障体系的总体目标、体系框架和建设内容，可有效指导各部门进行数据安全保障体系建设，提高政务数据资源的安全防护能力，促进杭州市大数据产业的健康发展。

安全现状与存在的问题

◆ 建设成就：

基础设施防护改善、管理水平稳步提升、数据安全防护能力增强

◆ 存在的主要问题：

- 顶层设计有待加强，标准规范不够健全
- 组织架构尚不健全，人员配备尚不完备
- 制度规程不够完善，管控措施覆盖不全
- 缺少技术防护手段，安全防护能力不足
- 云上系统保障不足，监管缺乏有效手段
- 缺乏联动防护机制，应急预案流于形式

规划提出的总体防护目标

◆ **总体目标：**

通过“顶层设计、健全管理、创新技术、协同运营、夯实基础”的数据安全保障体系建设，保障全市政务数据完整性、机密性和可用性，保障个人信息安全，保障国家重要数据安全。

◆ **分项目标：**

a) 建立全市数据安全顶层设计

b) 提升全市数据安全管理水平

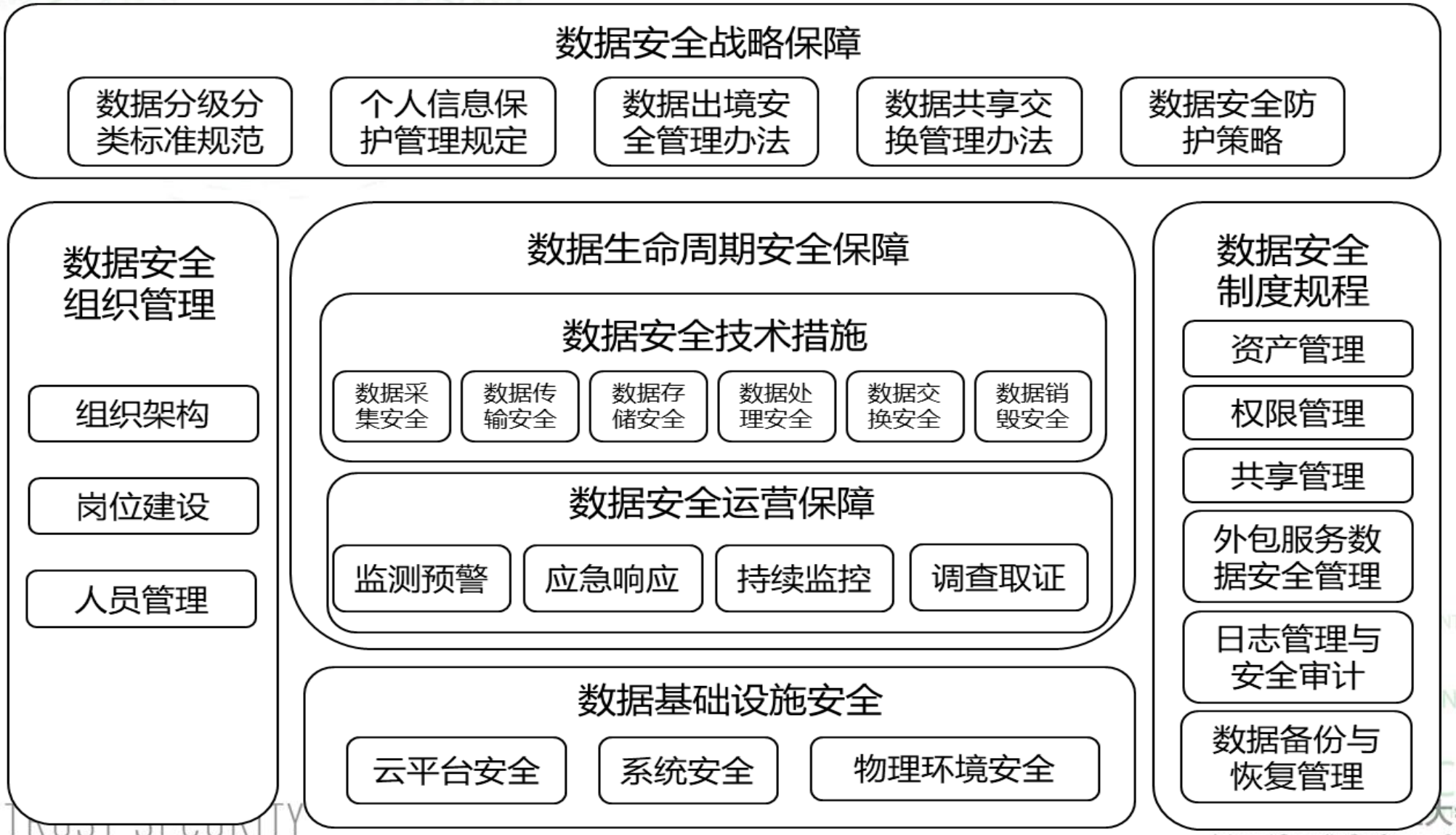
c) 补强数据安全“短板“

d) 加强数据安全运营监管

e) 提高数据应急恢复能力

f) 夯实基础设施安全保障能力

保障体系框架


数据安全战略保障
数据分级分类标准规范
个人信息保护管理规定
数据出境安全管理办法
数据共享交换管理办法
数据安全防护策略
数据安全组织管理
组织架构
岗位建设
人员管理
数据生命周期安全保障
数据安全技术措施
数据采集安全
数据传输安全
数据存储安全
数据处理安全
数据交换安全
数据销毁安全
数据安全运营保障
监测预警
应急响应
持续监控
调查取证
数据基础设施安全
云平台安全
系统安全
物理环境安全
数据安全制度规程
资产管理
权限管理
共享管理
外包服务数据安全管理
日志管理与安全审计
数据备份与恢复管理

建设内容

1.加强数据安全战略保障

- **建立数据分类分级标准规范**
  - 数据分类应以科学、稳定、实用和便于扩展为原则，便于数据的分析和利用
  - 数据分级是为了确定各类型政务数据的重要或敏感程度制定不同的共享策略
- **制定个人信息保护管理规定**
  - 目的明确、选择同意、最少够用、公开透明、确保安全、主体参与原则
  - 建立管理部门检查、第三方机构评估和用户投诉举报的监督机制
- **建立数据出境安全管理办法**
  - 出境数据涉及个人信息和重要数据时，需进行安全评估
  - 重点评估数据出境目的，目的不具有合法性、正当性和必要性的，不得出境

建设内容

1.加强数据安全战略保障

- **建立数据共享交换安全管理办法**
  - 明确数据共享交换平台的网络安全管理规范和技术要求
  - 数据提供部门“谁主管，谁提供，谁负责”，数据使用部门“谁经手，谁使用，谁管理，谁负责”，落实安全责任制
- **建立数据全生命周期的安全管控策略**
  - 数据采集/产生、数据传输、数据存储、数据处理、数据交换、数据销毁各阶段的安全管控措施

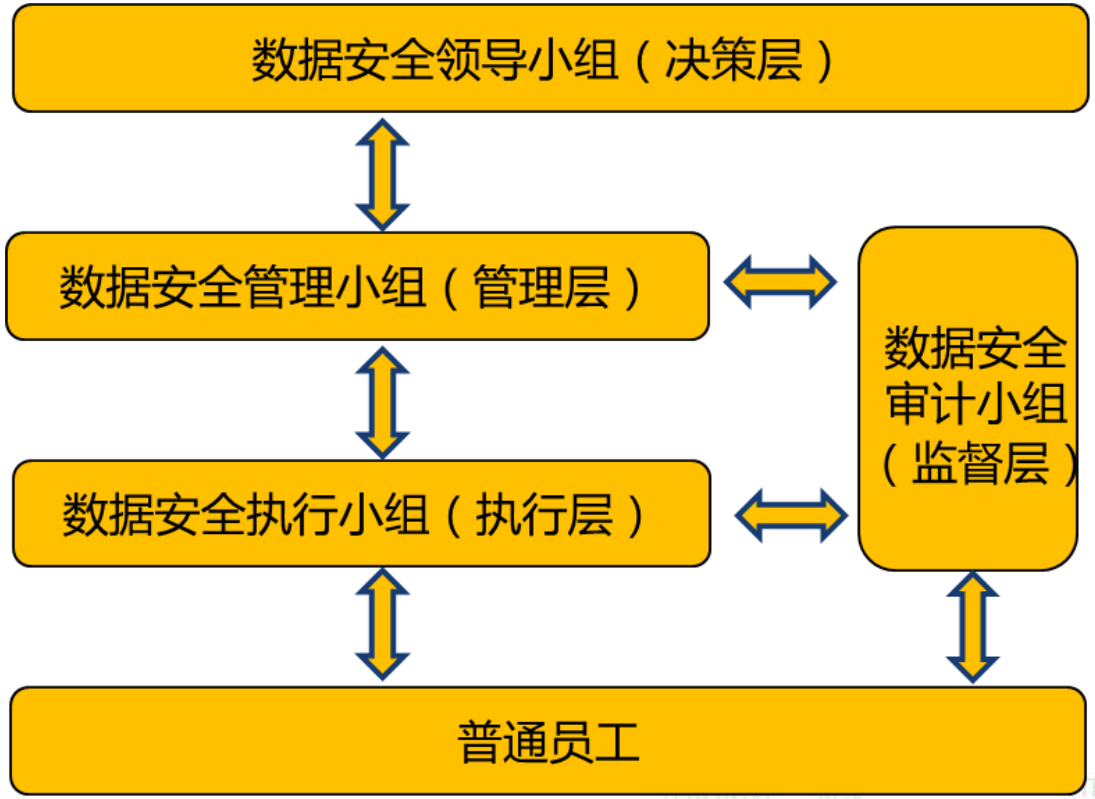
数据资源局和数据资源开发协会正在推进杭州市数据立法的相关事宜，完善战略保障内容。

建设内容

2.建立和完善数据安全组织管理

- 完善数据安全组织
  - 全市、各单位组织架构完善
- 落实数据安全岗位职责
  - 岗位职责覆盖数据生命周期
- 加强人员管理与教育培训
  - 加强人力资源管理
  - 加强教育培训

政务数据安全检查重点检查内容！



数据安全组织架构

建设内容

3.制定并落实数据安全管理制度与规程

- 信息系统与政务数据资产管理
- 用户访问权限管理
- 政务数据共享安全管理
- 外包服务数据共享管理
- 监测预警与应急响应管理
- 日志管理与安全审计
- 数据备份与恢复管理
- 数据归档安全管理

建议重点建设与落实的管理制度

建设内容

4.构建覆盖数据生命周期的技术防护手段

生命周期阶段	防护目标	技术手段
数据产生/采集	自动化的数据分类分级、质量控制	数据识别与自动化打标、在线质量监控工具
数据传输	数据传输的机密性和完整性保护	数据加密、安全通道（VPN）、可信通道
数据存储	防止敏感数据泄露，重要数据被破坏	存储数据加密、数据容灾备份、数据运维审计
数据使用	数据在授权范围内访问和处理	统一账号权限管理、数据脱敏和防泄漏、日志管理与审计、异常行为监控
数据交换	在授权范围内交换数据，数据交换过程安全	数据交换监控，通道加密
数据销毁	数据销毁后永久删除不可恢复	软硬件数据销毁工具

建设内容

5.提升数据安全运营保障能力

- 加强全市网络安全态势感知与通报预警能力
  - 形成覆盖全市电子政务网络及重要政务系统的安全态势感知与通报预警能力
  - 依托威胁情报的接入、大数据技术等进一步提高对网络攻击事件的预警能力
- 提高数据安全协同防御和应急指挥能力
  - 在各政务部门已有的政务数据安全事件应急响应体系基础上，建立覆盖全市的应急监控、快速响应、资源共享的全方位应急指挥体系。
- 提高数据安全持续监管能力
  - 定期开展对辖区内政务部门的数据安全监督检查和专项检查
  - 加强对第三方服务机构（云服务商、大数据服务提供商）的持续监督管理

建设内容

5.提升数据安全运营保障能力

- 落实安全事件调查取证和追责机制
  - 常态化的对符合事件调查启动条件的安全事件进行调查和取证，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。（依据《杭州市政务数据安全管理办法》）
- 探索网络数据安全保险形成风险管理闭环
  - 引入第三方网络数据安全风险服务机构和保险服务机构，通过技术手段和金融手段加强综合和闭环的网络安全风险管理手段

建设内容

6.保障数据基础设施安全——推动全市业务安全上云

“上云为常态、不上云为例外”，新的政务系统依托政务云平台建设，现有未迁移的政务系统逐步迁移至政务云平台。

制定杭州市政务系统入云安全指南，指导各政务部门在政务系统入云过程中采取合适的安全措施和执行必要的安全活动，控制安全风险，保障政务系统的入云安全。

建设内容

6.保障数据基础设施安全——加强政务云安全防护能力

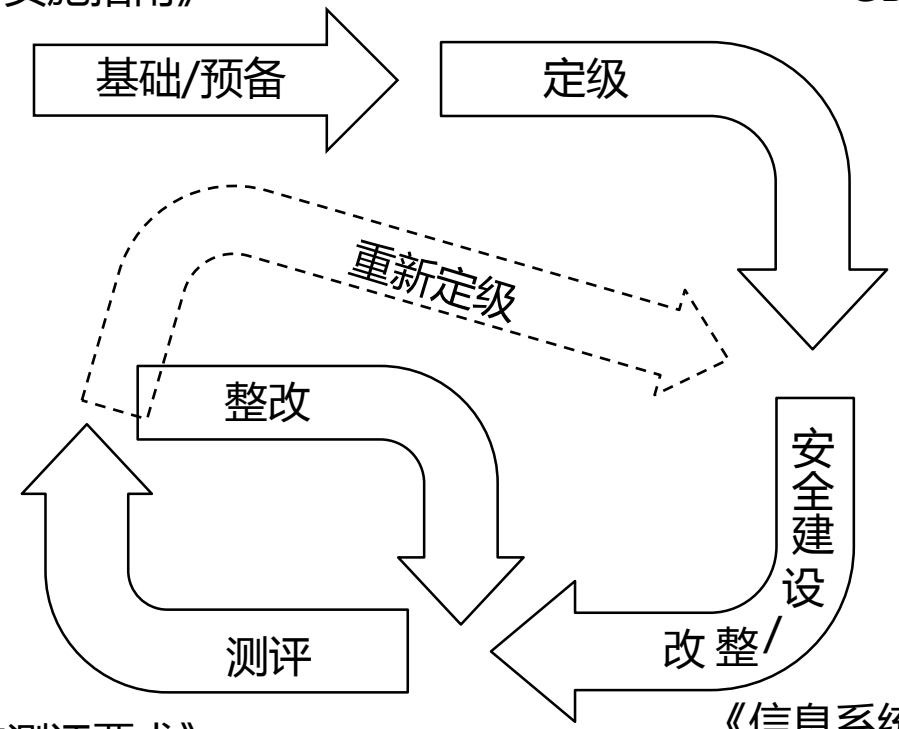
- 理清政务云各参与方的安全管理职责，合理划分管理权限，落实安全责任制
- 政务云服务商加强对政务云平台的安全防护建设，提供按需、弹性的安全防护资源服务
- 各政务部门加强云上政务系统的安全防护建设

建设内容

6.保障数据基础设施安全——落实网络安全等级保护制度

《计算机信息系统安全保护等级划分准则》
《信息系统安全等级保护实施指南》
GB 17859-1999
GB/T 25058-2010

《信息系统安全保护等级定级指南》
GB/T 22240-2008



GB/T 22239-2008
GB/T 25070-2010
GB/T 20271-2006
GB/T 20269-2006
《信息系统安全等级保护基本要求》
《信息系统定级保护安全设计技术要求》
《信息系统通用安全技术要求》
《信息系统安全管理要求》

GB/T 28448-2012
GB/T 28449-2012
《信息系统安全等级保护测评要求》
《信息系统安全等级保护测评过程指南》

建设步骤

- 第一阶段，围绕“顶层设计、健全管理、夯实基础”的建设目标
  a) 建立全市统一的规章制度和标准规范
  b) 建立基于大数据技术的网络安全监测预警和信息通报平台
  c) 完善全市数据安全管理组织机构及人员
  d) 完善各级政务部门数据安全制度体系
  e) 加强政务系统安全保障水平
- 第二阶段，围绕“创新技术、协同运营”的建设目标
  a) 加强数据生命周期安全防护能力，落实相关技术产品和工具
  b) 形成全市统一的通报预警与应急响应中心，具有主动防御能力
  c) 常态化的政务部门和第三方服务机构开展数据安全能力检查
  d) 落实数据安全事件的调查取证和责任认定机制

第三部分

杭州市政务数据安全责任落实情况检查

检查情况概述

目的	检查各单位《政务数据安全管理办法》的落实执行情况，数据安全责任书的落实情况。
时间	XXX月至XXX月
检查方式	单位自查（根据下发的检查表），实地抽查

重点检查内容

各区县（市）、开发区、管委会	市直属部门
1、数据安全组织建设情况	1、数据安全组织建设情况
2、数据安全制度制定和执行情况	2、数据安全制度制定和执行情况
3、数据安全培训开展情况	3、数据安全培训开展情况
4、辖区内数据安全检查落实情况	4、风险评估与等级保护落实情况
5、辖区内应急管理制度落实情况	5、应急管理制度落实情况
6、辖区内安全责任落实情况	6、数据安全责任落实情况

具体检查内容与检查方式

1.各区县（市）、开发区、管委会数据安全检查

检查项	检查内容	检查方式
数据安全组织建设情况	是否建立了本辖区数据安全管理领导小组，人员组成是否合理；	检查组织架构文件和任命文件
	领导小组的工作职责、范围和内容是否明确	检查领导小组工作责任文件
	是否定期召开领导小组会议，讨论和完善辖区内数据安全建设	检查小组会议纪要
数据安全制度制定和执行情况	是否制定了辖区内政务数据安全工作制度，明确辖区内各部门数据安全管理工作的重点内容，并提供相关管理制度模板	检查工作制度文件和管理制度模板
	是否对辖区内各部门的数据安全管理制度建设和落实情况进行了有效的监督和管理	检查对辖区内政务部门的监督检查记录文件

具体检查内容与检查方式

1.各区县（市）、开发区、管委会数据安全检查

检查项	检查内容	检查方式
数据安全培训开展情况	是否定期开展本辖区政务数据安全专项培训，培训计划、培训内容、培训方式是否合理	检查年度培训计划以及培训记录和人员签到表
辖区内数据安全检查落实情况	是否制定了辖区内政务数据安全检查制度，明确政务数据安全年度检查以及重要保障时期专项检查的范围、重点、方法及流程	检查年度检查计划，对于已开展年度检查的需要检查记录文件
	是否制定了年度检查计划	检查对辖区内政务部门的监督检查记录文件
	是否设立了政务数据安全监察员角色，相关人员是否签订了保密协议	检查政务数据安全监察员的任命文件以及保密协议是否齐备

具体检查内容与检查方式

1.各区县（市）、开发区、管委会数据安全检查

检查项	检查内容	检查方式
辖区内应急管理制度落实情况	是否建立了辖区内政务数据安全事件应急预案	检查政务数据安全事件应急预案文件
	是否建立了辖区内政务数据安全信息通报制度	检查政务数据安全信息通报制度文件，并按照制度文件规定的程序检查以往的通报记录。
	是否建立了政务数据安全事件调查制度和流程，明确了启动政务数据安全事件调查的条件、调查的组织人员、调查的实施方法、调查结果的处置等内容	检查政务数据安全事件调查制度文件
辖区内安全责任落实情况	是否明确了本辖区数据安全工作责任，将数据安全职责层层落实到具体部门、具体岗位和具体人员	检查数据安全责任清单，清单中应明确本单位负责政务数据监督管理的部门和人员，以及辖区内各部门政务数据安全的第一责任人。

具体检查内容与检查方式

2.市直属部门安全检查

检查项	检查内容	检查方式
数据安全组织建设情况	是否建立了本单位数据安全管理领导小组，人员组成是否合理；	检查组织架构文件和任命文件
	领导小组的工作职责、范围和内容是否明确	检查领导小组工作责任文件
	是否定期召开领导小组会议，讨论和完善辖区内数据安全建设	检查小组会议纪要
数据安全制度制定和执行情况	是否制定了本单位政务数据安全工作制度，管理制度是否齐备	检查政务数据安全管理制度文件及相关执行表单

具体检查内容与检查方式

2.市直属部门安全检查

检查项	检查内容	检查方式
数据安全培训开展情况	是否建立了政务数据安全培训制度，定期开展政务数据安全专项培训，培训内容和培训方式是否合理	检查年度培训计划和培训记录
风险评估与等级保护落实情况	本年度是否开展了风险评估活动，是否对发现的安全风险进行了整改	检查风险评估报告，检查安全措施整改情况
	本年度是否对三级以上系统开展了等保测评活动，是否对不符合项进行了整改	检查相关系统的等级保护测评报告，检查不符合项的整改情况

具体检查内容与检查方式

2.市直属部门安全检查

检查项	检查内容	检查方式
应急管理制度落实情况	是否制定了政务数据安全事件应急预案	检查政务数据安全事件应急预案文件
	是否定期组织开展安全检查、安全测试和应急演练工作	检查本年度开展的安全检查、安全测试与应急演练的执行记录文件
	在重大节日及敏感期间，是否按要求加强对重要信息系统的安全监控，加强值班，随时应对各类突发事件。	检查本年度开展的安全检查、安全测试与应急演练的执行记录文件
	是否对本部门发生的安全事件进行及时处置并按规定进行通报	抽查以往的安全事件应急处置记录文件，检查是否按照应急预案规定的时间进行应急处置和信息通报。
本部门安全责任落实情况	是否明确了本单位数据安全工作责任，将数据安全职责层层落实到具体部门、具体岗位和具体人员，	检查数据安全责任文件，文件中应明确本单位负责政务数据安全各环节的岗位、人员信息。


ISC
2018
ISC互联网安全大会
360互联网安全中心
谢 谢！
ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China