密级等级：机密
受控状态：受控
文件编号：CFSZ-SM-001-1.0

IT服务管理体系手册

2022年5月4日

泰州城发数字科技有限公司

变 更 履 历

版本	变更内容	编制人/ 创建日期	审核人/ 审核日期	批准人/ 批准日期	备注
V1.0	**初始版本，文档建立**	综合事务部 2022.5.4	史佳 2022.5.4	张俊 2022.5.4	

目录

01 手册的管理

1 IT服务管理手册的批准

管理者代表负责组织编制《IT服务管理手册》，总经理负责批准。

2 IT服务管理手册的发放、更改、作废与销毁

a）综合事务部负责按《文件控制程序》的要求，进行《IT服务管理手册》的登记、发放、回收、更改、归档、作废与销毁工作；

b）各相关部门按照受控文件的管理要求对收到的《IT服务管理手册》进行使用和保管；

c）综合事务部按照规定发放修改后的《IT服务管理手册》，并收回失效的文件作出标识统一处理，确保有效文件的唯一性；

d）综合事务部保留《IT服务管理手册》修改内容的记录。

3 IT服务管理手册的换版

当依据的ISO/IEC20000-1：2018标准有重大变化、组织的结构、内外部环境、生产技术、信息技术服务风险等发生重大改变及《IT服务管理手册》发生需修改部分超过1/3时，应对《IT服务管理手册》进行换版。换版应在管理评审时形成决议，重新实施编、审、批工作。

4 IT服务管理手册的控制

a）本《IT服务管理手册》标识分受控文件和非受控文件两种：

——受控文件发放范围为公司领导、各相关部门的负责人、内审员；

——非受控文件指印制成单行本，作为投标书的资料或为生产、销售目的等发给受控范围以外的其他相关人员。

b）《IT服务管理手册》有纸质文件和电子文件，电子版本文件的有效格式为PDF文档。

本手册由综合事务部提出、归口，并负责起草。

本手册主要起草人：综合事务部

本手册审核人：史佳

本手册批准人：张俊

02 颁布令

随着公司业务的开拓，为满足顾客有关信息技术服务的相关要求，提高公司信息技术服务管理水平，防止由于信息技术服务的不及时等导致的公司和客户的损失。公司开展贯彻 ISO/IEC 20000 《信息技术服务管理－规范》国际标准工作，建立、实施和持续改进文件化的信息技术服务管理体系，制定了泰州城发数字科技有限公司《IT 服务管理手册》。

《IT 服务管理手册》是企业的法规性文件，是指导企业建立并实施信息技术服务管理体系的纲领和行动准则，用于贯彻企业的信息技术服务管理方针、目标，实现信息技术服务管理体系有效运行、持续改进，体现企业对社会的承诺。

《IT 服务管理手册》符合有关信息安全法律、法规要求及 ISO/IEC 20000-1：2018 《信息技术服务管理－规范》标准和企业实际情况，现正式批准发布，2022 年 5 月 4 日起实施。企业全体员工必须遵照执行。

全体员工必须严格按照《IT 服务管理手册》的要求，自觉遵循信息技术服管管理方针，贯彻实施本手册的各项要求，努力实现公司信息技术服务管理方针和目标。

公司总经理：张俊

日期：2021-03-01

03 人事任免书

1、 为贯彻执行信息技术服务管理体系，满足 ISO/IEC 20000 《信息技术服务管理－规范》标准的要求，加强领导，特任命 史佳 为我公司信息技术服务管理者代表。

授权代表有如下职责和权限：

a、按照 ISO/IEC 20000 《信息技术服务管理－规范》的要求，组织相关资源，识别、建立、实施和保持信息技术服务管理体系，不断改进信息技术服务管理体系，确保其有效性、适宜性和符合性。

b、根据服务管理的策略和目标，给与权利和责任，以保证服务管理过程的设计，提升和改进；

c、确保服务管理流程与 SMS 的其它组件进行了整合；

d、确保资产，包括许可证，根据法律法规要求和合同义务，被用于管理交付服务；

e、向公司最高管理者报告信息技术服务管理体系的业绩，如：服务方针和服务目标的业绩、客户满意度状况、各项服务活动及改进的要求和结果等。

f、组织 ISO/IEC 20000 体系的管理评审，主持信息技术服务管理体系内部审核，推动内部审核活动。

g、推动公司各部门领导，积极组织全体员工，通过工作实践、教育培训、业务指导等方式不断提高员工对满足客户需求的重要性的认知程度，以及为达到公司服务管理目标所应做出的贡献。

h、负责与信息技术服务管理体系有关的协调和联络工作；

2、 授权公司 史佳 为 IT 服务管理项目责任人，其主要职责（角色）和权限为：确保 IT 服务管理体系得到形成、实施、运行和控制。

3、 授权各部门主管为 IT 服务管理体系在本部门的责任人，对 ITSMS 要求在本部门的实施负责。

本授权书自任命日起生效执行。

公司总经理：张俊

日期：2022 年 5 月 4 日

04 企业概况

一、 公司基本情况

城发数科是在市委、市政府关心和支持下，由城投集团控股与省电信合资成立的数字新基建公司，公司以“做泰州数字化转型主力军”为使命，以建设高科技现代化国有企业为目标，聚焦“新城建、新引擎、新能力”，致力于提升沉淀本地数字化自主研发、自主运营能力，助力数字政府、数字经济、数字民生、数字服务建设与运营，推动本土数字产业做大做强。

新城建方面：聚焦城市信息模型 CIM、建筑信息模型 BIM、智能市政基础设施、城市安全平台、城市综合管理、智慧社区、智能建造等领域，助力构建提升城市品质和人居环境质量、提升城市管理水平的信息数字化城市基础设施体系。

新引擎方面：致力工业智改数转，深入行业研究、建设生态体系，为企业智改数转提供诊断评估、规划设计、解决方案等服务，助力泰州及周边地市企业的数字化转型、产业提档升级。

新能力方面：集聚软件研发、数据治理、安全运营等高层次人才，不断探索创新应用，沉淀本地软件研发、平台运营、数据运营、信息安全服务等能力，推动泰州本土数字产业做大做强，加强自有产品和能力输出，打造区域数字科创基地。

公司名称：泰州城发数字科技有限公司

所在地址：泰州市海陵区凤凰路 88 号 19 层

电话号码：

05 信息技术服务方针目标

为防止由于信息技术服务的不及时所导致的企业和客户的损失，本公司建立了信息技术服务管理体系，制订了信息技术服务方针，确定了信息技术服务目标。

本公司信息技术服务管理方针包括内容如下：

服务管理方针：

提升服务意识　创造服务价值

公司 IT 服务管理目标：

1) 客户回访满意率达到 90%以上；
2) 事件解决率达 95%以上；
3) 客户投诉及时处理率达到 95%；
4) 重大变更成功率达到 95%；

范围

1) 本手册之规定适用于 IT 服务相关所有部门及部门人员；具体涉及部门及角色，见附录一 IT 服务管理组织结构；

服务范围：

计算机信息系统运行维护服务

IT服务管理手册

1 范围

1.1 总则

为了建立、实施、运行、监视、评审、保持和改进文件化的信息技术服务管理体系（简称ITSMS），确定信息技术服务方针和目标，对信息技术服务及信息安全进行有效管理，确保全体员工理解并遵照执行信息技术服务管理体系文件、持续改进信息技术服务管理体系的有效性，特制定本手册。

1.2 应用

1.2.1 覆盖范围

本IT服务管理手册规定了泰州城发数字科技有限公司信息技术服务管理体系要求、管理职责、内部审核、管理评审和信息技术服务管理体系改进等方面内容。

1.2.2 删减说明

本IT服务管理手册采用了ISO/IEC20000-1：2018标准正文的全部内容，无删减。

2 规范性引用文件

下列文件中的条款通过本《IT服务管理手册》的引用而成为本《IT服务管理手册》条款。凡注日期的引用文件，其随后所有的修改单或修订版均不适用于本标准，然而，管理者代表应研究是否可使用这些文件的最新版本。凡不注日期的引用文件、其最新版本适用于本IT服务管理手册。

ISO/IEC 20000-1:2018《信息技术-服务管理体系-要求》

ISO/IEC 20000-2:2005《信息技术-服务管理实施指南》

ISO/IEC 20000-3:2009《信息技术-服务管理范围定义和适用性指南》

3 术语和定义

ISO/IEC 20000-1:2018《信息技术-服务管理体系-要求》、ISO/IEC 20000-2:2005《信息技术-服务管理实施指南》、ISO/IEC 20000-3:2009《信息技术-服务管理范围定义和适用性指南》规定的术语和定义适用于本《IT服务管理手册》。

3.1 本公司

指泰州城发数字科技有限公司，包括泰州城发数字科技有限公司所属各部门。

3.2 服务可用性

一项服务或服务组件在指定的时间或时间段完成要求的功能的能力。

注：可用性通常可以用客户实际使用服务或服务组件的时间与约定服务时间的比率或百分比来表示。

3.3 配置项

为交付一项或多项服务需要控制的元素。

3.4 绩效

可测量的结果。

3.5 事件

计划外的服务中断、服务质量下降或尚未对客户服务造成影响的事态。

3.6 信息安全

保持信息的保密性、完整性和可用性

3.7 信息安全事件

单个或一系列意外或突发的、具有损害业务运营和威胁信息安全的极大可能性的事态。

[ISO / IEC 12207：2018,3.28]

3.8 已知错误

已找到根本原因或已有方法可降低或消除对其服务的影响的问题。

3.9 问题

造成一个或多个事件的根本原因。

3.10 发布

将一项或多项变更的结果，将一组一个或多个新的变更的配置项部署到实际运行环境。

3.11 变更请求

对服务，服务组件或服务管理体系进行改变的提议。

3.12 风险

不确定性的影响

3.13 服务

通过帮助客户达成预期的结果而向客户交付价值的手段。

3.14 服务组件

一项服务的单个单元，该单元与其它单元结合可交付一项完整的服务。

3.15 服务连续性

按照商定的服务可用性或连续无中断交付服务的能力。

3.16 SLA 服务级别协议

服务提供方和客户之间定义服务和服务指标的形成文件的协议

3.17 服务管理

一组能力和过程，用以指挥和控制服务提供方设计、转换、交付和改进服务的活动和资源。

3.18 SMS 服务管理体系

指挥和控制服务提供方的服务管理活动的管理体系。

3.19 服务提供者

为客户提供一项服务或多项服务的组织。

3.20 服务请求

请求提供信息、建议、服务访问或预先批准的变更。

3.21 服务要求

客户和用户对服务的需求，包括服务级别要求，以及服务提供方的需求和服务管体系要求以及义务。

其他术语详见术语表

4.0 组织环境

4.1 理解组织及其环境

最高管理者应确定与本公司质量目标和战略方向相关并影响实现服务管理体系预期结果的各种内部因素（公司的价值观、文化、知识、绩效等相关因素）和外部因素（国际、国家、地区和当地的各种法律法规、技术、竞争、文化和社会因素等）。这些因素可以包括需要考虑的正面和负面因素或条件。

本公司定期对这些内部和外部因素的相关信息进行监视和评审，以确保其充分和适宜。

具体见《公司环境分析控制程序》。

4.2 理解相关方的需求和期望

公司应确定：

a）服务管理体系及服务的相关方；

b）相关方的要求；

公司应对这些相关方及其要求的相关信息进行监视和评审，以便于理解和持续满足相关方的需求和期望。

本公司应考虑以下相关方：

--顾客；

--最终用户或受益人；

--业主，股东；

--银行；

--外部供应商；

--雇员及其他为组织工作者；

--法律法规及监管机关；

--地方社区团体；

--非政府组织；。

理解相关方的需求和期望可以帮助本公司更好的建立清晰的方针和目标，做到目的明确。满足相关方的要求并争取做到更高的期望值。具体见《相关方需求和期望控制程序》。

4.3 确定服务管理体系范围

本公司应明确服务管理体系的边界和适用性，以确定其范围。

在确定范围时，本公司应考虑：

a）4.1 中提及的各种内部和外部因素；

b）4.2 中提及的要要求；

C) 组织交付的服务。

根据本组织产品和服务特点，标准的所有条款均适用于本组织并决定全部予以实施。

本公司服务管理体系的范围详见 1.2 章节

4.4 服务管理体系

本公司确保按照本标准的要求，建立、实现、维护和持续改进服务管理体系，包括其所需要过程及其相互作用。

5 领导

5.1 领导和承诺

最高管理者应通过以下方面，证实其对服务管理体系的领导作用和承诺：

a) 确保指定服务管理体系的服务方针和服务目标，与战略方向一致；

b) 确保服务管理计划的创建、实施和维护，以支持服务管理方针，实现服务管理目标和服务要求；

c) 确保关于服务管理体系和服务决策授权合理分配；

d) 确保为组织确认的客户创造价值；

e) 确保对服务生命周期的相关方进行控制和管理；

f) 确保将服务管理体系要求整合到组织过程中；

g) 确保服务管理体系及服务所需资源可用；

h) 沟通有效的服务管理的重要性，实现服务管理目标；交付价值和符合服务管理体系要求；

i) 确保服务管理体系达到预期效果；

j) 指导并支持相关人员为服务管理体和服务的有效性做出贡献；

k) 促进服务管理体系和服务持续改进；

l) 支持其他相关管理者在其职责范围内发挥领导作用，以证明他们在其责任范围内的领导作用。

5.2 方针

5.1.1 制定服务管理方针

最高管理者制定服务体系方针，方针应考虑并满足以下内容：

a) 适应本公司的宗旨和环境并支持其战略方向；

b) 为建立服务管理目标提供框架；

c) 包括对满足适用的服务管理相关要求的承诺；

d) 包括对持续改进服务管理体系及服务的承诺。

本公司的服务管理方针，详见“服务管理方针”

5.1.2 沟通服务管理方针

服务管理方针应：

a) 可获得并保持文件信息；

b) 在组织内得到沟通；

c) 适用时，可为相关方获取。

5.3组织的角色，责任和权限

公司最高管理者依据制定的组织结构图(见附件B)，对各部门与岗位的职责、权限和相互关系进行明确规定，以保证整个组织内的相关权限得到分派、沟通和理解，以：

取保服务管理体系符合ISO/IEC20000-1：2018要求；

向最高管理者报告管理体系和服务绩效。

本公司IT服务管理团队由体系负责人、IT服务管理委员会、内审组以及各过程与人员组成。具体角色职责及定义参见《IT服务管理角色与职责说明》

本公司IT服务管理体系定义和实施的过程包括：

1）服务提供过程：

a) IT服务级别管理；

b) IT连续性和可用性管理；

c) IT能力管理；

d) IT安全管理；

e) IT预算和核算管理。

2）控制、发布过程：

A）IT配置管理；

B）IT变更与发布管理。

3）解决过程：

A）IT事件管理；

B）IT问题管理。

4）关系过程

A）IT业务关系管理；

B）IT供应商管理。

在每个过程的过程描述文档中，将对过程的范围、目标、角色职责、活动交互、绩效指标及评价方法进详细的定义。

1） 各过程之间的接口

过程之间的接口定义和通过接口的信息传递将在过程定义文档中进行详细的描述，在此对IT服务管理各过程之间的接口简要描述。

本公司IT服务管理体系以IT服务级别管理过程为核心，以IT配置管理为基础，将IT服务管理体系中的各过程串联起来。

IT服务级别管理过程为多个过程提供输入，各过程也将服务级别协议（SLA）要求的执行情况估为输出返回到IT服务级别管理过程。

IT配置管理过程为IT服务支持过程及部分IT服务交付过程提供所有需要的配置项及其属性信息，并接受来自IT变更发布管理对配置信息的修改。

5.3.1 管理者代表

公司任命了管理者代表，并授与了相应的权利和责任，详见管代任命书；

6.1 应对风险和机遇的措施

本公司在基于考虑到服务管理体系标准4.1&4.2条款所提出的问题和要求，制定《风险和机遇控制程序》，明确过程运行中的风险和机遇事件的识别方法/途径、风险和机遇事件的评估方式、制定并实施主要风险和机遇事件的应对措施的要求、评价这些措施有效性的方法。以便：

a）确保服务管理体系可达到预期结果；

b）预防或减少不利影响；

c）实现服务管理体系和服务的持续改进。

6.1.2 本公司去人和形成文件化信息：

a) 有关的风险：

1) 组织；

2) 不满足服务要求；

3) 服务生命周期中的相关方；

b) 风险对客户的影响和服务管理体系及服务的机遇；

c) 风险接受标准

d) 风险管理的方法

6.1.3 本公司应策划：

a) 应对风险和机遇的措施及优先级；

b) 如何：

1) 将这些措施整合到服务管理体系过程中；并予以实现；

2) 评价这些措施的有效性。

6.2.1 制定目标

本公司在相关职能和层次上制定服务管理目标。

服务管理目标满足：

a) 与服务管理方针保持一致；

b) 可测量；

c） 考虑适用的要求；

d） 予以监视；

e） 予以沟通；

f） 适当时更新。

本公司服务管理目标详见本手册 0.5 章

6.3 策划服务管理体系

本公司制定、实施和维护服务管理计划。计划考虑到服务管理方针，服务管理目标，风险与机遇，服务要求和本标准的要求。

服务清单

影响服务管理体系和服务的已知限制；

有关的方针，标准和法律法规要求、合同的义务；

服务管理体系和服务的权限、职责；

运行服务管理体系和服务的所需的人员、技术、信息和财务资源；

服务生命周期中和相关方采取的工作方法；

支持服务管理体系的技术；

如何测量、审核、报告和改进服务管理体系和服务的有效性。

7 支持

7.1 资源

本公司确定提供建立、实现、维护和持续改进服务管理体系和运行服务所需的人员、技术、信息和财务资源，已满足服务要求和实现服务管理目标。

7.2 能力

本公司IT服务管理委员会须对所有参与IT服务管理的岗位和岗位责任做明确定义。

以确保服务工作人员的工作应符合服务要求，这些人员应在接受相应的教育和培训后，具备相应的技能和经验等基本能力。服务人员应当：

a） 选择有资质的人员；

b） 适当通过提供培训或采取其它措施以获得必要的能力资格；

c） 对采取措施的有效性进行评价；

d） 确保其工作人员都知道如何尽力达成服务管理目标并满足服务要求；

e） 坚持对教育、培训、技能和经验做适当的记录。

IT服务管理委员会同时须通过培训或其他的宣讲等方式来确保员工理解他们的业务活动的重要性以及相关性，并知晓如何达成IT服务管理的目标。

7.3 意识

本公司取保在其控制下的工作人员知晓：

a） 服务管理方针；

b） 服务管理目标；

c） 与工作有关的服务；

d） 对其服务管理体系有效性的贡献，包括改进绩效带来的益处；

e） 不符合服务管理体系要求带来的后果。

7.4 沟通

本公司确定与服务管理体系和其服务相关的内部和外部的沟通，包括：

a） 沟通什么；

b） 何时沟通；

c） 与谁沟通；

d） 谁负责沟通。

公司建立并保持《信息交流管理程序》对该过程进行控制

7.5 成文信息

7.5.1 文件的建立和维护

公司在开发、经营、服务和日常管理活动中，按ISO/IEC 20000-1:2018标准要求，建立、实施、运行、监视和评审、保持和改进文件化的信息技术服务管理体系。IT服务管理体系文件分以下几个层次：

a） 一级文件：服务管理策略和目标的文件；（如： IT服务管理手册包括方针、目标）；

b） 二级文件：文档化的服务管理流程或程序；（如：IT服务管理体系的程序文件）；

c） 三级文件：为本部分ISO / IEC 20000要求的特殊流程所创建的文档化的策略和规划、文档化的服务目录、文档化的SLA、服务管理计划的文档，包括：管理规范、操作手册及作业指导书以及为确保有效操作SMS和交付服务所需的并由服务提供者决定补充的外来文件。

d） 四级文件：IT服务管理体系的产出物文件模版（表单、报告模版等）；

7.5.2 文件控制

本公司编制了《文件控制程序》具体按文件控制程序要求进行控制。记录是一种特殊类型的文件，并且需要按照7.5.2节的要求被控制。

一个文档化的流程，包括授权和责任，控制的定义需要被建立，需要有：

a） 在发行前建立和批准文件，以保持适宜和重复性；

b） 予以妥善保护（如防止泄密、不当使用、或者缺失等）；

c） 必要时对文件进行检查和保持；

d） 确保文件的改动和现行修订状态是经认可的；

e） 确保适用文件的有关版本在使用时可获得；

f） 确保外来文件得以识别且其发行量受到控制；

g） 若保留作废文件，需防止作废文件被随意使用并对上述文件做好适当的标识；

h） 取保文件版本变更控制（例如版本控制）；

i） 确保文件存储和保护，包括保持可读性。

7.5.3 记录控制

本公司编制了《记录控制程序》具体按记录控制程序要求进行控制。

记录应保存，并用来证实SMS符合要求和有效运作。

一个文件的流程需要建立对控制的定义，包括标识、贮存、保护、检索、保存和记录的处置的方式。

记录应清晰，易于识别和检索。

7.5.4 服务管理系统成文信息

服务管理体系的成文信息包括：

a） 服务管理体系范围；

b） 服务管理的方针和目标；

c） 服务管理计划；

d） 变更管理方针、信息安全方针和服务连续性计划（一个或多个）；

e） 服务管理体的过程；

f） 服务要求；服务目录；

g） 服务级别协议（SLA）；

h） 与外部供应商的合同；

i） 与内部供应商和充当供应商的客户的协议；

j） ISL/IEC20000-1:2018标准要求的程序；

k） 证明符合ISL/IEC20000-1:2018标准和服务管理体系要的记录。

7.6 知识

公司应确定和保持必要的知识，已运行服务管理体系和服务。这些知识应予以保持，并在需要范围内可得到。

为应对不断变化的需求和发展趋势，公司制定《组织知识管理程序》以确定如何获取更多必要的知识，并进行更新。

组织知识是从其经验中获得的特定知识，是实现组织目标所使用的共享信息。组织知识可以基于：

a）内部资源（如：知识产权、从经验获得的知识、从失败和成功项目中获得的教训、获取和分享未形成文件的知识和经验、过程、产品和服务的改进结果）；

b）外部资源（如：标准、学术交流、专业会议以及从顾客和外部供方收集的知识）

8 运行

8.1 运行策划和控制

本公司策划、实现和控制满足要求所需的过程，通过下列内容以及实现风险和机遇中确定的措施；

a) 基于要求、建立过程的准则；

b) 按照准则实施过程控制；

c) 本公司保持成文信息达到必要的程度，以确信这些过程按计划得到执行。

8.2 服务组合

8.2.1 服务交付

本公司运行服务管理体系，取保协作活动和资源。本公司执行交付服务所需的活动。

8.2.2 服务策划

a) 智慧城建、系统集成事业部应当组织对新的或变更的服务进行测试，以验证它们是否符合服务要求和设计文件。新的或更改的服务应由智改数转事业部和有关方面事先约定验收标准。如果服务不符合验收标准，智慧城建、系统集成事业部和有关各方应当做出必要的决定和部署的行动。

b) 发布和部署管理过程应用于部署已批准的新的或变更的服务到真实环境。

c) 随着转化活动的完成，服务提供者应当及时向有关方面报告关于对预期成果取得的成效。

8.2.3 控制服务生命周期的相关方

8.2.3.1 物流任何相关方涉及到支持服务生命周期中执行活动，本公司对 ISO/IEC20000-1：2018 的要求和交付的服务负责。

本公司确认和应用 ISO/IEC20000-1：2018 评估和选择服务生命周期中的其它相关方。其它相关方可以是外部供应商、内部供应商和客户冲淡的供应商。

其它相关方不应提供和运行服务管理体系范围内所有的服务、服务组件或流程。

本公司确认和成文化下列内容：

a) 其它相关方提供和运行的服务；

b) 其它相关方提供和运行的服务组件；

c) 其它相关方运行的服务管理体系范围内的流程或部分流程。

8.2.3.2 本公司对其相关方定义和应用下列控制措施：

a) 测量和评估过程绩效；

b) 测量和评估服务、服务组件满足服务要求的有效性。

8.2.4 服务目录管理

本公司创建和维护一个或多个服务目录。服务目录包括描述服务的组织、客户、用户和其他相关的信息、他们预期的结果和服务间依赖关系。

a) 智慧城建、系统集成事业部负责与相关部门沟通，制订公司的《服务目录》。服务目录应定义所有服务，并包含服务名称、服务目标或标准、联系接口、服务提供时间和例外、安全方面的考虑和安排。

b) 《服务目录》是公司所提供的服务内容的汇总，公司与客户签署 SLA 时应参考《服务目录》。

c) 公司应该根据当前的服务能力对《服务目录》进行更新与维护。

8.2.5 资产管理

办公室取保管理用于交付的服务的资产满足服务要求和有关的方针、标准和法律法规要求、合同的义务。

8.2.6 配置管理

8.2.6.1 智慧城建、系统集成事业部应根据《配置管理程序》的要求，评估所有与IT服务相关的重要资产和配置项，识别、定义、维护IT服务和基础设施的组件，明确配置项之间的关系、属性和作用，定义命名规范、版本号，制订和实施《配置项分类定义表》，以确保有效管理IT资产和配置。

8.2.6.2 每个配置项均有唯一标识，并记录在CMDB中,同时每个配置项记录的信息记录应包括:

a）配置项的说明；

b）配置项和其它配置项之间的关系；

c）配置项和服务组件之间的关系；

d）状态；

e）版本；

f）位置；

g）有关更改请求；

h）相关的问题和已知错误。

8.2.6.3 被管理的配置项主要包括：信息系统和软件（包括第三方软件）的发布、相关系统文档、例如要求规范、设计、测试报告、发布文档、每个应用环境配置基线、或描述应用环境、标准硬件组成和发布、备份和电子资料库、如最终软件库（DSL）、配置管理包或工具、许可证、安全组件、如防火墙、服务相关文档、例如服务级别协议、活动程序、务支持设施、例如机房电源。

8.2.6.4 智慧城建、系统集成事业部根据配置项之间的关系、属性、状态类别、重要程度和优先级，确定配置管理数据库的范围、分解的层数、详细的程度，完成配置管理数据库的构建。

8.2.6.5 智慧城建、系统集成事业部制订《配置管理计划》，并每年末进行更新。主要包括：配置管理的范围、目标、策略、标准角色和责任、配置管理过程定义服务和基础设施中配置项，配置控制变更，记录和报告配置项情况，证实配置项的完整性和正确性责任、可检索、可审计的要求，如出于安全、法律、规章或业务目的、配置控制（访问、保护、版本、开发、发布控制）、交互控制过程，及信息接口和发布、资源管理策划和建立，以便使资产和配置受控，并维持配置管理系统，如培训活动、与配置相关的供应商管理要求和活动。

8.2.6.6 综合管理在配置管理过程中应监控配置项的整个生命周期，确保只有被授权且可识别的配置项才被接受，并记录从接受到销毁的全过程；没有被认可的变更请求，不能添加、修改、替换或删除配置项。

8.2.6.7 智慧城建、系统集成事业部应保存有效的配置记录，以反映配置项状态、位置和版本的变化，并通过各种状态监控配置项的变更，例如订购、接收、测试、使用、变更、拆卸、取消。配置项的更新信息应作为配置管理计划和变更管理的输入。

8.2.6.8 为保护系统、服务和基础设施的完整性和安全性，配置项信息应被保存在一个安全环境。应：保护其不受未授权访问、变更或破坏、提供灾害后恢复方法、对受控软件、测试产品和支持文档等备份的恢复进行限制。

8.2.6.9 配置评审程序应包含缺陷记录、执行纠正措施和报告结果。

8.2.6.10 智慧城建、系统集成事业部应定期填写《配置项管理记录》，包括：配置项最新版本、配置项的位置和软件主要版本的位置、相互依赖关系、版本历史。在任何时候都可核对配置项以下内容：服务配置项或系统、变更、基准线、开发或发布、版本或变量。

8.2.6.11 智慧城建、系统集成事业部应定期组织相关部门实施配置认可和审核活动，并检查是否有充分的资源以支持：保护物理配置和公司的知识资本、确保公司控制其配置、原件和许可证、确保配置信息是准确、可控、可见。

8.2.6.12 智慧城建、系统集成事业部应确保变更、发布、系统或环境符合其合同约定或事先约定的要求且配置记录是准确的。

8.2.6.13 在审核中出现的缺陷或不符合项应被记录、评估和改进。

8.3 关系和协议

8.3.1 总则

本公司使用供应商以：

a) 提供和运行服务

b) 提供和运行服务组件；

c) 运行服务管理体系范围内的流程或部分流程。

8.3.2 业务关系管理

8.3.2.1 智改数转事业部应当建立目录包括所有客户、用户和各利益相关方，并对于每一个客户应当指定专人负责管理客户关系管理和客户满意度。

8.3.2.2 智改数转事业部按照《业务关系管理程序》要求，牵头并定期组织智改数转事业部，开展服务管理评价活动，讨论、汇报服务范围、SLA、合同或业务需求的变化，及性能、成绩、结果和措施计划，形成会议纪要。

8.3.2.3 当服务目标、服务需求、支持合同、业务等发生新增、变更或撤销时，智慧城建、系统集成事业部应按《新的或变更的服务设计管理程序》的要求，提出并评估服务范围和SLA的改进方案，由智慧城建、系统集成事业部组织实施。

8.3.2.4 智改数转事业部与客户建立有效的互动、沟通关系，以便及时了解客户的需求或重大变更，并依据需求进行响应。根据《业务关系管理程序》，定义、收集、分析客户满意度数据和信息，监控客户满意度的趋势。

8.3.2.5 智改数转事业部根据《业务关系管理程序》中的客户投诉管理过程，负责收集、统计、分析客户投诉的记录，识别投诉的发展趋势和存在问题，确保服务的连续性目标的实现。同时联络客户在计划的时间间隔复审服务的表现。

8.3.3 服务级别管理

8.3.3.1 根据公司的战略策划、资源要求及客户需求，智慧城建、系统集成事业部在与智慧城建、系统集成事业部和其他相关部门沟通、确定 SLA 时，应考虑：可接受持续损失服务的最大周期、可接受降级服务的最大周期，服务恢复时，可接受降级服务级别。

8.3.3.2 智改数转事业部代表客户，与智慧城建、系统集成事业部签订《服务级别协议》应明确：服务要求和期望服务工作量特征的协议、服务目标协议、服务级别实现、工作量的测量和报告，以及服务目标不能完成的分析与说明。

8.3.3.3《服务级别协议》包含以下内容：服务的简述、术语表、客户职责、智改数转事业部职责和义务、服务目标、服务时间、工作量限制（最大及最小工作量），支持和相关服务、影响和优先级描述、授权细节，及授权人员联系信息、有效期或 SLA 变更控制机制（包含升级和通知过程）、服务中断采取的纠正措施，计划和协调中断，包括通知事件及频率、沟通的简述，包括报告、投诉程序、在 SLA 中规定条款的例外情况。

8.3.3.4 智慧城建、系统集成事业部应依据与客户签订的 SLA 以及《供应商管理程序》的要求，组织签署与供应商之间的支持合同（或协议），并应由相关方定期评审。

8.3.3.5 当出现重要业务变更时，智改数转事业部应及时与智慧城建、系统集成事业部部沟通，按原过程重新组织相关部门，调整、修订《服务级别协议》，并作为服务改进计划的输入。

8.3.4 供应商管理

8.3.4.1 智慧城建、系统集成事业部按《供应商管理程序》的要求，指定专人管理与供应商的关系、合同和绩效。并对供应商提供的 IT 服务的过程进行管理，完善供应商管理制度和采购规范，建立和维护公司《合格 IT 供应商名单》,并确保：

a）供应商了解其对本公司承担的责任。

b）服务要求满足协议约定的服务级别和范围。

c）管理变更。

d）记录与相关各相关方的业务交流。

e）了解所有供应商的业绩并采取相应改进措施。

8.3.4.2 智慧城建、系统集成事业部负责组织相关部门对供应商提供服务的所满足的需求、范围、服务级别、接口和沟通过程等进行评审并达成一致，按公司正式授权，组织签署与供应商之间的支持合同或供货协议。主要包含以下内容：

a) 供应商提供的服务范围；

b) 服务、流程和各方之间的依赖关系；

c) 供应商必须满足的要求；

d) 服务目标；

e) 供应商在与其它各方在服务管理过程中的接口；

f) 在 SMS 中供应商的所有行为；

g) 工作量特点；

h) 合同的例外情况，以及将如何处理这些情况；

i) 服务提供者和供应商的权力和责任；

j) 由供应商提供的报告和信息；

k) 收费的依据；

l) 预计终止或提前终止合同，及将服务转让给第三方时的行为和责任。

8.3.4.3 智慧城建、系统集成事业部负责拟制公司《合格 IT 供应商名单》，并负责《合格 IT 供应商名单》的维护和管理。

8.3.4.4 当公司与供应商的支持合同或供货协议需要修订或变更时，智慧城建、系统集成事业部应重新组织相关部门进行合同评审，在评审中应讨论和明确对本公司 SLA 影响和变更，并按照《变更管理程序》的要求实施。

8.3.4.5 智慧城建、系统集成事业部按《供应商管理程序》的要求，对公司合格供应商进行年度评审，监督、记录供应商对本公司 SLA 的落实情况，拟制《供应商合作分析报告》，将评定的结果及时反馈给相关供应商，并组织进行相关调整和改进。

8.3.4.6 智慧城建、系统集成事业部应组织管理与供应商之间的合同冲突，并在支持合同或供货协议中明确。如果争议无法通过正常途径解决时，应交由更高级别的解决途径。

8.3.4.7 智慧城建、系统集成事业部应确保所有合同冲突被记录、调查、解决并正式关闭。

8.3.4.8 对每一个内部供应商和充当供应商的客户，智慧城建、系统集成事业部应开发、协商和维护成文的协议，以定义服务等级目标，其他承诺活动和相互间的借口。

8.4 供应与需求

8.4.1 服务预算和核算

8.4.1 编制《服务的预算和核算管理程序》，明确服务的预算和核算过程与其它财务管理流程之间应有的接口。

8.4.2 应当有以下内容的策略和书面流程：

a) 应对支出进行预算，以便开展有效的财务控制和为决策制定提供服务。

b) 服务提供者应当监测和报告预算的支出，审查财务预算，从而管理成本。

注：许多服务提供者对服务费进行记账。对预算编制和核算范围的服务过程中不包括赊账。

8.4.3 智慧城建、系统集成事业部应根据国家的有关法律法规和财务政策，以及公司的业务策略（包括产品策略、销售策略、服务策略等），组织拟制、审核本部门的总体性和阶段性的IT服务费用预算及成本标准。

8.4.4 服务组件的预算和核算应至少包括；

a）资产 - 包括用于提供服务的许可证，

b）共享资源，

c）管理费用，

d）资本和运营开支，

e）外部提供的服务，

f）人员， 设施；

g）将间接成本和直接成本分配给各项服务，为每个服务提供一个整体成本；

h）有效的财务控制和审批。

8.4.5 智慧城建、系统集成事业部根据公司业务发展战略、公司现有的SLA要求，及本部门业务的特点，按部门工作计划的内容，组织拟制本部门阶段性的费用预算计划，经计划财务部汇总、报批后实施。

8.4.6 在预算期间出现的服务变更引起的预算变化，相关部门应按变更管理流程的要求执行预算变更申请。

8.4.7 在对《服务级别协议》进行评审时，计划财务部应根据公司策略，评估实现服务目标和需求的成本，并根据确定的服务级别协议跟踪成本的变化。

8.4.8 计划财务部应根据预算跟踪财务变化，并对超出预算要求的变化，提前向相关部门提出预警信号.

8.4.2 需求管理

本公司每年度管理评审时，对需求进行管理，包括：

a) 确定服务当前需求和预测未来需求；

b) 监视和评审需求与服务使用情况

8.4.2 能力管理

8.4.3.1 智慧城建、系统集成事业部负责现有IT服务系统能力水平的策划，根据《能力管理程序》的要求，制订《能力计划》，应在计划中描述业务需求，应包括：

a）现行的和预计的服务需求；

b）协议要求对可用性，服务的连续性和服务级别的预期影响；

c）升级服务能力的时间范围、阀值和成本；

d) 法律、法规、合同或组织变更的潜在影响；

e) 新技术，新工艺的潜在影响；

f) 能够进行预测分析的程序，或它们的引用。

g) 为达到SLA所要求的服务级别目标和业务需求所应具备的人员技能、技术可行性、信息和财务资源的能力。

8.4.3.2 智慧城建、系统集成事业部应当与客户和有关方面确定并认同能力和性能要求，当出现临时的新增或变更服务引起能力计划需要进行变更时应通过变更管理过程来控制。

8.4.3.3 智慧城建、系统集成事业部应当监测能力的使用，分析能力数据并优化性能。该服务提供者应提供足够的能力以完成协议能力和性能要求。

8.5 服务设计、构建与转换

8.5.1 变更管理

8.5.1.1 变更管理方针， 制定变更管理方针， 公司变更管理方针为：**区分变更类型，遵守变更流程。**

8.5.1.2 本公司形成的相应程序将应用于所有新的有可能变更的服务，这对服务和客户将产生重大影响。变更由变更管理策略控制，对于新的或变更的服务的评估、审批、调度和审查范围的变更应当由变更管理流程控制。新的或变更的服务范围的配置项影响应由配置管理流程控制。

8.5.1.3 公司IT服务管理委员会应当审查新的或变更合同约定的服务要求以及新的或变更的服务计划，设计和开发新的或变更的服务过程中有关规定给予的规划和设计活动的输出。在此基础上，应当接受或拒绝输出。同时应当采取必要行动，以确保发展和新的或变更的服务可以进行有效的转化，采用公认的输出。

8.5.1.4 智改数转事业部负责与客户沟通，智慧城建、系统集成事业部配合，收集客户对现有SLA的满意度水平。分析、整理客户新的或变更服务的要求，及时反馈客户的改进需求。

8.5.1.5 当出现新服务或变更服务时，智慧城建、系统集成事业部根据《新的或变更的服务设计管理程序》的要求，组织实施服务管理和提供服务策划和实施工作。

8.5.1.6 智慧城建、系统集成事业部组织对新服务或变更服务策划结果的验证、确认，验证通过后按《新的或变更的服务设计管理程序》实施。

8.5.1.7 智慧城建、系统集成事业部应报告新服务或变更服务按计划实施所达到的结果，智慧城建、系统集成事业部按《发布管理程序》，执行实施发布评审，比较实际结果与期望结果的一致性。

8.5.1.8 新的或变更的服务计划

1) 公司智慧城建、系统集成事业部应确定新的或变更的服务的要求。新的或变更的服务应当被规划以符合服务要求。新的或变更的服务的规划应由客户和利益相关方认可。

2) 作为计划的输入，智慧城建、系统集成事业部应当考虑到提供新的或变更的服务潜在的财务、组织和技术上的影响。智慧城建、系统集成事业部也应考虑到新的或变更的服务对SMS的潜在影响。

3) 新的或变更的服务的计划应包含或引用包括但不限于以下内容：

a）设计、开发和转化活动的权力和责任；

b）活动应当由以下各方履行：服务提供者和包括与服务接口的其它各方；

c）与各利益相关方沟通；

d）人员、技术、信息和财务资源；

e）计划活动的时间表；

f）对风险的确定，评估和管理；

g）依赖的其它服务；

h）新的或变更的服务的测试要求；

i）服务验收标准；

j）用可衡量的术语表示提供新的或变更的服务的预期输出。

4）对于要被删除的服务，智慧城建、系统集成事业部应做出服务删除计划。计划应包括删除、归档、处理数据，文件和服务组件的转移的日期。服务组件可以包括基础设施和与应用程序相关的许可证。

5）智慧城建、系统集成事业部应当对那些致力于新的或变更的服务组件条款的各方加以识别鉴定。应当评估其能力以满足服务需求。评价的结果应当予以记录并采取必要的行动。

8.5.2 服务设计与转换

8.5.2.1 策划新的或变更的服务

8.5.2.1.1 智慧城建、系统集成事业部负责对新的或变更的服务进行设计和文档化时应至少包含以下内容：

a） 交付新的或变更的服务时的权力和责任；

b） 提供新的或变更的服务时服务提供者、客户和其他各方需执行的活动；

c） 新的或变更的人力资源需求，包括对适当的教育、培训、技能和经验的要求；

d） 交付新的或变更的服务时的财政资源需求；

e） 新的或变更的技术来支持提供新的或变更的服务；

f） 新的或改变的计划和策略，要求符合本部分的 ISO / IEC 20000；

g） 新的或变更合同和其它文件的变化协议，以配合服务变更要求；

h） 对 SMS 的变更；

i） 新的或变更的服务水平协议；

j） 对服务目录进行更新；

k） 在交付新的或变更的服务过程中使用的程序、措施和信息。

8.5.2.1.2 智慧城建、系统集成事业部应当确保设计使新的或变更的服务满足服务要求。

8.5.2.1.3 新的或更改服务，应当按照文件化的设计制定。

8.5.2.1.4 新的或变更的服务的转化

a) 智慧城建、系统集成事业部应当组织对新的或变更的服务进行测试，以验证它们是否符合服务要求和设计文件。新的或更改的服务应由智改数转事业部和有关方面事先约定验收标准。如果服务不符合验收标准，智慧城建、系统集成事业部和有关各方应当做出必要的决定和部署的行动。

b) 发布和部署管理过程应用于部署已批准的新的或变更的服务到真实环境。

c) 随着转化活动的完成，服务提供者应当及时向有关方面报告关于对预期成果取得的成效。

8.5.3 发布与部署管理

8.5.3.1 智慧城建、系统集成事业部根据《变更管理程序》的要求，结合业务对信息系统、基础设施、服务和文档等进行策划，识别发布的内容、种类、层次、影响等，制订发布策略来配置发布活动，包括：发布频度和类型、发布管理的角色和责任、发布测试和实施的授权、所有发布的唯一标识和描述、分组变更以进行版本发布、为提高效率和可重复性，建立、安装、发布分发过程自动化方法、发布的验证和接受。

8.5.3.2 智慧城建、系统集成事业部根据需要负责制订《发布方案》，确保相关的信息系统、基础设施、服务和文档得到认可、授权、预定、协调和跟踪。一般包括：发布日期和交付描述、本次发布关闭或解决的相关变更、问题和已知错误，以及在发布测试期间被识别的已知错误、在可行的情况下，为每个实施地点制订一份活动计划、如发布失败，可以被撤销或修复的方式、验证和验收过程、对客户和服务支持人员的交流、准备、备案和培训、采购、存储、分发、联系、接受和销毁商品的后勤工作和过程、确保服务级别所需的支持资源、可能对发布测试和实施造成影响的相关变更和风险的标识、与相关人员、客户代表安排的更新、评审会议。

8.5.3.3 当进行重大升级时，智慧城建、系统集成事业部组织安排仿真环境的验证和评审，确保发布进入生产时与预期状态一致。发布的结果包括发布通告、安装指南、基于相关配置基准线的已安装软硬件等。

8.5.3.4 智慧城建、系统集成事业部按《发布方案》的安排，组织上线实施工作。并及时向智慧城建、系统集成事业部反馈上线成功的验证信息。如果发布未成功，则应按《发布计划》中制订的撤销计划的内容，实施回退操作，并将发布情况及时报告智慧城建、系统集成事业部。

8.5.3.5 智慧城建、系统集成事业部对发布未成功的原因进行确认，如需重新实施变更，则按《变更管理程序》的要求执行。如属潜在问题引起的发布未成功，则应按《问题管理程序》的要求执行。

8.5.3.6 发布成功后，智慧城建、系统集成事业部应及时将发布信息对配置管理数据库进行更新,并对事件、问题知识库进行更新。

8.5.3.7 智慧城建、系统集成事业部负责发布文档的保存。并负责上线文档的保存。

8.5.3.8 智慧城建、系统集成事业部组织对 IT 服务系统的运行监控，收集系统运行信息，完成《月度服务质量分析报告》。

8.6 解决与完成

8.6.1 事件和服务请求管理

8.6.1.1 智慧城建、系统集成事业部智改数转事业部按照事件定义文件及《事件和服务请求管理程序》的要求，根据事件的影响和紧急程度确定事件处理优先级别，并基于优先级别确定解决事件的目标。其中应包括：

a）接收请求、记录、优先级分配、分类。

b）一线事件解决或转移。

c）考虑安全事件。

d）事件跟踪和生命周期管理。

e）一线客户联系。

f）事件升级。

g）事件解决、验证和关闭。

8.6.1.2 事件报告方式包括电话、拜访、传真或者电子邮件，所有事件应在智改数转事业部正式记录，并可检索和分析。

8.6.1.3 智慧城建、系统集成事业部对升级的事件提供解决方案，协助智改数转事业部关闭事件。

8.6.1.4 智慧城建、系统集成事业部负责对升级的技术问题提供处理事件的技术支持，协助智改数转事业部解决未知错误。

8.6.1.5 智慧城建、系统集成事业部组织建立事件知识库，以确保智改数转事业部人员可访问经常更新的知识库。知识库中包括技术专家、以前事件、相关问题、已知错误、配置管理数据库（CMDB）、检查清单等有助于恢复服务的各种信息。

8.6.1.7 对重大事件的处理，智慧城建、系统集成事业部按相关要求执行。

8.6.1.8 智慧城建、系统集成事业部应在证实事件已经解决并且服务已经恢复的时候，事件才能最终关闭。

8.6.2 问题管理

8.6.2.1 智慧城建、系统集成事业部根据《问题管理程序》对问题原因的预先识别、分析、管理直至关闭，以减少对业务的影响。对问题过程应确定以下方面内容:

a）确定问题；

b）记录问题；

c）优先顺序分配；

d）分类；

e）更新记录；

f）升级；

g）解决；

h）关闭。

8.6.2.2 智慧城建、系统集成事业部根据日常检查、测试、事故数量和类型的趋势分析等纠正措施，识别潜在问题、确定其根本原因和其潜在的预防措施。所有被识别的问题都应该得到记录。

8.6.2.3 在问题得到解决后，智慧城建、系统集成事业部将相关信息应加入问题知识库，智慧城建、系统集成事业部同时应升级所有相关文件，如用户指南和系统文件。应对该问题解决的有效性进行监测，复审和报告。

8.6.2.4 记录对服务或问题管理过程的改进，并作为服务改进计划的输入,同时最新的已知的错误和问题解决方案应提供给事件管理和服务请求管理流程。

8.7 服务保障

8.7.1 服务可用性和服务连续性管理

8.7.1.1 智慧城建、系统集成事业部应当评估和记录服务的连续性和服务可用性的风险。并确定并与客户和有关各方就服务的连续性和可用性要求达成一致。同时应对业务计划的适用性、服务要求、SLA和风险予以考虑。 与客户纸定的服务连续性和可用性要求致少包括：

a) 获得服务的权利；

b) 服务响应时间；

c) 点对点服务的可用性。

8.7.1.2 智慧城建、系统集成事业部应按照《服务连续性和可用性管理程序》的要求，拟制《服务连续性和可用性计划》，根据客户业务优先级、服务级别协议和评估的风险，按设计的工作量计划维护有效的服务能力，并与《服务级别协议》的目标保持一致。应考虑：

a) IT服务连续性和可用性计划考虑可用性的要求和目标以及对服务和系统组成的关系。

b) 应清晰的分配调用IT服务连续性和可用性计划的责任，并清晰的计划对每个目标采取措施的责任。

c) 备份服务恢复所需的数据、文件、软件、任何设备和必要员工，在重大服务失败或灾难时，保持快速有效。

d) 在远程的安全地点，所有IT服务连续性和可用性文件应存储和维护至少一份，与其他必要的设备保存在一起。

e) 当不能正常进入服务位置时，可获得服务的连续性计划，联系人名单和CMDB。

f) 针对服务的连续性计划和可行性计划的变化需求，智慧城建、系统集成事业部应组织相关部门评估其影响。

8.7.1.3 服务的连续性和可用性的监控和测试

1) 定期开展IT服务连续性计划的测试。使员工理解调用、执行计划的角色与职责，并能访问IT服务连续性文件。

2) 智慧城建、系统集成事业部每年末组织对《服务连续性和可用性计划》进行评审，并根据业务需求的变化及时调整计划的内容和目标，确保从普通到重大服务失效的任何环境下都能满足与客户协商的要求。

3) 当业务环境发生重大变化时，智慧城建、系统集成事业部应重新组织评审、修订《服务连续性和可用性计划》。并通过能力管理和配置管理活动，评价所有服务组成的有效性，预知可能的、潜在的问题，并采取预防措施。

4) 对《服务连续性和可用性计划》中内容和目标的变更，智慧城建、系统集成事业部应及时组织相关部门按《变更管理程序》的要求进行评估、验证和确认，确保变更的效果及满足SLA的要求。

5) 智慧城建、系统集成事业部应定期对可用性信息进行测量和记录，应对计划之外的不可用性进行被调查、评估，并采取适当的纠正或预防措施。可用性活动包括：

a) 监控和记录服务的可用性、服务准确的历史数据。

b) 与SLA中定义需求相比较，以识别不符合SLA有效目标的事项。

c) 记录不符合项，并组织评审。

d) 考虑、评估供应商的影响。

e) 预计未来的可用性。

8.7.3 信息安全管理

8.7.3.1 信息安全策略

8.7.3.1.1 本公司制定有《信息安全管理程序》，描述相关风险的控制，及运行和维护控制的方式。

8.7.3.1.2 考虑到服务的要求和法律法规要求和合同义务，指派有相应的安全负责人以管理审批信息安全策略。安全负责人应具备以下方面的职责：

a) 与服务提供者、客户和供应商相关人员沟通信息安全策略，以及遵守该策略的重要性；

b) 确保信息安全管理目标的完成；

c) 明确管理信息安全风险所采取的方法和接受风险的准则；

d) 确保信息安全风险评估是在计划的时间间隔进行的；

e) 确保信息安全内审的进行；

f) 确保对审核结果进行评审，以确定改进的机会。

8.7.3.2 信息安全控制措施

8.7.3.2.1 根据公司业务及SLA要求，智慧城建、系统集成事业部组织制订信息安全管理策略、目标，并负责识别、分类信息安全资产，并对信息安全资产实施和操作物理的、管理的和技术的信息安全控制措施进行以便：

a) 保证信息资产的保密性，完整性和可用性；

b) 满足信息安全策略的要求；

c）实现信息安全管理目标；

d）管理信息安全的相关风险。

8.7.3.2.2 对这些信息安全控制应作记录，并说明与控制相关的操作和维护的风险。 包括:

a）提供服务所需要的信息安全资产目录。

b）根据信息安全资产对服务的重要性以及所要求的保护级别对信息安全资产进行分类，并指派相应的安全负责人。

c）对信息安全资产实施安全风险评估，并应考虑以下因素：

d）特性（例如软件漏洞、运行错误、通信失败）。

e）发生的可能性。

f）潜在的业务影响。

g）信息安全政策目标，满足客户特定安全需要以及所采用的法规条例。

h）历史经验。

8.7.3.2.3 智慧城建、系统集成事业部应当复审信息安全控制的有效性,采取必要的行动并对所采取的行动进行报告。

8.7.3.2.4 智慧城建、系统集成事业部应当具有识别那些需要访问，使用或管理信息和服务的外部组织,并对这些外部组织进行归档，协商并实施信息安全控制。

8.7.3.3 信息安全事件

信息安全事件应：

a)记录和分类

b)考虑信息安全风险，进行有先排序

c)需要时，升级；

d)解决；

e)关闭。

绩效评价

9.1 监视、测评、分析和评价

本公司建立了内部审核及管理评审控制程序等以及SMS的有效性和服务效果进行监督和度量。以证实SMS和各项服务的能力可以实现服务管理目标并达到服务的要求。同时已识别不符合本部分的ISO / IEC 20000-1:2018的要求，包括服务提供者或服务要求确定SMS的要求。

同时应对内部审核和管理评审的结果予以记录，其中包括不符合项，关注以及确定的行动。应将结果和行动通知各利益相关方。

9.2 内部审核

9.2.1 本公司编制有《内部审核控制程序》明确了审核计划、实施审核，报告结果和保存审计档案的权力和责任，同时公司在计划的时间间隔内进行内部审计，以确保SMS和服务是否：

a) 履行本ISO / IEC 20000的规定；

b) 符合服务要求和服务提供者确定的SMS要求；

c) 得到有效地实施和维护。

9.2.2 在编制审计方案时应考虑过程和被审计领域的地位和重要性，以及以往审核的结果。应对审计准则，范围，频率和方法进行记录。

9.2.3 审计师的选择和审核的实施应确保其客观性和公正性。审核人员不应审核自己的工作。

应对不符合项进行通报，并进行排序和责任分配并采取行动。被审计的该部分负责人须确保任何纠正和纠正措施，不得无故迟延，及时消除不合格项及其成因。后续活动应包括对所采取措施的行为验证和结果报告。

9.2.4 本公司 IT 服务管理团队须采取方法对 IT 服务管理体系的过程加以监控及测量，包括例行检查（管理评审：偏重于查变化---外部变化：法律法规/客户，内部变化：人员变化/组织机构变化（对公司的冲击）、内部审核---偏重于查风险）和日常检查（偏重于查符合/不符合，即合策划检查定期回顾，关注绩效、成果、问题和纠正计划），以确保体系的运行与设计相符，并根据检查结果采取纠正与预防措施，确保各过程目标的达成。

9.3 管理评审

9.3.1 本公司编制有《管理评审控制程序》对评审策划及实施作了描述。最高管理者应在计划的时间间隔内对SMS和各项服务进复核，以确保其持续的适宜性和有效性。复核需要包括对SMS开展的必要更改的重要性进行评估，包括服务管理的策略和目标。

对管理评审的输入应包括但不限于以下信息：

a) 以往管理评审提出的措施的状态；

b) 与服务管理体系相应的外部和内部因素的变化；

c) 有关服务管理体系绩效，包括以下方面的趋势：

1） 不符合和纠正措施；

2） 监视和测量结果；

3） 审核结果；

d) 持续改机改进的机遇；

e) 客户和其它相关方反馈；

f) ISO/IEC20000-1:2018服务管理方针和其它方针的遵循性、适宜性；

g) 实现服务管理目标；

h) 服务绩效；

i) 服务生命周期中其它相关方的绩效；

j) 当前和预测的人员、技术、信息和财务资源界别，和人、技术资源资源能力；

k) 风险评估的结果、应对风险和机遇措施的有效性；

1） 影响服务管理体系和服务的变更；

管理评审输出应包括与持续改进机遇相关的决定以及变更服务管理体系和服务的任何需求。

管理评审的记录应予以保留。

9.4 服务报告

9.4.1 智慧城建、系统集成事业部应就向客户提交的服务报告的内容、报告周期与客户协商并达成一致。

9.4.2 智慧城建、系统集成事业部拟制内部服务报告，对计划间隔内的客户服务状况、问题趋势、服务数据、SLA目标实现等进行汇总、统计和分析，组织召开月度服务质量分析会议，形成会议纪要后发放。

9.4.3 服务报告主要包括的内容：执行服务级别目标的绩效，违反SLA、安全管理要求等的不符合项和结论、工作量特征，如能力、资源利用、报告主要事件、变更、定期趋势信息、客户满意度分析。

9.4.4 服务报告应及时、清晰、可靠和简明，便于分析、决策和有效沟通。

9.4.5 当出现有关IT服务系统配置项的变更时，智慧城建、系统集成事业部应按《变更管理程序》的要求执行。

10 改进

10.1 不符合及纠正措施

10.1.1 若出现不合格，包括投诉所引起的不合格，应对不合格做出反应，适用时：

a） 采取措施，以控制并予以纠正；

b） 处置后果；

10.1.2 通过以下活动，评价是否需要采取措施，以消除不符合的原因，避免其再次发生或其他场合发生：

a） 评审不符合；

b） 确定不符合的原因；

c） 确定类似的不符合是否存在，或可能发生

10.1.3 实现任何需要的措施；

10.1.4 评审任何所采取措施的纠正措施的有效性；

10.1.5 保持不符合，纠正措施的成文信息。

10.2 持续改进

10.2.1 本公司将形成一个对SMS和各项服务持续改进的策略。该策略应包括改善机会的评价标准。同时本公司已建立《纠正和预防措施控制程序》包括对改进的鉴定、记录、评估、审批、优先级管理、测量和报告的权力和责任。改善机会包括纠正和预防措施，应记录在案。

应对已确定的不符合的原因予以纠正。应采取纠正措施以查明并消除不符合的原因，以防止再次发生。应当采取预防措施，以消除潜在不合格的原因，以防止发生。

a） 日常检查：在例行的本公司IT内审和IT管理评审之外，本公司IT服务管理团队还须按需开展日常检查来确保IT服务管理体系的持续改进。

b） 相关（事件、问题、变更、信息安全、业务关系、连续性、可用性和能力管理）过程需定期（每月一次）对本过程运行效果进行总结研讨，针对发现的问题，须提出改进措施并执行。

c） 各过程负责人需须定期（每年一次）对本过程执行效果进行总结研讨，必要时对过程文件进行修订、评审和发布。

10.2.2 管理改进

改进的机会应被优先考虑。本公司在对持续改进策略的改进机会做决定时，应使用评价标准。对批准的改进内容加以规划。同时应当管理改进的活动，包括但不限于：

a） 设置改进目标，包括质量、价值、能力、成本、生产力、资源利用率、风险降低等方面；

b） 确保对批准的改进得以实施；

c） 在需要时修改服务管理策略、计划、过程和流程；

d） 对照设定的目标检查改进完成的情况，对没有实现的目标，采取必要的行动；

e） 对改进实施情况予以报告。

f） 本公司IT服务管理团队根据IT服务管理体系检查阶段的结果，采取改进措施不断改善IT服务管理和服务交付，逐步提高IT服务管理和服务交付的效果和效率，内容包括：

1） 根据 IT 内审不合格项进行根源分析并加以改进，并根据 IT 内审结果决定是否需要对部分服务进行调整；

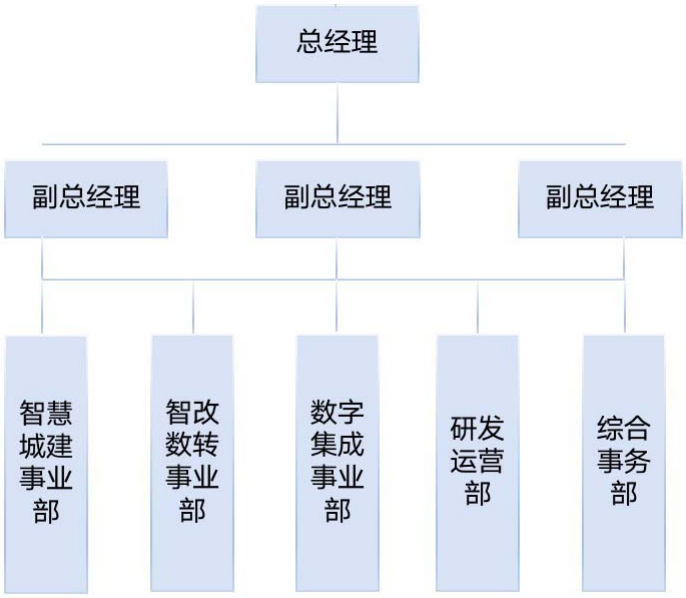
2） 基于 IT 管理评审报告，从满足业务和客户需求出发，进行 IT 服务管理调整、改进或升级；

3） 根据体系检查结果进行 IT 服务管理过程的优化和改进，包括过程策略的变更、过程接口的变更和角色职责的变更等，如修订 IT 服务管理策略、过程、程序和计划等；

4） 通过 IT 服务管理委员会会议、定期用户满意度调查和定期客户回访等取得服务相关信息，并对于未能满足服务要求的服务进行改善，并记入《服务改善计划》中。

附录 A　组织架构图

泰州城发数字科技有限公司
组织架构图



附录B　ITSM职能分配表

标准条款		管理层/管理者代表	智慧城建、系统集成事业部	综合事务部	智改数转事业部	研发运营部
4	公司环境	★	☆	☆	☆	☆
4.1	理解公司及其环境	★	☆	☆	☆	☆
4.2	理解利益相关方的需求和期望	★	☆	☆	☆	☆
4.3	确定服务管理体系的范围	★	☆	☆	☆	☆
4.4	服务管理体系及其过程	★	☆	☆	☆	☆
5	领导作用	★	☆	☆	☆	☆
5.1	领导和承诺	★	☆	☆	☆	☆
5.2	方针	★	☆	☆	☆	☆
5.3	公司的角色、职责和权限	★	☆	★	☆	☆
6	策划	★	☆	☆	☆	☆
6.1	风险和机遇的应对措施	★	☆	☆	☆	☆
6.2	服务管理目标及其实现的策划	★	☆	☆	☆	☆
6.3	策划服务管理体系	★	☆	☆	☆	☆
7	支持	☆	☆	★	☆	☆
7.1	资源	☆	☆	★	☆	☆
7.2	能力	☆	☆	★	☆	☆
7.3	意识	☆	☆	★	☆	☆
7.4	沟通	☆	☆	★	☆	☆
7.5	形成文件的信息	☆	☆	★	☆	☆
7.6	知识	☆	☆	★	☆	☆
8	运行	☆	★	☆	☆	☆
8.1	运行策划和控制	☆	★	☆	☆	☆
8.2	服务组合	☆	★	☆	☆	☆
8.2.1	服务交付	☆	★	☆	☆	☆

标准条款		管理层/管理者代表	智慧城建、系统集成事业部	综合事务部	智改数转事业部	研发运营部
8.2.2	策划服务	☆	★	☆	☆	☆
8.2.3	控制服务生命周期的相关方	☆	☆	☆	☆	☆
8.2.4	服务目录管理	☆	★	☆	☆	☆
8.2.5	资产管理	☆	★	☆	☆	☆
8.2.6	配置管理	☆	★	☆	☆	☆
8.3	关系与协议	☆	☆	☆	★	☆
8.3	总则	☆	☆	☆	☆	☆
8.3	业务关系管理	☆	☆	☆	★	☆
8.3	服务级别管理	☆	★	☆	☆	☆
8.3	供应商管理	☆	☆	☆	☆	☆
8.4	供应与需求	☆	☆	☆	☆	☆
8.5	服务设计、构建和转接	☆	☆	☆	☆	★
8.6	解决与完成	☆	☆	☆	☆	☆
8.7	服务保障	☆	★	☆	☆	☆
9	绩效评价	★	☆	☆	☆	☆
9.1	监视、测量、分析和评价	☆	☆	☆	☆	☆
9.2	内部审核	★	☆	☆	☆	☆
9.3	管理评审	★	☆	☆	☆	☆
9.4	服务报告	☆	☆	☆	☆	☆
10	改进	★	☆	☆	☆	☆
10.1	总则	★	☆	☆	☆	☆
10.1	不符合及纠正措施	☆	★	★	☆	☆
10.2	持续改进	☆		★	☆	☆

注： “★”为主要职能， “☆”为配合职能

附录C　部门工作职责

各部门负责人

根据本规定要求，确定相关信息技术服务管理组织、机构人选，并推动本部门信息技术服务管理工作的开展落实。

各流程经理

依据本规定要求，切实履行相关职责，完成信息技术服务管理体系中各项流程工作的运转；负责完成本流程运行质量的具体日常管理工作并及时与质管处沟通；负责本流程的持续改进工作。

全体员工

理解并遵守本规定定义的内容，配合流程经理的工作，确保各自岗位职责范围内涉及的相关流程工作的开展。

1.公司管理事务部分

1.1综合事务部

向公司总经理报告。
负责公司日常行政事务，组织建立和监督执行公司各项行政制度，参与公司发展战略规划的制订。
负责公司的日常法律事务，组织法律合同年检、知识产权保护等工作，协调、处理法律咨询、法律纠纷。
负责拟制、发送、签收公司与上级单位和相关部门间的往来公文；协调、处理上级主管部门、各级政府部门的相关接口工作。
负责公司行政部设施环境、固定资产（包括租赁资产）的实物管理，负责公司日常性办公用品采购工作。
负责管理公司的公共车辆，保证公司公共车辆的状态良好和满足公司人员的用车需求。
协助公司各项产业和国际标准贯彻，并在行政制度方面予以配合。
负责公司的企业文化建设。
负责制定公司人事管理制度，研究、分析并提出改进工作意见和建议。负责人事考核、考查工作，建立人才库，规范人才培养。
负责编制年、季、月度用工平衡计划和工资计划。负责编制员工培训大纲、课程计划，组织员工培训工作。
拟制劳动人事统计工作制度，建立健全人事劳资统计核算标准，核定各岗位工资标准，定期编制劳资人事等有关的统计报表。
负责招聘、录用、辞退工作，组织拟制每一职位的工作标准及其所需资格、条件，组织签订员工劳动合同，依法对员工实施管理。
负责拟制员工劳动纪律管理制度，负责考勤、奖惩、差假、调动等管理工作。
配合公司经营目标，组织拟制人力资源发展及人员编制数额计划，确保人员编制的合理性和准确性。
负责员工各项福利与劳动保护管理工作，营造员工与公司之间的和谐关系。
负责组织和管理对公司现有供应商的评审和监督管理，拟制公司合格供应商名单，负责监督、评审、记录供应商对服务水平承诺的落实情况。
根据公司的发展规划，负责组织相关部门讨论、确定采购需求规划，拟定供应商发展、采购计划和预算评估报告。拟制并审核公司采购管理制度。
负责组织和管理公司供应商的开发工作，跟踪新技术、新产品和新方案，比较现有合格供应商、采购和运营的状况，根据公司相关部门的需求寻找新的供应商，持续对系统建设和运维工作更高的性能价格比提出改进目标。

1.2财务

1） 负责公司财务战略的制定、财务管理及内部控制工作，向公司总经理报告。

2) 建立科学、系统符合企业实际情况的财务核算体系和财务监控体系，向公司经营决策提供依据，协助总经理制定公司战略，组织公司财务战略规划的制订。
3) 制定公司资金运营计划，对公司生产经营活动所需要的资金筹措方式进行成本计算，监督资金管理报告和预、决算，提供最为经济的筹资方式。
4) 组织对重大项目和经营活动的财务风险评估、指导、跟踪和财务风险控制，审核公司重大资金流向和重大财务支出。
5) 根据法律法规、会计准则、公司政策以及上级主管部门的要求，组织制订公司财务管理制度，负责拟制、审核公司的总体性和阶段性的财务规划。
6) 负责监督、审计公司财务管理制度和财务计划的执行情况，审核财务报表，向总经理提交财务管理工作报告、财务分析和改进建议。
7) 负责管理公司资产，监督公司资产的运行效率，保证公司资产的安全和优化配置。
8) 参与公司重要事项的分析和决策，为企业的生产经营、业务发展及对外投资等事项提供财务方面的分析和决策依据。
9) 协调公司同银行、工商、税务等政府部门的关系，维护公司权益。
10) 向上级主管单位汇报公司经营状况、经营成果、财务收支及计划的具体情况，对公司经营状况和预算执行情况进行分析。
11) 负责部门人员及其他日常管理工作。

2 公司技术管理部分

2.1 智慧城建、系统集成事业部

1) 进行运维项目的技术支持、方案设计、产品选型及招投标工作；
2) 负责运维项目的实施，制订符合顾客需求和合同要求的运维服务体系，按照约定的服务范围和服务级别提供满足客户需要的服务；
3) 负责针对运维项目实施所需外包服务和备品件提出采购的需求计划；
4) 负责运维项目实施过程中质量记录的填写和整理工作；
5) 负责运维项目实施过程中的过程检验工作；
6) 负责运维过程中不合格品的控制；
7) 负责利用统计技术分析运维过程中的问题，并制订纠正和预防措施；
8) 负责运维项目的验收；
9) 协助综合事务部做内部培训工作；
10) 配合智改数转事业部做好文件资料的归档备案。

2.1 智慧城建、系统集成事业部总监

1) 全面负责项目开智慧城建、系统集成事业部工作，向负责技术的公司副总经理报告。

2) 经负责技术的公司副总经理特别授权，管理和监督IT服务管理的重点工作。

3) 在负责技术的公司副总经理缺席时，受其委托代行其职务。

4) 负责组织公司的IT服务管理需求分析和规划工作，审核公司所有IT服务管理的需求说明书，报批后监督执行，并审核相关评估报告和改进建议。

5) 审核相关IT服务管理的发展计划和相关服务设计，报批后监督执行，并并审核相关服务评估报告和改进建议。

6) 审核公司在IT服务、软件开发和运行维护方面的工作计划、过程文件，审核相关资源需求计划，持续提高公司技术服务的工作效率。

7) 审核运维和项目开智慧城建、系统集成事业部与客户、公司内部其他部门和供应商之间的服务目录、服务级别以及对客户的服务级别承诺文件。在ISO20000开始贯彻的初期，当公司尚不能与客户签署正式的服务级别协议时，公司中作为运维和项目开智慧城建、系统集成事业部的代表，与智改数转事业部签署经过批准后的服务级别协议。

8) 负责领导公司IT服务、软件开发和运行维护方面的事件管理、问题管理、可用性管理、IT服务持续性管理、信息安全管理方面的日常工作，保证符合对客户的服务级别承诺。

9) 负责审核规划IT系统运维有关分担服务级别协议所规定责任的部门和人员分工，审核相关的分工文件和服务级别承诺文件。

10) 负责领导公司IT服务、软件开发和运行维护方面的状况监督、运维管理，与相关部门沟通IT服务、运维技术的改进和落实，提高运维服务效率、改进运维服务质量。

11) 负责项目开智慧城建、系统集成事业部常事务管理。

2.2 智改数转事业部

智改数转事业部：智能化改造和数字化转型。为推进数字产业化、即在已有网络的基础上，通过科技创新把云加进来，使二者很好地融合，建设云网融合的新型信息基础设施，推动电信产业的发展；

2)负责

1) 负责所有IT服务产品的智改数转事业部的管理，向项目开智慧城建、系统集成事业部经理报告。

2) 负责前端的客户需求和客户关系管理，负责拟制智改数转事业部建设规划，对智改数转事业部进行有效的管理，提高客户满意度。

3) 负责直接响应用户服务请求，即对于用户发出的错误报告、服务请求、变更请求等事故进行记录和处理。

4) 负责接听客户咨询电话，按照公司的规定的内容向客户提供信息。

5) 在公司规定的范围内，在I T客户提出新的服务请求而需进行有关变更时,智改数转事业部负责联络有关方面，维修或替换有关的软硬件组件。

6) 在公司规定的范围内，智改数转事业部承担维护客户基本信息等日常运作管理中的特定任务。

7) 现场服务工作监督和回访结果的反馈，工程移交情况跟踪和客户意见的反馈工作。

8) 负责备品备件的管理及坏件返修工作。

9) 负责工程移交文档的初审和各类资料归档工作。

2.3 智慧城建、系统集成事业部

1) 负责IT服务技术实施与合同客户技术支持工作，向经理报告。
2) 负责完成技术组技术支持工作目标，完成项目开智慧城建、系统集成事业部达的各项技术任务指标。
3) 负责IT服务技术方案的制定或审核工作（包括负责项目现场工程师技术报告审核）。
4) 负责IT服务重点客户和服务项目小型机专项技术巡检和技术支持工作。
5) 负责现场工程师技术能力评价和成长目标的考核。
6) 按照项目开智慧城建、系统集成事业部训计划要求，组织技术培训及人员技术学习的指导。
7) 参与新产品系统的配置管理、能力管理、变更管理、发布管理、可用性管理和IT服务持续性管理的工作，保证其顺利运行。

文件编号：CFSZ-1001-1.0　　受控状态：受　控

泰州城发数字科技有限公司

信息安全管理手册

（依据 GB/T22080-2018 ISO/IEC 27001：2013）

编　　制：综合事业部

审　　核：史佳

批　　准：张俊

发布时间：2022/5/4　　实施时间：2022/5/4

变更履历：

No.	变更原因	变更内容	版本	日期	编写者	审批者

目　录

01 信息安全管理手册发布令

为提高泰州城发数字科技有限公司的信息安全管理水平，保障我公司业务活动的正常进行，防止由于信息系统的中断、数据的丢失、敏感信息的泄密所导致的公司和客户的损失，我公司于 2022 年 5 月开展贯彻 GB/T22080-2018 ISO/IEC27001：2013《信息技术-安全技术-信息安全管理体系要求》国际标准工作，建立、实施和持续改进文件化的信息安全管理体系，制定了泰州城发数字科技有限公司《信息安全管理手册》。

《信息安全管理手册》是企业的法规性文件，是指导企业建立并实施信息安全管理体系的纲领和行动准则，用于贯彻企业的信息安全管理方针、目标，实现信息安全管理体系有效运行、持续改进，体现企业对社会的承诺。

《信息安全管理手册》符合有关信息安全法律、法规要求及 GB/T22080-2018 ISO/IEC27001：2013《信息技术-安全技术-信息安全管理体系-要求》标准和企业实际情况，现正式批准发布，手册自 2022 年 5 月 4 日起实施。企业全体员工必须遵照执行。

全体员工必须严格按照《信息安全管理手册》的要求，自觉遵循信息安全管理方针，贯彻实施本手册的各项要求，努力实现公司信息安全管理方针和目标。

该体系覆盖范围为领导层、研发运营部、综合事业部、智慧城建/数字集成事业部。

总经理：张俊

批准日期：2022 年 5 月 4 日

02 管理者代表任命书

为贯彻执行信息安全管理体系，满足 GB/T22080-2018 ISO/IEC27001：2013《信息技术-安全技术-信息安全管理体系-要求》标准的要求，加强领导，特任命 **史佳** 为我公司信息安全管理者代表。

授权信息安全管理者代表有如下职责和权限：

1. 确保按照标准的要求，进行资产识别和风险评估，全面建立、实施和保持信息安全管理体系；
2. 负责与信息安全管理体系有关的协调和联络工作；
3. 确保在整个组织内提高信息安全风险的意识；
4. 审核风险评估报告、风险处理计划；
5. 负责组织编写和批准发布程序文件，负责年度培训计划、支持性文件的审批。
6. 主持信息安全管理体系内部审核，任命审核组长，批准内审工作报告；
7. 向总经理报告信息安全管理体系的运行情况和所有改进要求，包括内外部审核情况。

本授权书自任命日起生效执行。

总经理：张俊

批准日期：2022 年 5 月 4 日

03 企业概况

强基赋能 打造高科技现代化国有企业

泰州城发数字科技有限公司

城发数科是在市委、市政府关心和支持下，由城投集团控股与省电信合资于 3 月 28 日挂牌成立的数字新基建公司，公司以“做泰州数字化转型主力军”为使命，以建设高科技现代化国有企业为目标，聚焦“新城建、新引擎、新能力”，致力于提升沉淀本地数字化自主研发、自主运营能力，助力数字政府、数字经济、数字民生、数字服务建设与运营，推动本土数字产业做大做强。

新城建方面：聚焦城市信息模型 CIM、建筑信息模型 BIM、智能市政基础设施、城市安全平台、城市综合管理、智慧社区、智能建造等领域，助力构建提升城市品质和人居环境质量、提升城市管理水平的信息数字化城市基础设施体系。

新引擎方面：致力工业智改数转，深入行业研究、建设生态体系，为企业智改数转提供诊断评估、规划设计、解决方案等服务，助力泰州及周边地市企业的数字化转型、产业提档升级。

新能力方面：集聚软件研发、数据治理、安全运营等高层次人才，不断探索创新应用，沉淀本地软件研发、平台运营、数据运营、信息安全服务等能力，推动泰州本土数字产业做大做强，加强自有产品和能力输出，打造区域数字科创基地。

04 信息安全管理方针及目标

为防止由于信息系统的中断、数据的丢失、敏感信息的泄密所导致的企业和客户的损失，本公司建立了信息安全管理体系，制订了信息安全方针，确定了信息安全目标。

信息安全管理方针：建立安全理念，建设安全文化，坚持以人为本，把握数据安全

本公司信息安全管理方针包括内容如下：

一、信息安全管理机制

公司采用系统的方法，按照 GB/T22080-2018 ISO/IEC27001：2013 建立信息安全管理体系，全面保护本公司的信息安全。

二、信息安全管理组织

1．公司总经理对信息安全工作全面负责，负责批准信息安全方针，确定信息安全要求，提供信息安全资源。

2．公司总经理任命管理者代表负责建立、实施、检查、改进信息安全管理体系，保证信息安全管理体系的持续适宜性和有效性。

3．在公司内部建立信息安全组织机构，信息安全管理委员会，保证信息安全管理体系的有效运行。

4．与上级部门、地方政府、相关专业部门建立定期经常性的联系，了解安全要求和发展动态，获得对信息安全管理的支持。

三、人员安全

1．信息安全需要全体员工的参与和支持，全体员工都有保护信息安全的职责，在劳动合同、岗位职责中应包含对信息安全的要求。特殊岗位的人员应规定特别的安全责任。对岗位调动或离职人员，应及时调整安全职责和权限。

2．对本公司的相关方，要明确安全要求和安全职责。

3．定期对全体员工进行信息安全相关教育，包括：技能、职责和意识。以提高安全意识。

4．全体员工及相关方人员必须履行安全职责，执行安全方针、程序和安全措施。

四、识别法律、法规、合同中的安全

及时识别顾客、合作方、相关方、法律法规对信息安全的要求，采取措施，保证满足安全要求。

五、风险评估

1．根据本公司业务信息安全的特点、法律法规要求，建立风险评估程序，确定风险接受准则。

2．采用先进的风险评估技术，定期进行风险评估，以识别本公司风险的变化。本公司或环境发生重大变化时，随时评估。

3．应根据风险评估的结果，采取相应措施，降低风险。

六、报告安全事件

1．公司建立报告信息安全事件的渠道和相应的主管部门。

2．全体员工有报告信息安全隐患、威胁、薄弱点、事故的责任，一旦发现信息安全事件，应立即按照规定的途径进行报告。

3．接受信息安全事件报告的主管部门应记录所有报告，及时做出相应的处理，并向报告人员反馈处理结果。

七、监督检查

定期对信息安全进行监督检查，包括：日常检查、专项检查、技术性检查、内部审核等。

八、业务持续性

1．公司根据风险评估的结果，建立业务持续性计划，抵消信息系统的中断造成的影响，防止关键业务过程受严重的信息系统故障或者灾难的影响，并确保能够及时恢复。

2．定期对业务持续性计划进行测试和更新。

九、违反信息安全要求的惩罚

对违反信息安全方针、职责、程序和措施的人员，按规定进行处理。

信息安全目标如下：

1. 客户信息安全事故为零。

2. 公司的重大信息安全事故为零。

总经理：张俊

批准日期：2022 年 5 月 4 日

05 关于成立 ISMS 工作小组的决定

为确保本公司信息安全管理体系的有效运行，认真贯彻信息安全管理方针，特授权以下人员组成 ISMS 工作小组。

序号	姓名	部门	角色
01	史佳	综合事务部	组长（管理者代表）
02	王存雨	智慧城建事业部	组员
03	张宇	智改数转事业部	组员
04	周甫	数字集成事业部	组员
05	邓恺	研发运营部	组员

总经理：张俊

批准日期：2022 年 5 月 4 日

1.机构职责

1.1 职责权限

1.1.1 总经理

(1) 向公司宣传达成信息安全目标和遵守信息安全方针的重要性，并满足法律和持续改进的要求。
(2) 组织制定并批准信息安全管理方针、信息安全目标和计划。
(3) 为发展、贯彻、运行和保持 CFSZ 提供充足的资源；为员工提供所需的资源、培训，并赋予其职责范围内的自主权。
(4) 负责任命信息安全管理者代表、工作小组组长，并定期进行管理评审。
(5) 决定风险的可接受水平。
(6) 负责批准公司信息安全管理手册和管理评审计划。
(7) 对公司的信息安全负总责，并对相关工作进行控制。

1.1.2 管理者代表

(1) 协助总经理确保信息安全管理体系得到建立、实施和保持。代表公司就管理体系有关事宜与内外部进行联络、组织、协调工作。
(2) 组织和协调 CFSZ 工作小组各项工作，贯彻国家的有关法律法规、标准和其他要求，负责管理体系建设工作，确保按标准要求建立、实施、保持和持续改进管理体系。
(3) 负责程序文件和支持性文件的审批。
(4) 定期向公司管理层报告管理体系运行业绩，包括改进需求。
(5) 在公司内促进全体员工在工作中形成以顾客为关注焦点、保持信息安全的理念和意识的形成。

1.1.3 综合事业部

(1) 负责文件控制、记录控制。
(2) 负责本公司保密工作的管理。

(3) 安全区域的保卫管理部门，负责安全区域的管理。
(4) 负责全公司人员安全管理，包括人员聘用管理，保密协议签署，员工的能力、意识和培训，员工离职管理。
(5) 对信息安全日常工作实施动态考核，将信息安全管理作为企业管理的重要工作内容。
(6) 参与涉密及司法介入的信息安全事件的调查。
(7) 做好各种财务预算计划，并认真监督执行，按期作出财务决算报告；
(8) 做好记帐、结帐、报帐工作，正确核算各项费用开支、成本核算和财务损益等工作。
(9) 负责公司的员工社保等相关缴费工作。
(10) 执行公司计算机、网络、口令、信息安全秘密等管理，执行有关制度
(11) 参与公司信息协调沟通、信息安全内部审核和管理评审
(12) 参与有关的信息安全持续改进

1.2.4 智慧城建/数字集成事业部

(1) 我公司信息安全管理体系的归口管理部门。
(2) 负责公司的软件产品开发、售后服务。
(3) 负责局域网上所承担的各类信息系统的管理职能；
(4) 负责涉密信息上网、涉密计算机运行、检修、报废的监督管理。
(5) 负责我公司信息系统安全日常管理。
(6) 认真执行信息安全管理的方针、标准、安全策略和规范。
(7) 负责内部审核的组织、管理评审的组织和体系的改进

1.2.5 研发运营部

(1) 负责智能卡、智能卡发卡设备的市场拓展，参与投标活动。
(2) 负责软件产品的销售。
(3) 参与公司资产识别与风险评估
(4) 执行公司计算机、网络、口令、信息安全秘密等管理，执行有关制度
(5) 参与公司信息协调沟通、信息安全内部审核和管理评审
(6) 参与有关的信息安全持续改进

2. 引用标准

ISO/IEC 27000：2013 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T22080-2018 ISO/IEC 27001：2013 信息技术 安全技术 信息安全管理体系 要求

ISO/IEC 27002：2013 信息技术-安全技术-信息安全管理实用规则

3. 术语和定义

可用性：保证被授权的使用者需要时能够访问信息及相关资产。

保密性：保证信息只被授权的人访问。

信息安全：保持信息的保密性、完整性和可用性。

信息安全管理体系（CFSZ）：是整个管理体系的一部分，建立在业务风险的方法上，以开发、实施、完成、评审和维护信息安全。

[注意：管理体系包括组织的结构、方针、计划、活动、责任、实践、程序、过程和资源]

完整性：保护信息和处理过程的准确和完整。

风险接受：接受一个风险的决定。

风险分析：系统化地使用信息识别来源和估计风险。

风险评估：风险分析和风险评价的整个过程。

风险评价：比较估计风险与给出的风险标准，确定风险严重性的过程。

风险管理：指导和控制组织风险的联合行动。

风险处理：选择和实施措施以更改风险的处理过程。[ISO Guide 73]

适用性声明：描述适用于组织的 CFSZ 范围的控制目标和控制措施。这些控制目标和控制措施是建立在风险评估和处理过程的结论和结果基础上。

4. 组织环境

4.1 了解组织和它的背景

本公司应确定与 CFSZ 相关的目的和影响其达到预期效果的能力的内外部问题。依据 GB/T22080-2018 ISO/IEC 27001：2013《信息技术 安全技术 信息安全管理体系 要求》的要求，结合本公司的业务活动和风险的实际情况建立、保持并持续改进信息安全管理体系。

GB/T22080-2018 ISO/IEC 27001：2013 信息安全管理体系标准建立在国际上通用的 PDCA 管理理论模式上，即计划、实施、检查、改进的基础上。

4.2 理解相关方的需求和期望

本公司应确定：

a) CFSZ 的相关方；

b) 和这些相关方有关信息安全的要求。

4.3 确定 CFSZ 的范围

根据本公司的业务性质、地理位置、信息资产和技术的特点，本公司的信息安全管理体系的管理范围：

1、泰州城发数字科技有限公司所涉及的软件外包、定制软件开发、服务和日常管理的重要信息系统和生产系统等软件开发；

2、与所述信息系统有关的活动；

3、与所述信息系统有关的部门和所有正式员工；

4、所述活动、系统及支持性系统包含的全部信息资产；

4.4 CFSZ 的建立

组织应按照本国际标准的要求建立、实施、保持和持续改进CFSZ。

a. 方针的制订

CFSZ 方针是本公司信息安全管理的纲领，提供了本公司信息安全的管理方向，确定了信息安全管理目标的框架，体现了公司信息安全方面的长期战略。

CFSZ 方针体现和包括了以下内容：阐述了有关信息安全行为的总体指导思想和原则，提供了制订信息安全管理目标的框架；考虑了业务及法律或法规的要求，以及合同的安全义务；体现了本公司建立和保持 CFSZ 作为公司的发展战略和风险管理手段的信息安全管理的长期战略要求；确立了风险评价的标准和风险评估的方法；体现公司管理层加强及支持信息安全管理的意图和承诺。

信息安全方针应由公司管理层审批后，以适当的方式传达给员工。

b. 制定系统化的风险评价方法

CFSZ 工作小组制订《风险评估程序》，并组织各相关部门实施。该程序确立了适用于 CFSZ，并满足信息安全法律法规要求的风险评估方法。通过建立和保持该程序，将有助于公司管理层为 CFSZ 建立安全策略和目标，识别并确定可接受风险的水平和标准。

c. 识别风险

CFSZ 工作小组按照《风险评估程序》从以下几个方面，对风险进行识别：

识别 CFSZ 范围内所有的信息资产及其负责人，并对资产的保密性、完整性和可用性价值进行评估；

识别各信息资产所可能面对的威胁；

识别各威胁可能利用的脆弱性；

确认以上信息资产的保密性、完整性和可用性受损后所产生的影响和潜在后果。

d. 评估风险

CFSZ 工作小组按照《风险评估程序》，评价安全问题所可能导致的业务危害，考虑该危害的严重程度时，必须考虑到信息资产的保密性、完整性和可用性受损后所产生的现实后果和长远影响。

根据与这些信息资产有关的主要威胁和脆弱性，以及当前采取的控制措施，评价安全问题出现的可能性。

根据《风险评估程序》，计算风险系数。

根据风险评价的结果，决定风险是否接受或应采取的处理措施。

e. 确定和评价提供处理风险的可选措施

CFSZ 工作小组根据风险评价的结果，确定可接受风险的水平，决定风险处理措施，包括以下内容：

使用合适的控制措施接受风险，但应保证该风险在可接受水平，并应保证符合公司的信息安全方针避免风险、转移风险。

f. 选择处理风险的控制目标和控制措施

CFSZ 工作小组负责从 GB/T22080-2018 ISO/IEC 27001：2013 附录 A 中选择适当的控制目标和控制措施，如有必要可在 GB/T22080-2018 ISO/IEC 27001：2013 附录 A 范围之外增加额外的控制目标和控制措施，但应对这些额外的控制目标和控制措施予以记录。

g. 残余风险的确认

CFSZ 工作小组应对采取控制措施后的残余风险予以预测，由公司管理层批准残余风险（见《风险评估报告》）。

h. 由公司管理层授权实施和运作 CFSZ（见：手册“发布令”页）。

i. 适用性声明(版本号：1.0)

CFSZ 工作小组负责拟定“适用性声明(版本号：1.0)”。

“适用性声明”应对未采用的 GB/T22080-2018 ISO/IEC 27001：2013 附录 A 中的条款的原因予以说明，同时对采用的 GB/T22080-2018 ISO/IEC 27001：2018 附录 A 以外的所有控制措施予以说明。

具体参见《适用性声明》(版本号：1.0)

5. 领导力

5.1 领导力和承诺

公司管理层应展示关于 CFSZ 的领导力和承诺：

a) 确保信息安全方针和信息安全目标被建立，并与组织战略方向兼容;

b) 确保信息安全管理体系的要求集成到组织的过程中;

c) 确保信息安全管理体系所需要的资源是可用的;

d) 传达有效的信息安全管理和符合信息安全管理体系要求的重要性;

e) 确保信息安全管理体系达到其预期的效果;

f) 指导和支持员工，有助于信息安全管理体系的效率;

g) 推进持续改进;

h) 支持其他相关管理角色展示他们的领导力，同样适用于他们的职责范围。

5.2 方针

公司管理层应建立信息安全方针：

a) 适合组织的宗旨;

b) 包括信息安全目标（见 6.2），或为建立信息安全目标提供框架;

c) 包括满足有关信息安全适当要求的承诺;

d) 包括 CFSZ 持续改进的承诺。

信息安全方针应：

e) 是以文档化的身份可用的;

f) 在组织内传达;

g) 适当时，对相关方是可用的。

5.3 组织的角色、职责和权限

公司管理层应确保与信息安全相关角色的职责和权限被分配和传达。公司管理层应分配职责和权限：

a）确保 CFSZ 符合本国际标准的要求;

b）将 CFSZ 绩效报告给公司管理层。注：公司管理层也可以分配组织内 CFSZ 绩效报告的职责和权限。

设立 CFSZ 工作小组为专门的机构，并任命其人员，使其负责 CFSZ 的建立、实施、保持和改进，明确所有相关人员在体系中的职责和义务（参见公司相关任命文件），确保体系运行的有效性。

6. 策划

6.1 处理风险和机遇的行动

6.1.1 总则

当规划 CFSZ 时，本公司应当考虑 4.1 提到的问题和 4.2 中所提到的要求，并确定需要处理的风险和机遇：

a）确保 CFSZ 实现预期的效果；

b）防止或减少不良影响；

c）实现持续改进；

d）处理这些风险和机遇的行动；

e）如何

1）集成和实施这些行动到 CFSZ 过程中；

2）评估这些行动的有效性。

6.1.2 信息安全风险评估

1）识别风险

CFSZ 工作小组按照《风险评估程序》从以下几个方面，对风险进行识别：

识别 CFSZ 范围内所有的信息资产及其负责人，并对资产的保密性、完整性和可用性价值进行评估；

识别各信息资产所可能面对的威胁；

识别各威胁可能利用的脆弱性；

确认以上信息资产的保密性、完整性和可用性受损后所产生的影响和潜在后果。

2）评估风险

CFSZ 工作小组按照《风险评估程序》，评价安全问题所可能导致的业务危害，考虑该危害的严重程度时，必须考虑到信息资产的保密性、完整性和可用性受损后所产生的现实后果和长远影响。

根据与这些信息资产有关的主要威胁和脆弱性，以及当前采取的控制措施，评价安全问题出现的可能性。

根据《风险评估程序》，计算风险系数。

根据风险评价的结果，决定风险是否接受或应采取的处理措施。

6.1.3 信息安全风险处置

1）确定和评价提供处理风险的可选措施

CFSZ 工作小组根据风险评价的结果，确定可接受风险的水平，决定风险处理措施，包括以下内容：

使用合适的控制措施接受风险，但应保证该风险在可接受水平，并应保证符合公司的信息安全方针避免风险、转移风险。

2）选择处理风险的控制目标和控制措施

CFSZ 工作小组负责从 GB/T22080-2018 ISO/IEC 27001：2013 附录 A 中选择适当的控制目标和控制措施，如有必要可在 GB/T22080-2018 ISO/IEC 27001：2013 附录 A 范围之外增加额外的控制目标和控制措施，但应对这些额外的控制目标和控制措施予以记录。

3）残余风险的确认

CFSZ 工作小组应对采取控制措施后的残余风险予以预测，由公司管理层批准残余风险（见《风险评估报告》）。

4） 由公司管理层授权实施和运作 CFSZ（见：手册“发布令”页）。

5） 适用性声明(版本号：1.0)

CFSZ 工作小组负责拟定“适用性声明(版本号：1.0)”。

“适用性声明”应对未采用的 GB/T22080-2018 ISO/IEC 27001：2013 附录 A 中的条款的原因予以说明，同时对采用的 GB/T22080-2018 ISO/IEC 27001：2013 附录 A 以外的所有控制措施予以说明。

具体参见《适用性声明》(版本号：1.0)

6.2 可实现的信息安全目标和计划

a. CFSZ 工作小组根据《适用性声明》(版本号：1.0)和《风险评估报告》所列控制措施，制定《风险处理计划》。《风险处理计划》应对所选控制措施的实施制定具体的工作方案和时间表。

b. 该方案还应考虑到资金的保证，并规定具体的负责部门和负责人。

c. CFSZ 工作小组应组织完成《风险处理计划》，实施《适用性声明》和《风险评估报告》中所选择的控制措施，以达到保护信息安全、降低信息安全风险的目标。

d. 规定如何度量所选控制措施的有效性，并指明这些度量方法如何用于评估控制措施的有效性，产生可比且可再现的结果。

7. 支持

7.1 资源

为确保 CFSZ 的有效运行，公司管理层应提供充足必要的资源，该资源包括资金、技术、人力等方面，以保证：

a. 建立、贯彻、运行和保持 CFSZ

b. 确保信息安全程序支持业务要求

c. 识别和强调法律和法规的要求和合同的安全义务

d. 正确地应用所有实施的控制措施以保持充分的安全

e. 必要时进行评审，并对评审结果做出适当的响应

f. 需要时，改善 CFSZ 的有效性

7.2 能力

为有效地实施信息安全管理，贯彻信息安全管理方针，实现信息安全目标，必须对 CFSZ 涉及的所有人员进行培训，以增强其信息安全意识，保证其胜任所在岗位的工作。

按公司 CFSZ 中的《各级员工任职要求》，行政人事签定相关协议，并根据 QMS 体系文件的 6.2 条款及《人力资源控制程序》中的规定对人员进行适当的培训。以上文件对以下方面做出了规定：

a. 确定人员有效地完成 CFSZ 工作所必需的能力

b. 提供能力培训，必要时，可聘用有能力的人员以满足需求

c. 评估培训和所采取行动的效果

保持员工的教育、培训、技能、经验和资格记录（4.3.3 款）

7.3 意识

本公司控制措施下工作的人员应意识到：

a) 信息安全方针;

b) 他们对 CFSZ 有效性的贡献，包括提高信息安全绩效的收益;

c) 不符合 CFSZ 要求所带来的影响。

7.4 沟通

本公司应确定有关 CFSZ 内部和外部沟通的需求：

a) 沟通什么;

b) 何时沟通;

c) 和谁沟通;

d) 谁应该沟通;

e) 怎样的沟通过程是有效的。

7.5 文档化的信息

7.5.1 总则

由 CFSZ 工作小组负责建立 CFSZ 文件体系，确保其适合本公司的规模、活动类型、安全要求的范围和复杂性，对文件的载体本手册不做具体要求，但其内容至少包括以下方面：

a. 文件化的安全方针（具体要求见 4.2.1b）和控制目标

b. CFSZ 的范围(具体内容见 4.2.1a)

c. 支持 CFSZ 的程序和控制措施

d. 风险评估方法的描述(见 4.2.1c)

e. 风险评估报告(具体要求见 4.2.1)

f. 风险处理计划（具体要求见 4.2.2）

g. 为确保信息安全管理进程中的计划、运行和控制的有效性而必需的文件化程序（见本手册的《制度文件清单》）

h. CFSZ 程序所要求的记录

i. 适用性声明（见《适用性声明》）

7.5.2 文件控制

CFSZ 的文件均应受控，按《文件控制程序》的要求执行，该程序应满足以下要求：

a. 文件发布前应审批其适用性

b. 必要时评审并更新文件，并重新审批

c. 确保标识文件的版本和修改内容

d. 确保在使用地点可得到文件的最新版本

e. 确保文件保持字迹清楚，标识明确

f. 确保文件对需要者现时可用，并根据与其密级相适合的程序要求进行转移、存放及最后的处置

g. 确保外部文件得到识别

h. 确保文件的发放受控

i. 防止无意中使用作废文件

j. 如因某些目的需保留上述作废文件，应予以适当的标识公司制订的 CFSZ 体系文件均有唯一性标识。

为了便于公司管理体系运作实施的简便有效，对公司 QMS、EMS 与 CFSZ 中基本相同过程/要素所规定的文件/记录表格均使用 QMS 中给定的标识，而对 CFSZ 特有的文件/记录表格标识采用如下规定：

a. “信息安全管理手册”

b. “程序文件”

c. “作业文件”

d. “记录文件”

7.5.3 记录控制

CFSZ 的记录均应受控，按《记录控制程序》的要求执行，以确保可在适当的时机，提供 CFSZ 要求和运行效果的符合性证据。该程序应对记录的标识、保存、保护、获取、保留时间和处置要求做出明确的规定。

8. 运行

CFSZ 工作小组还应组织全体员工的培训，以提高全体员工的信息安全意识，具体参见本手册 5.2.2 款。

CFSZ 工作小组负责针对公司所选择的控制目标和控制手段编写运行程序（如：《业务连续性与事故报告及响应程序》等）。程序中应规定控制对象、参数或控制要求及监督检查的内容，并符合相关法律法规的要求。

公司管理层应为 CFSZ 的有效运行提供必要的人力、物力和财力资源，具体参见本手册 5.2 款。

CFSZ 工作小组负责制定《业务连续性与事故报告及响应程序》，确保员工可及时地将发现的安全事故、安全故障或安全薄弱点报告给相关负责人，并迅速对其做出响应。

8.1运行计划及控制

本公司应策划、实施和控制用来满足信息安全要求过程，并实施在 6.1 中确定的行动。组织还应当实施计划，以实现在 6.2 中确定的信息安全目标。

本公司应保存相关的文档化信息，以保证过程已按照计划完成。 组织应控制计划内的变更并评审非计划变更的结果，必要时，采取措施以减轻任何不良影响。

本公司对部分集成项目施工采取外包，且确保外包过程被确定和受控。

8.2信息安全风险评估

本公司应按计划的时间间隔或重大变更被提出或发生时执行信息安全风险评估，考虑 6.1.2a）中建立的准则。 组织应保留信息安全风险评估结果的相关文档化信息。

8.3信息安全风险处置

本公司应实施信息安全风险处置计划。 组织应保留信息安全风险处置结果的文档化信息。

9. 绩效评价

9.1监视、测量、分析和评价

a. CFSZ 工作小组应按 CFSZ 体系文件的有关规定对 CFSZ 的运行情况进行适宜的监控和评审,并及时对所发现的不符合进行整改,以便迅速从处理结果中发现错误及时识别安全破坏事故,不论其是否成功;使公司管理层确定员工的信息安全活动或通过信息技术实施的信息安全活动是否达到了所期望的目标;利用指标来帮助发现安全事件,从而防止安全事故的发生;确定为解决破坏安全问题所采取的措施是否有效。

b. CFSZ 工作小组应定期评审 CFSZ 的有效性,评审内容包括安全政策、安全目标和安全控制,同时还应考虑到安全审核的结果、安全事故及所有利益相关方的建议和反馈。

c. 测量控制措施的有效性,验证已满足安全需求。

d. 在评审残余风险和可接受风险的水平时,应考虑以下方面的变化:

组织

技术

业务目标和过程

已识别的威胁

所实施控制措施的有效性

外部事件:如法律法规的变化或社会环境的变化

e. CFSZ 工作小组应按计划定期进行 CFSZ 内审,具体参见《内部审核控制程序》。

f. 公司应每年进行 CFSZ 管理评审,以确保 CFSZ 的范围保持充分,CFSZ 的改进得到确认。具体参见《管理评审控制程序》。

g. 根据监视和评审活动的发现,更新安全计划。

应记录可能影响 CFSZ 有效性的行为和事件。

9.2内部审核

按《内部审核控制程序》执行。以确保 CFSZ 的控制目标、控制手段、过程和程序：

a. 符合 GB/T22080-2018 ISO/IEC27001：2013 标准和相关法律法规的要求；

b. 符合识别的信息安全要求；

c. 被有效地实施和维护；

d. 达到预想的业绩。

在制定内审程序时应考虑被审核区域和过程的状态和重要性，包括前次审核的结果。应确定审核准则、范围、频次和方法。选择有资质的审核员，确保审核过程客观公正。审核员不应审核自己的工作。

被审核区域的管理者负责保证及时采取措施以消除被发现的不符合及其原因。改进行为应包括对措施实施和效果的验证。

9.3管理评审

公司管理层应按《管理评审控制程序》的要求定期举行公司管理体系的管理评审，以确保 CFSZ 的持续适宜性、充分性和有效性。该评审包括对安全方针和安全目标的评审，并将评审结果以文件的形式记录下来。

管理评审的输入

a. CFSZ 审核和评审的结果

b. 相关方的反馈

c. 用于改善 CFSZ 绩效和有效性而在公司中使用的技术、产品和程序

d. 预防和纠正措施的状况

e. 初始风险评价中未列出的脆弱性和威胁

f. 有效性度量的结果

g. 前次管理评审后的跟踪措施

h. 影响 CFSZ 的任何改变

i. 改进的建议

管理评审的输出

a. 改善 CFSZ 的有效性

b. 更新风险评估和风险处理计划

当发生以下导致影响 CFSZ 的内外部事件时，应对信息安全有关的程序做必要的更改；

商务要求

安全要求

影响外部商务要求的商务过程

法律法规环境

合同责任

风险水平和（或）风险接受水平

c. 资源需求

d. 对测量控制措施有效性的改进

10. 改进

10.1 不符合及纠正措施

按《纠正和预防控制程序》执行，针对 CFSZ 实施和运行中出现的不符合原因采取纠正措施，以防止其再次发生。程序内容应包括：

a. 识别 CFSZ 实施和运行中的不符合

b. 确认不符合的原因

c. 评估所需措施，应确保不符合不再发生

d. 确定并实施所需的纠正措施

e. 记录措施实施的结果

f. 评审已实施的纠正措施

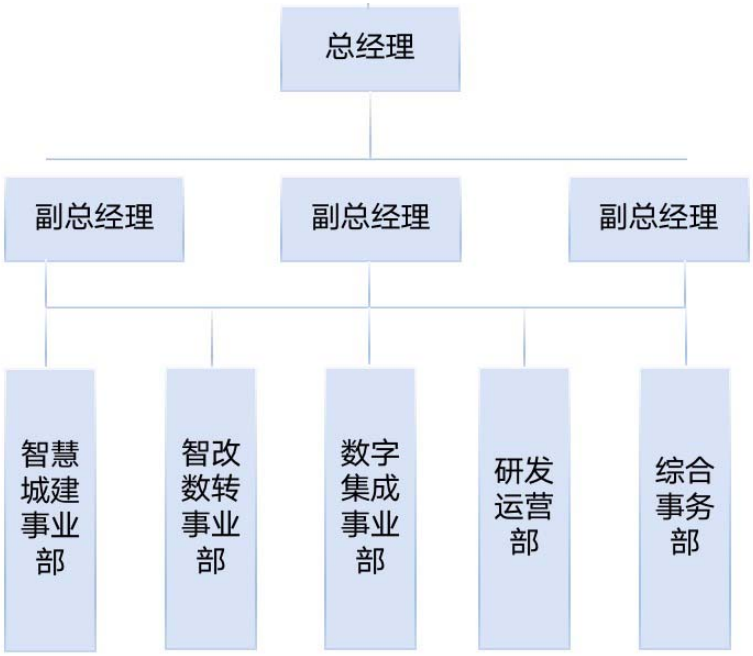
10.2 持续改进

公司应通过运用信息安全管理方针、安全目标、审核结果、对监控事件的分析、纠正和预防措施和管理评审的信息，持续改进 CFSZ 的有效性。

附录

附录 1、组织结构图

. 泰州城发数字科技有限公司组织机构图



附录 2 管理体系职责分配表

管理职责 \ 部门		领导层	综合事业部	研发运营部	智慧城建/数字集成事业部
4 组织背景	4.1 了解组织和它的背景	★	○	○	○
	4.2 理解相关方的需求和期望	★	★	○	○
	4.3 确定 CFSZ 的范围	★	★	○	○
	4.4 CFSZ	★	★	○	○
5 领导力	5.1 领导力和承诺	★	○	○	○
	5.2 方针	★	○	○	○
	5.3 组织的角色、职责和权限	★	★	○	○
6 计划	6.1 处理风险和机遇的行动	○	○	○	★
	6.2 可实现的信息安全目标和计划	○	○	○	★
7 支持	7.1 资源	★	○	○	○
	7.2 能力	○	★	○	○
	7.3 意识	○	★	○	○
	7.4 沟通	★	★	○	○
	7.5 文档化的信息	★	★	○	○
8 运行	8.1 运行计划及控制	★	★	○	○
	8.2 信息安全风险评估	★	★	○	○
	8.3 信息安全风险处置	★	★	○	○
9 绩效评价	9.1 监视、测量、分析和评价	★	★	○	○
	9.2 内部审核	★	★	○	○

管理职责 \ 部门		领导层	综合事业部	研发运营部	智慧城建/数字集成事业部
	9.3 管理评审	★	★	○	○
10 改进	10.1 不符合及纠正措施	★	★	○	○
	10.2 持续改进	★	★	○	○
控制目标与控制要求		★	★	★	★
A.5.1 信息安全方针		★	○	○	○
A.6.1 内部组织		★	★	★	★
A.6.2 移动设备和远程办公		★	★	○	★
A.7.1 任用前		○	★	○	○
A.7.2 任用中		○	★	○	○
A.7.3 任用终止和变更		○	★	○	○
A.8.1 资产的责任		○	★	○	○
A.8.2 信息分类		○	★	○	○
A.8.3 介质处理		○	★	○	○
A.9.1 访问控制的业务需求		○	○	○	★
A.9.2 用户访问管理		○	★	○	○
A.9.3 用户责任		○	★	○	○
A.9.4 系统和应用访问控制		○	○	○	★
A.10.1 密码控制		○	○	○	★
A.11.1 安全区域		○	★	○	○
A.11.2 设备安全		○	○	○	★
A.12.1 操作程序及职责		○	○	○	★

部门 / 管理职责	领导层	综合事业部	研发运营部	智慧城建/数字集成事业部
A.12.2 防范恶意软件	○	★	★	★
A.12.3 备份	—	★	—	★
A.12.4 日志记录和监控	○	○	○	★
A.12.5 操作软件控制	○	○	★	○
A.12.6 技术漏洞管理	○	○	★	○
A.12.7 信息系统审计的考虑因素	○	○	○	★
A.13.1 网络安全管理	○	○	○	★
A.13.2 信息传输	○	○	○	★
A.14.1 信息系统安全需求	○	○	○	★
A.14.2 开发和支持过程的安全	○	○	★	○
A.14.3 测试数据	○	○	★	○
A.15.1 供应商关系的信息安全	○	○	★	○
A.15.2 供应商服务交付管理	○	○	○	★
A.16.1 信息安全事件的管理和改进	○	○	○	★
A.17.1 信息安全的连续性	○	○	○	★
A.17.2 冗余	○	○	○	★
A.18.1 法律和合同规定的符合性	○	★	○	○
A.18.2 信息安全评审	○	★	○	★

注：★为主控部门　　○为配合部门　　—为无关部门

文件编号：

CFSZ-1002-1.0

信息安全适用性声明

版本：V1.0

编　　制：综合事务部

审　　核：　史佳

批　　准：张俊

受控状态：受控

泰州城发数字科技有限公司　发布

发布日期：2022 年 5 月 4 日　　实施日期：2022 年 5 月 4 日

变 更 记 录

变更日期	版本	变更说明	编写	审核	批准

信息安全适用性声明

1 目的与范围

本声明描述了在 GB/T22080-2016 ISO/IEC27001:2013 附录 A 中，适用于本公司信息安全管理体系的目标/控制、是否选择这些目标/控制的理由、公司现行的控制方式、以及实施这些控制所涉及的相关文件。

2 相关文件

《信息安全管理手册》

3 职责

《信息安全适用性声明》由信息安全管理小组编制、修订，由管理者代表批准。

4 声明

本公司按 GB/T22080-2016 ISO/IEC27001:2013 建立信息安全管理体系。

根据公司风险评估的结果和风险可接受水平，GB/T22080-2016ISO/IEC27001:2013《信息安全管理体系》附录 A 的下列条款被选择（或不选择)用于本公司信息安全管理体系。公司目前没有外包软件开发相关的业务活动，故删除 A.14.2.7 条款

A.5 信息安全方针和策略

A.5 信息安全方针和策略	A.5.1 信息安全管理指导				
	A.5.1.1	信息安全方针和策略	是	信息安全方针文档应经过管理层的批准，并向所有员工和外部相关方公布和沟通	信息安全管理手册
	A.5.1.2	信息安全方针和策略的评审	是	按计划的时间间隔或当发生重大变化时，应对信息安全方针文档进行评审，以确保其持续的适宜性、充分性和有效性	信息安全管理手册 管理评审时评审方针

A.6 信息安全组织	A.6.1 内部组织				
	A.6.1.1	信息安全角色和职责	是	在组织内，管理者应通过清晰的方向、可见的承诺、明确的任务分配、信息安全职责沟通等方式积极支持安全工作	信息安全管理手册
	A.6.1.2	责任分割	是	应明确规定所有的信息安全职责	信息安全管理手册
	A.6.1.3	与政府部门的联系	是	应与相关政府机构保持适当联系	《相关方一览表》》《相关方信息安全管理程序》
	A.6.1.4	与特定相关方的联系	是	应保持与特殊利益团体或其他专业安全协会和行业协会的适当联系	《相关方一览表》《相关方信息安全管理程序》
	A.6.1.5	项目管理中的信息安全	是	本公司各项目组对项目中的信息安全目标、项目信息安全风险评估和处置、定期风险监控实施有效的安全管理。	《执行项目信息安全管理规定》
	A.6.2 移动设备和远程工作				
	A.6.2.1	移动设备策略	是	本公司建立实施《笔记本电脑管理规定》，对笔记本电脑的移动办公实施有效可行的安全管理。	《笔记本电脑管理规定》
	A.6.2.2	远程工作	是	本公司按照《数据安全管理程序》要求，对远程工作进行合适的保护，以防范设备和信息被窃、信息的未授权泄露、对组织内部系统的未授权远程访问或设施滥用。	《数据安全管理程序》《远程工作策略》

A.6 信息安全组织

A.7 人力资源安全

A.7 人力资源安全	A.7.1 任用前				
	A.7.1.1	审查	是	综合事务部对初始录用员工进行能力、信用考察，定期对关键信息安全岗位进行年度考察，对于不符合安全要求的不得录用或进行岗位调整。	《人力资源控制程序》
	A.7.1.2	任用条款及条件	是	在《劳动合同》中明确规定保密的义务及违约的责任。	《人力资源控制程序》
	A.7.2 任用中				
	A.7.2.1	管理职责	是	公司管理者要求员工、合作方以及第三方用户加强信息安全意识，依据建立的方针和程序来应用安全，服从公司管理，当有其他的管理制度与信息安全管理制度冲突时，首选信息安全管理制度执行。	《人力资源控制程序》
	A.7.2.2	信息安全意识、教育和培训	是	组织应对组织的所有员工，适当时，还包括合同方和第三方用户进行适当的意识培训、定期更新的、与他们工作相关的组织方针和程序培训	《人力资源控制程序》
	A.7.2.3	纪律处理过程	是	违背组织安全方针和程序的员工，公司将根据违反程度及造成的影响进行处罚，处罚在安全破坏经过证实的情况下进行。处罚的形式包括精神和物质两方面。	《信息安全奖惩规定》
	A.7.3 任用的终止和变更				
	A.7.3.1	任用职责的终止或变更	是	员工离职按照公司《人力资源控制程序》的要求，进行离职或变更活动的管理；第三方用户完成合同时，应进行明确终止责任的沟通。再次沟通保密协议和重申是否有竞业禁止要求等。	《人力资源控制程序》

A.8 资产管理

A.8 资产管理	A.8.1 资产职责				
	A.8.1.1	资产清单	是	信息安全管理小组按照《信息安全风险识别与评价管理程序》组织各部门按业务流程识别所有信息资产。根据重要信息资产判断准则确定公司的重要信息资产，在《信息资产风险评估表》中进行重要资产标识，并明确资产责任人。 当信息资产增添或报废时，信息安全管理小组组织资产使用部门对“重要信息资产”进行修订。	《信息安全风险识别与评价管理程序》
	A.8.1.2	资产责任主体	是	信息安全管理小组组织相关部门依据《信息安全风险识别与评价管理程序》中的要求和方法识别资产并指定资产负责人，记录在“信息资产风险评估表”中。	《信息安全风险识别与评价管理程序》
	A.8.1.3	资产的可接受使用	是	制定相应的业务系统应用管理制度，重要设备有使用说明书，规定了资产的合理使用规则。使用或访问组织资产的员工、合作方以及第三方用户应该了解与信息处理设施和资源相关的信息和资产方面的限制。并对信息资源的使用，以及发生在其责任下的使用负责。	《信息处理设施管理程序》
	A.8.1.4	资产归还	是	员工离职或工作变动前，应办理资产归还手续，然后方能办理移交手续。	《信息处理设施管理程序》
	A.8.2 信息分级				
	A.8.2.1	信息的分级	是	本公司的信息密级划分为：公开信息、内部信息、机密信息三级。不同密级事项的界定，由涉及秘密事项产生部门按照《商业秘密管理程序》规定的原则进行。	《商业秘密管理程序》

	A.8.2.2	信息的标记	是	对于属于机密信息的文件（无论任何媒体），密级确定部门按《商业秘密管理程序》里关于密级的要求进行适当的标注；公开信息不需要标注，其余均标注受控或机密。 信息的使用、传输、存储等处理活动按《用户访问管理程序》等进行控制。	《商业秘密管理程序》 《用户访问管理程序》
	A.8.2.3	资产的处理	是	信息的使用、传输、存储等处理活动按《用户访问管理程序》等进行控制。	《用户访问管理程序》 《信息处理设施管理程序》
	A.8.3 介质处理				
	A.8.3.1	移动介质的管理	是	可移动计算媒体包括光盘、磁带、磁盘、盒式磁带和已经印刷好的报告，各部门按其管理权限并根据风险评估的结果对其实施有效的控制。 媒体移动的记录予以保持。	《信息处理设施管理程序》
	A.8.3.2	介质的处置	是	对于含有敏感信息或重要信息的介质在不需要或再使用时，介质处置部门按照相关规定的要求，采取安全可靠处置的方法将其信息清除。	《信息处理设施管理程序》
	A.8.3.3	物理介质的转移	是	为避免被传送的介质在传送（运输）过程中发生丢失、未经授权的访问或毁坏，造成信息的泄露、不完整或不可用，负责介质（包括保密产品的运输）传送的部门采用以下方法进行控制： a）选择适宜的安全传送方式，对保密产品运输供方进行选择与评价，并与之签订保密协议； b）保持传送活动记录。	《信息处理设施管理程序》

A.9 访问控制

A.9 访问控制	A.9.1 访问控制的业务要求				
	A.9.1.1	访问控制策略	是	本公司基于以下原则制定文件化的访问控制策略（在《用户访问管理程序》中描述），明确规定访问的控制要求，规定访问控制规则和每个用户或用户组的访问权力，访问规则的制定基于以下方面考虑： a）每个业务应用的安全要求； b）在不同系统与网络间，访问控制与信息分类策略要保持一致； c）数据和服务访问符合有关法律和合同义务的要求； d）对各种访问权限的实施管理。	《用户访问管理程序》访问控制策略
	A.9.1.2	网络和网络服务的访问	是	本公司建立并实施网络服务安全策略，以确保网络服务安全与服务质量。	《用户访问管理程序》访问控制策略
	A.9.2 用户访问管理				
	A.9.2.1	用户注册和注销	是	根据访问控制策略确定的访问规则，访问权限管理部门对用户（包括第三方用户)进行书面访问授权，若发生以下情况，对其访问权将从系统中予以注销： a）内部用户雇佣合同终止时； b）内部用户因岗位调整不再需要此项访问服务时； c）物理访问合同终止时； d）其它情况必须注销时。	《用户访问管理程序》访问控制策略
	A.9.2.2	用户访问配置	是	用户访问公司信息和应用系统功能的授权执行《用户访问管理程序》。 为支持访问限制的要求，各应用系统按下列要求控制： a）控制用户访问应用系统功能的菜单； b）控制用户访问权，例如读、写、删除及执行。	《用户访问管理程序》访问控制策略

	A.9.2.3	特殊访问权限管理	是	特权分配以“使用需要”（Need-to-use)和“事件紧跟”(Event-QYYS/event)为基础，即需要时仅以它们的功能角色的最低要求为据，有些特权在完成特定的任务后将被收回，确保特权拥有者的特权是工作所需要的且不存在多余的特权（最小特权原则)。 网络系统管理员、安全员拥有特权，只有经过书面授权，其特权才被认可。 当特权拥有者因公出差或其它原因暂时离开工作岗位时，特权部门负责人应对特权实行紧急安排，将特权临时转交可靠人员，以保证系统正常运行；当特权拥有者返回工作岗位时，及时收回特权；特权的交接应有可靠安全的方法。	《用户访问管理程序》访问控制策略
	A.9.2.4	用户的秘密鉴别信息管理	是	各系统管理员按以下过程对被授权访问该系统的用户口令予以分配： a）管理员根据入职员工的工作岗位分配相关临时口令。 b）当用户忘记口令时，可由系统管理员帮其找回或重新分配安全的口令。 c）禁止将口令以无保护的形式存储在计算机系统内。	《用户访问管理程序》访问控制策略
	A.9.2.5	用户访问权限的复查	是	用户访问权限主管部门每半年对一般用户访问权进行评审，对特权用户每季度进行评审一次，注销非法用户或过期无效用户的访问权，评审结果应予以保持。	《用户访问管理程序》访问控制策略
	A.9.2.6	访问权限的移除或调整	是	员工离职或工作变动前，应解除对信息和信息处理设施访问权限，或根据变化作相应的调整。	《用户访问管理程序》访问控制策略
	A.9.3 用户职责				
	A.9.3.1	秘密鉴别信息的使用	是	本公司明确规定了口令安全选择与使用要求，所有用户须严格遵守。	《用户访问管理程序》访问控制策略
	A.9.4 系统和应用访问控制				

	A.9.4.1	信息访问限制	是	根据本公司管理要求和访问策略，向授权的用户提供访问信息和应用系统功能。用户访问公司信息和应用系统功能的授权执行《用户访问管理程序》。 为支持访问限制的要求，各应用系统按下列要求控制： a）控制用户访问应用系统功能的菜单； b）控制用户访问权，例如读、写、删除及执行。	《用户访问管理程序》 访问控制策略
	A.9.4.2	安全登录规程	是	本公司通过路由技术手段提供安全的系统登录程序。	《用户访问管理程序》 访问控制策略
	A.9.4.3	口令管理系统	是	公司部署实施口令管理，通过技术手段提供有效的、互动的设施以确保口令质量。除非一次性的口令系统，通过操作系统的强制措施要求用户定期变更口令。	《用户访问管理程序》 口令控制策略
	A.9.4.4	特权实用程序的使用	是	研发运营部应对系统工具程序（System Utility Program）的使用进行限制和严格控制，只有经过授权的系统管理员才可以使用系统工具程序，如漏洞扫描工具等。	《用户访问管理程序》 特权访问管理策略
	A.9.4.5	程序源代码的访问控制	是	为降低计算机程序被破坏的可能性，系统设计开发部按以下要求对源程序库（源代码）实施管理： a）可能的话，不将源程序库保存在运作系统中，源程序尽量与应用分开； b）各项应用应指定程序库管理员； c）信息技术支持人员不应当自由访问源程序库； d）源程序库的更新和向程序员发布的源程序，应由指定的程序库管理员根据授权来完成。	《用户访问管理程序》 访问控制策略

A.10 密码

A.10 密码	A.10.1 密码控制				
	A.10.1.1	密码控制的使用策略	是	识别需要采用加密保护的信息以及保护的手段，本公司在与外部信息交换过程中涉及的需用加密控制的信息有：员工从外部远程访问公司系统数据、员工从外部访问公司邮箱，针对此类信息与外部交换的过程应使用 VPN 加密控制；财务人员使用的 USB KEY。	《数据安全管理程序》 远程工作策略 加密控制策略 信息交换策略
	A.10.1.2	密钥管理	是	公司对识别的需要使用加密控制技术的信息，若在采用加密手段时要对密钥的使用进行管理	《数据安全管理程序》 加密控制策略

A.11 物理和环境安全

A.11 物理和环境安全	A.11.1 安全区域				
	A.11.1.1	物理安全边界	是	公司的安全周边为当前公司的办公场所。已具备基本的安全保护。	《安全区域管理程序》 物理访问策略
	A.11.1.2	物理入口控制	是	外来人员进入公司办公区域前需要进行登记。临时访问的第三方应在接待部门同意后，经前台登记可以进入。进入特别安全区域须被授权，进出有记录。	《安全区域管理程序》 物理访问策略
	A.11.1.3	办公室、房间和设施的安全保护	是	本公司制定《安全区域管理程序》，避免出现对办公室、房间和设施的未授权访问。另外，对特别安全区域内的研发运营部和设施进行必要的控制，以防止火灾、盗窃或其它形式的危害，这些控制措施包括： a）办公区域内配备有一定数量的消防设施； b）易燃、易爆物品严禁存放在安全区域内，并与安全区域保持一定的安全距离； c）办公室或房间无人时，应关紧窗户，锁好门；	《安全区域管理程序》 物理访问策略
	A.11.1.4	外部和环境威胁的安全防护	是	办公场所配有消防设施，装修符合消防安全要求；办公区域内的消防设施由综合事务部协调第三方统一管理。	《安全区域管理程序》
	A.11.1.5	在安全区域工作	是	公司没有独立机房，服务器等存储设备存放在公司的独立区域内；公司高管办公室为安全区。相关管理制度确保重要的信息处理设备和保密文件严格受控。	《安全区域管理程序》
	A.11.1.6	交接区	是	公司外的送水人员、邮件快件投递人员、送货人员在送水、投递、送货送餐过程中，未经允许不得进入前台接待区以外的安全区域。	《安全区域管理程序》 物理访问策略
	A.11.2 设备				

	A.11.2.1	设备安置和保护	是	设备使用部门负责对设备进行定置管理和保护。为降低来自环境威胁和危害的风险，减少未经授权的访问机会，特采取以下措施： a）设备的定置，要考虑到尽可能减少对工作区不必要的访问； b）对需要特别保护的设备加以隔离； c）采取措施，以尽量降低盗窃、火灾、爆炸、吸烟、灰尘、震动、化学影响、电源干忧、电磁辐射等威胁造成的潜在的风险； d）禁止在信息处理设施附近饮食、吸烟。	《安全区域管理程序》 设备及布缆安全策略
	A.11.2.2	支持性设施	是	针对重要服务器及设备提供 ups，确保不间断供电，其他办公电脑和网络连接设备经风险评估可以接受供电中断的风险。机房环境和机房支持设施由研发运营部负责管理。	《安全区域管理程序》 设备及布缆安全策略
	A.11.2.3	布缆安全	是	为保障传输数据或支持信息服务的电源布缆和通信布缆免受窃听或破坏，现对布缆安全要求如下： a）信息处理设施的电源和通信线路不得采用明线布置，应在地下、墙内或采用线槽保护。 b）电缆布线要避开公共区域。 C)电源电缆与通信电缆分开，防止干扰。通信电缆与电力电缆分开铺设，防止干扰。	《安全区域管理程序》 设备及布缆安全策略
	A.11.2.4	设备维护	是	计算机信息网络系统设备及用户计算机终端（包括笔记本电脑）由研发运营部按照《信息处理设施管理程序》进行维护。	《信息处理设施管理程序》
	A.11.2.5	资产的移动	是	重要信息设备、保密信息的迁移应被授权，迁移活动应被记录。	《安全区域管理程序》
	A.11.2.6	组织场所外的设备与资产安全	是	笔记本电脑在离开规定的区域时，经过部门领导授权并对其进行严格控制，防止其丢失和未经授权的访问，具体按照《笔记本电脑管理规定》执行。	《笔记本电脑管理规定》 便携式计算机安全策略
	A.11.2.7	设备的安全处置或再利用	是	含有敏感信息的设备在报废或改作他用时，由使用部门用安全的处置方法，将设备中存储的敏感信息清除并保存清除记录。	《安全区域管理程序》

	A.11.2.8	无人值守的用户设备	是	对于无人值守的设备需按照公司管理程序的要求，实施必要的管理。 托管的服务器由托管方负责执行维护。	《安全区域管理程序》
	A.11.2.9	清空桌面和屏幕策略	是	公司制定清除桌面、清除屏幕的要求并实施，各部门负责人负责监督。 各部门员工自觉履行该策略的日常实施。	《安全区域管理程序》 清洁桌面和清屏策略

A.12 运行安全

A.12 运行安全	A.12.1 运行规程和职责				
	A.12.1.1	文件化的操作规程	是	本公司按照信息安全方针的要求，建立并实施文件化的作业程序，文件化程序的控制执行《文件控制程序》。	《文件控制程序》
	A.12.1.2	变更管理	是	对信息处理设施、软件等方面的更改实施严格控制。在更改前评估更改所带来的潜在影响，正式更改前履行更改审批手续，并采取必要的措施确保不成功更改的恢复。	《信息系统应用管理程序》 变更管理安全策略
	A.12.1.3	容量管理	是	公司负责对信息网络系统的容量（CPU 利用率、内存和硬盘空间大小、传输线路带宽）需求进行监控，并对将来容量需求进行策划，适当时机进行容量扩充。	《信息系统监控管理程序》
	A.12.1.4	开发、测试和运行环境的分离	是	软件开发、测试活动分别在不同的工作组完成，且通过不同的虚拟机实施业务活动。	《信息系统开发监视管理程序》
	A.12.2 恶意代码防范				
	A.12.2.1	恶意代码的控制	是	研发运营部为控制恶意软件的主管部门，负责提供防范恶意软件的技术工具并对技术工具进行实时升级，各部门具体负责本部门的恶意软件预防控制工作。 a）技术工具的应用及其升级要求； b）查杀病毒的周期； c）预防恶意软件意识培训； d）预防恶意软件的一般要求； e）对重要系统的防范恶意软件的特殊要求； f）发生恶意软件的侵害应急措施。	《病毒防范管理程序》 病毒防范策略
	A.12.3 备份				

	A.12.3.1	信息备份	是	本公司根据风险评估的结果对重要数据库、软件等进行备份。研发运营部为对公司所有服务器中的数据进行备份，并定期对备份的数据进行恢复测试。	《信息备份管理规定》
	A.12.4 日志和监视				
	A.12.4.1	事态日志	是	外部人员进入由前台进行登记。 公司所有的信息处理设施其日志处于打开状态，做审计时的证据。	《信息系统监控管理程序》
	A.12.4.2	日志信息的保护	是	实施控制，防止对日志记录设施的未经授权的更改和出现操作问题.	《信息系统监控管理程序》
	A.12.4.3	管理员和操作员日志	是	管理员和操作员的日志应该包括： a）事情（成功或失败）发生的时间； b）事情的有关信息（如：操作的文件）或故障信息； c）涉及哪一个账号以及哪一个管理员或操作员； d）涉及哪一个过程。	《信息系统应用管理程序》
	A.12.4.4	时钟同步	是	公司用网络时间协议保持所有服务器与主时钟同步。保持本地时间与世界标准时间（UTC）一致。	《信息系统应用管理程序》
	A.12.5 运行软件控制				
	A.12.5.1	运行系统的软件安装	是	研发运营部对软件在作业系统的执行进行严格控制，在新软件安装或软件升级之前，应经主管部门负责人审核同意后方可进行。 计算机终端用户除非授权，否则严禁私自安装任何软件。	《软件管理程序》
	A.12.6 技术脆弱性管理				
	A.12.6.1	技术脆弱性的管理	是	研发运营部及各产业群对技术薄弱点应进行风险评估，进行专项分析，制订风险处理计划，根据风险处理计划采取对应的技术和管理措施。	《技术薄弱点管理程序》 技术脆弱性管理策略
	A.12.6.2	软件安装限制	是	公司对所有岗位所需软件进行规定，限制所有人员安装软件的权限。	《个人计算机管理程序》

	A.12.7 信息系统审计的考虑				
	A.12.7.1	信息系统审计的控制	是	正式审核之前，审核组应明确技术性审核的项目与要求，防止审核活动本身造成不必要的安全风险。	

A.13 通信安全

A.13 通信安全	A.13.1 网络安全管理				
	A.13.1.1	网络控制	是	本公司网络安全控制措施包括： a)内外网通过硬件防火墙实施隔离； b)研发运营部在遇特定项目时，实施物理隔离； c)对网络设备定期维护； d)对防火墙、交换机等实施安全配置管理； e)对用户访问网络实施授权管理； f)实施有效的安全策略； g)对系统的变更进行严格控制； h)对网络的运行情况进行监控； i)对网络设备的变更进行控制； j)对网络系统管理与操作人员的管理。	《网络安全管理程序》 《信息处理设施管理程序》
	A.13.1.2	网络服务的安全	是	研发运营部根据组织的安全策略，识别现有的网络服务，由授权的网络系统安全管理员进行参数配置与维护管理。 选择资源良好的多家网络接入供应商。	《网络安全管理程序》 《用户访问管理程序》
	A.13.1.3	网络隔离	是	公司目前对网络进行了基本的逻辑隔离，具体要求按照《用户访问管理程序》的要求执行。	《用户访问管理程序》
	A.13.2 信息传输				

	A.13.2.1	信息传输策略和规程	是	公司在与顾客进行产品（设计）数据、测试程序等数据与软件交换的过程中采用以下的安全控制措施： a）签订安全保密协议； b）如果顾客有要求，采用加密方式传输数据； c）由授权人员接收并登记。	《网络安全管理程序》
	A.13.2.2	信息传输协议	是	在与顾客进行数据与软件交换的过程中签订相关的安全控制协议： 明确双方的安全责任与安全交接方式； 如果有要求，采用加密方式传输数据。	《网络安全管理程序》 信息交换策略
	A.13.2.3	电子消息发送	是	基于业务及管理的需要，及减少企业秘密被泄露与防范计算机病毒的原则，本公司建立了电子邮件安全使用的策略，并将该策略传达到所有员工予以执行。 本公司允许只有授权的用户履行审批手续才可以使用电子邮件。	《网络安全管理程序》 电子邮件策略
	A.13.2.4	保密或不泄露协议	是	由综合事务部在现有的管理制度中增加对员工信息安全管理要求。所有正式员工及临时聘用的员工，包括实习人员签订保密协议。	《保密协议》

A.14 系统获取、开发和维护

A.14 系统获取、开发和维护	A.14.1 信息系统的安全要求				
	A.14.1.1	信息安全要求分析和说明	是	研发运营部在进行新系统开发或系统更新时，首先对系统进行分析，根据业务功能要求及信息安全要求明确规定控制要求，包括： a） 系统的安全特性； b） 对现有的系统安全影响； c） 设计过程中的安全控制要求。 系统（软件）本身的功能及安全特性在设计开发输入时明确提出，并进行评审。	《信息系统开发建设管理程序》 《信息系统应用管理程序》 《信息系统监控管理程序》
	A.14.1.2	公共网络上应用服务的安全保护	是	公司购买了正版的杀毒软件、并且设置权限和网络安全管理程序、数据安全管理程序	《病毒防范管理程序》 《数据安全管理程序》
	A.14.1.3	应用服务事务的保护	是	应保护应用服务事务中的信息，以防止不完善的传输、错误路由、未授权的消息变更、未授权的泄露、未授权的消息复制或重放	《信息系统开发建设管理程序》 《信息系统应用管理程序》
	A.14.2 开发和支持过程中的安全				
	A.14.2.1	安全的开发策略	是	公司建立《信息系统开发建设管理程序》，统一规定安全的开发环境、编码规范、安全要求、安全检查等内容。	《信息系统开发建设管理程序》
	A.14.2.2	系统变更控制规程	是	为使信息系统的损害降至最小，对应用系统软件在开发过程中的任何更改，须进行适当的测试与评审，经开发软件负责人批准后予以实施。 操作系统（OS）及应用系统的升级须经过系统主管部门测试、评审与批准后方可进行。	《信息系统开发建设管理程序》 变更管理安全策略
	A.14.2.3	运行平台变更后对应用的技术评审	是	当操作系统（OS）发生更改时，操作系统更改对应用系统的影响应由系统主管部门进行评审，确保对应用程序的作业或安全措施无不利影响。	《信息系统开发建设管理程序》

	A.14.2.4	软件包变更的限制	是	本公司不鼓励修改软件包，如果有必要进行更改，更改部门在实施前进行风险评估，确定必须的控制措施，保留原始软件，并在完全一样的复制软件上进行更改，更改实施前须得到系统主管部门的授权。	《信息系统开发建设管理程序》 变更管理安全策略
	A.14.2.5	安全的系统工程原则	是	公司建立《信息系统开发建设管理程序》，对内部信息系统的规划、实施、定期检查与评估进行规定。	《信息系统开发建设管理程序》
	A.14.2.6	安全的开发环境	是	软件开发项目依据公司软件开发规范中规定的开发环境，建立本项目的安全开发环境。	《信息系统开发建设管理程序》
	A.14.2.7	外包开发	否	公司目前没有该项业务，删减。	
	A.14.2.8	系统安全测试	是	应用系统上线前，应指定部门和人员，按照事先定义的验收与测试标准进行验收，并提供测试报告。验收与测试宜考虑以下要素： 1）性能和计算机容量要求； 2）差错恢复和重启规程以及应急计划； 3）按照已定义标准，准备和测试日常的运行规程； 4）确定的一组安全控制措施要到位； 5）有效的人工操作规程； 6）系统的容错性； 7）新系统的安装对现有系统无负面影响的证据，特别是在高峰处理时间，例如月末； 8）考虑新系统对组织总体安全影响的证据； 9）新系统的操作或使用培训； 10）易用性，这影响到用户使用，避免人员出错。	《信息系统开发建设管理程序》
	A.14.2.9	系统验收测试	是		《信息系统开发建设管理程序》
	A.14.3 测试数据				
	A.14.3.1	测试数据的保护	是	当系统测试数据使用作业数据，并且包含敏感信息时，测试人员按以下要求对测试数据进行保护： a）对测试应用系统的活动进行授权；b）作业信息每一次复制到测试应用系统，须被系统主管部门授权； c）测试完成之后，立即从测试应用系统中消除作业信息。	《信息系统开发建设管理程序》

A.15 供应商关系

A.15 供应商关系	A.15.1 供应商关系中的信息安全				
	A.15.1.1	供应商关系的信息安全策略	是	对第三方的服务的交付，包括协议规定的安全安排、服务定义以及服务管理等方面进行管理和验收。确保第三方保持充分的服务能力，并且具备有效的工作计划，即便发生重大的服务故障或灾难也能保持服务交付的连贯性。	《相关方信息安全管理程序》
	A.15.1.2	在供应商协议中解决安全	是	综合事务部负责识别采购活动的风险，明确采购活动的信息安全要求，在采购合同中明确规定信息安全要求。	《供应商管理控制程序》供应商访问策略
	A.15.1.3	信息与通信技术供应链	是	综合事务部负责识别采购活动中相关信息、通信技术服务和产品供应链的风险，明确采购活动的信息安全要求，在采购合同中明确规定信息安全要求。	《相关方信息安全管理程序》
	A.15.2 供应商服务交付管理				
	A.15.2.1	供应商服务的监视和评审	是	相关部门人员跟踪管理第三方服务，确保第三方分配的职责符合协议要求。对协议要求，特别是安全要求的符合性进行监控得到充分可用的资源和技术技能支持。	《相关方信息安全管理程序》
	A.15.2.2	供应商服务的变更管理	是	对第三方服务更改的管理过程需要考虑： a）组织的更改，包括加强当前提供的服务，开发新应用程序和系统，修改和更新方针及程序，解决信息安全事件，提高安全性的新控制。 b）第三方服务的更改，包括更改和加强网络，使用新技术，更改服务设施的物理位置，更改供应商。	《相关方信息安全管理程序》供应商访问策略

A.16 信息安全事件管理	A.16.1 信息安全事件的管理和改进				
	A.16.1.1	职责和规程	是	事故主管部门接到报告以后，应立即进行迅速、有效和有序的反应。	《信息安全事件管理程序》信息安全监控策略
	A.16.1.2	报告信息安全事态	是	安全事件事故一经发生，发现者、事情、事故责任者应立即向主管部门报告，主管部门和责任部门应及时对事情、事故进行反应处理。所有员工有报告安全事态、事件的义务。	《信息安全事件管理程序》《安全奖惩管理规定》信息安全监控策略
	A.16.1.3	报告信息安全弱点	是	全体员工应按照要求及时识别安全薄弱点及可能的安全威胁，一旦发现应及时向有关人员或部门报告并记录，主管部门或安全管理负责人应采取有效的预防措施，防止威胁的发生。	《信息安全事件管理程序》
	A.16.1.4	信息安全事态的评估和决策	是	研发运营部针对所有员工报告的安全事态进行评估，确认是否造成损失，以判断安全事态、事件的影响，以及公司目前实施的控制措施的有效性。	《信息安全事件管理程序》信息安全监控策略
	A.16.1.5	信息安全事件的响应	是	信息安全小组对信息安全事件遵循《信息安全事件管理程序》，调动公司相关人员实施处理行动。	《信息安全事件管理程序》信息安全监控策略

A.16 信息安全事件管理

	A.16.1.6	从信息安全事件中学习	是	事故发生后，主管部门对事故发生的原因、类型、损失进行鉴定，提出防止此类事故再次发生的措施或建议，形成事故调查分析及处理报告，责成有关部门实施纠正措施。 事故和处理过程结果应予以记录，重大事故应提交公司管理层评审。	《信息安全事件管理程序》
	A.16.1.7	证据的收集	是	综合事务部负责发生法律纠纷与诉讼的证据收集，并确保证据收集应符合以下要求： a）所呈证据应符合国家有关的证据法规； b）符合用于提供可接受证据的任何已发布的标准或法规； c）对已收集到的证据进行安全的保管，防止未经授权的更改或破坏； d）收集到的证据符合法庭所要求的形式。	《信息安全事件管理程序》

A.17 业务连续性管理的信息安全方面

A.17 业务连续性管理的信息安全方面	A.17.1 信息安全的连续性				
	A.17.1.1	规划信息安全连续性	是	公司建立并实施《信息业务连续性管理程序》，在发生灾难或安全故障时，实施持续性管理计划，确保关键业务及时得到恢复。	《信息业务连续性管理程序》
	A.17.1.2	实施信息安全连续性	是	有关部门应编制《业务持续性管理实施计划》，由管理者代表批准，以便在储存数据、培训、测试等关键业务发生中断或故障后，实施持续性管理计划，以保证公司关键业务中断的及时恢复。 持续性计划应对应急措施和有关部门与人员的职责给予明确规定。	《信息业务连续性管理程序》
	A.17.1.3	验证、评审和评价信息安全连续性	是	每年综合事务部组织有关部门采取适宜的测试方法对《业务持续性管理实施计划》进行测试，并保持测试记录；每次测试后，研发运营部组织与计划有关的部门对计划的时效和有效性进行评审，必要时，对业务持续性计划进行修改。	《信息业务连续性管理程序》
	A.17.2 冗余				

	A.17.2.1	信息处理设施的可用性	是	研发运营部识别公司关键业务和关键应用，每年重新确定承载的信息处理设施的可用性，根据公司成本接受能力，编制需实现冗余的设施清单，并提交管理评审会议进行评审，公司总经理进行批准实施。	《信息处理设施管理程序》

A.18 符合性

A.18 符合性	A.18.1 符合法律和合同要求				
	A.18.1.1	可用的法律和合同要求的识别	是	综合事务部负责组织收集与信息安全有关的法律法规并对适用性评价，确定其实用范围和具体适用条款，形成适用的法律法规清单，将法律法规一起通过网络传达给有关部门并予以执行。 综合事务部负责每年应对法律法规的有效性进行重新评价，保持适用的法律、法规的有效最新版本。每年对法律法规的符合性进行评价。	《法律法规管理程序》

	A.18.1.2	知识产权	是	本公司严格执行国家有关知识产权方面的法律法规，保证使用合法的正版软件，并通过以下方法进行控制： a）确定获得合法软件的途径； b）每年进行一次软件资产清查，确保正在使用的软件已经被适当的授权； c）保留许可证、手册等拥有者的证明和证件； d）确保用户数不超过所允许的上限； e）只允许安装认可的软件和特许的产品； f）严禁员工私自安装任何软件。	《法律法规管理程序》
	A.18.1.3	记录的保护	是	各部门应按照有关法律、法规要求，明确规定重要记录的保存期限并提供适当的保护，防止丢失、损坏和伪造。	《法律法规管理程序》
	A.18.1.4	个人可识别信息的隐私和保护	是	对处理与个人数据与信息有关的部门应按照国家有关规定对个人信息进行妥善管理与保护，防止丢失或泄露个人秘密。	《法律法规管理程序》
	A.18.1.5	密码控制规则	是	使用符合相关协议、法律和法规的要求和限制的加密控制措施	《法律法规管理程序》
	A.18.2 信息安全评审				
	A.18.2.1	信息安全的独立评审	是	信息安全管理体系的内部审核员由有审核能力和经验的人员组成（包括 IT 方面的专家），并接受 ISMS 内部审核员培训且考评合格。内部审核员在现场审核时保持审核的独立性，并不审核自己的工作。内审员获得授权，在审核期间不受行政的领导的限制，直接对审核组长负责。	《法律法规管理程序》
	A.18.2.2	符合安全策略和标准	是	每年组织至少一次信息安全管理体系内部审核，每次审核的范围覆盖与信息安全管理体系有关的所有部门与安全区域，确保职责范围内的所有安全程序正确完成，符合安全方针和标准。	《法律法规管理程序》
	A.18.2.3	技术符合性评审	是	研发运营部对漏洞扫描工具进行管理，使用者应被授权，检查工作在监督的情况下进行，审核活动应被记录。	《法律法规管理程序》

信息安全策略

版 次 号：V1.0 版

受控标识：受控

发放编号：

编　　制：综合事务部 2022.05.04

审　　核：史佳 2022.05.04

批　　准：张俊 2022.05.04

2022-05-04 发布　　2022-05-04 实施

泰州城发数字科技有限公司　发布实施

目录

泰州城发数字科技有限公司 管理文件		
信息安全策略	文件编号	CFSZ/CL-03-2022
	版次	V1.0

信息资源保密策略	
介绍	保密策略是用于为信息资源用户建立限制的机制。通过一定权限管理以区分内外部用户的信息资源的访问。
目 的	该策略的目的是明确用户对信息资源沟通的保密需求。
适用范围	该策略适用于使用信息资源的所有人员。
术语定义	略
信息资源保密策略	■ 在公司内部保存和控制的电子文件应该得到控制，只有得到授权的人员才能访问； ■ 为加强信息安全，信息技术小组可以记录和评审信息系统中存储和传递的任何信息。为了达到此目的，综合事务部还可以捕获任何用户活动，如通讯记录以及访问的网站； ■ 为了商业目的，客户方将信息委托给公司内部保管，那么公司的所有工作人员都必须尽最大的努力保护这些信息的保密性和安全性。 ■ 用户必须向适当的管理者报告公司内部计算机安全的任何薄弱点，可能的误用事故或者相应授权协议的违背情况； ■ 在未经授权或获得明确同意的情况下，用户不可以尝试访问公司内部系统中包含的任何数据或程序。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
HXYD/SC-0301-2021 网络访问策略	
介绍	网络基础设施是提供给所有信息资源用户的中心设施。重要的是这些基础设施（包括电缆以及相关的设备）要持续不断的发展以满足需求，然而也要求同时高速发展网络技术以便将来提供功能更强大的用户服务。
目 的	该策略的目的是建立网络基础设施的访问和使用规则。这些规则是保持信息完整性、可用性和保密性所必需的。

适用范围	该策略适用于访问任何信息资源的所有人。
术语定义	略
网络访问策略	■ 用户不可以以任何方式扩散或再次传播网络服务。未经综合事务部批准不可以安装路由器、交换机或者无线访问端口； ■ 在未经综合事务部批准的情况下，用户不可以安装提供网络服务的硬件或软件； ■ 需要网络连接的计算机系统必须符合信息服务规范； ■ 下用户禁止私自下载、安装或运行安全程序或应用程序去扫描系统的安全薄弱点，如，口令破解程序、监听器、网络绘图工具、或端口扫描工具。即使网络管理人员因工作需要必须使用以上工具时，也应取得综合事务部批准。 ■ 在局域网上进行文件共享时必须指定访问权限，敏感信息严禁使用 everyone 权限。 ■ 任何员工在访问网络资源时必须使用专属于自己的帐号 ID，不得使用他人的帐号访问网络资源。 ■ 网络分为办公网络和生产环境网络，办公网络又分为日常办公网络和专用访问网络 ■ 生产环境网络与办公环境网络宜进行分割，以确保访问的控制。 ■ 不得从生产环境下载拷贝等操作 ■ 只能从公司指定办公网络（公司专门的网络通道）访问远程的服务器 ■ 修改远程服务器的内容必须要提前申请报告，且要有详细的操作步骤 ■ 网络管理人员拥有网络基础设施并对其负责，而且还要对基础设施的发展和增加进行管理； ■ 为了提供稳固的网络基础设施，所有电缆必须由综合事务部或被认可的合同方安装； ■ 所有连接到网络的硬件必须服从综合事务部的管理和监控标准； ■ 在没有综合事务部批准的情况下，不能对活动的网络管理设备的配置进行更改；

	■ 网络基础设施支持一系列合理定义的、被认可的网络协议。使用任何未经认可的协议都必须经过综合事务部的批准； ■ 支持协议的网络地址由综合事务部集中分配、注册和管理； ■ 网络基础设施与外部供应商网络的所有连接都由综合事务部负责。这包括与外部网络的连接； ■ 在未获得综合事务部书面授权的情况下，部门不得使用防火墙；
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
HXYD/SC-0302-2021 访问控制策略	
介绍	应根据业务和安全要求，控制对信息和信息系统的访问。
目 的	该策略的目的是为了控制对信息和信息系统的访问。
适用范围	该策略适用于进行信息和信息系统访问的所有人员。
术语定义	略
访问控制策略	■ 公司内部可公开的信息不作特别限定，允许所有用户访问； ■ 公司内部部分公开信息，根据业务需求访问，访问人员提出申请，经访问授权管理部门认可，访问授权实施部门实施后用户方可访问； ■ 公司网络、信息系统根据业务需求访问，访问人员提出申请，经综合事务部认可，实施后用户方可访问； ■ 综合事务部安全管理员按规定周期对访问授权进行检查和评审； ■ 访问权限应及时撤销，如在申请访问时限结束时、员工聘用期限结束时、第三方服务协议中止时； ■ 用户不得访问或尝试访问未经授权的网络、系统、文件和服务； ■ 远程用户应该通过公司批准的连接方式； ■ 在防火墙内部连接内部网络的计算机不允许连接 INTERNET ，除非获得综合事务部的批准； ■ 用户不得以任何方式私自安装路由器、交换机、代理服务器、无线网络

	访问点（ 包括软件和硬件 ）等； ■ 在信息网、外联网安装新的服务（ 包括软件和硬件 ）必须获得综合事务部的批准； ■ 用户不得私自撤除或更换网络设备。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
HXYD/SC-0303-2021 物理访问策略	
介绍	技术支持人员、安全管理员、IT 管理员以及其他人员可能因工作需要访问信息资源物理设施。对信息资源设施物理访问的批准、控制以及监控对于全局的安全是极其重要的。
目 的	该策略的目的是为信息资源设施物理访问的批准、控制、监控和删除建立规则。
适用范围	该策略适用于组织中负责信息资源安装和支持的所有人员，负责信息资源安全的人员以及数据的所有者。
术语定义	略
物理访问策略	■ 所有物理安全系统必须符合相应的法规，但不仅限于建设法规以及消防法规； ■ 对所有受限制的信息资源设施的物理访问必须形成文件并进行控制； ■ 所有信息资源设施必须依据其功能的关键程度或重要程度进行物理保护； ■ 对信息资源设施的访问必须只授权给因职责需要访问设施的支持人员和合同方； ■ 授权使用卡和/或钥匙访问信息资源设施的过程中必须包括设施负责人的批准； ■ 拥有信息资源设施访问权的每一个人员都必须接受设施应急程序培训，并且必须签署相应的访问和不泄密协议；

	■ 访问请求必须发自相应的数据/系统所有者； ■ 访问卡和/或钥匙不可以与他人共享或借给他人； ■ 访问卡和/或钥匙不需要时必须退还给信息资源设施负责人。在退还的过程中，卡不可以再分配给另一个人； ■ 访问卡和/或钥匙丢失或被盗必须向信息资源设施的负责人报告； ■ 卡和/或钥匙上除了退回的地址外不可以有标志性信息； ■ 所有允许来宾访问的信息资源设施都必须使用签字出/入记录来追踪来宾的访问； ■ 信息资源设施的持卡访问记录以及来宾记录必须保存，并依据被保护信息资源的关键程度定期评审； ■ 在持卡和/或钥匙的人员发生变化或离职时，信息资源设施的负责人必须删除其访问权限； ■ 在信息资源设施的持卡访问区，来宾必须由专人陪同； ■ 信息资源设施的负责人必须定期评审访问记录以及来宾记录，并要对异常访问进行调查； ■ 信息资源设施的负责人必须定期评审卡和/或钥匙访问权，并删除不再需要访问的人员的权限； ■ 对限制访问的房间和场所必须进行标记，但是描述其重要性的信息应尽可能少。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
供应商访问策略	
介绍	供应商在支持硬件和软件管理以及客户运作方面有重要作用。供应商可以远程对 数据和审核日志进行评审、备份和修改，他们可以纠正软件和操作系统中的问题，可以监控并调整系统性能，可以监控硬件性能和错误，可以修改周遭系统，并重新设置警告极限。由供应商设置的限制和控制可以

	消除或降低收入、信誉损失或遭破坏的风险。
目 的	该策略的目的是为减缓供应商访问组织资产带来的风险。
适用范围	该策略适用于所有需要访问组织的供应商。
术语定义	略
第三方访问策略	■ 供应商必须遵守相应的策略、操作标准以及协议，包括但不仅限于： ✧ 安全策略； ✧ 保密策略； ✧ 审核策略； ✧ 信息资源使用策略。 ■ 供应商协议和合同必须规定： ✧ 供应商应该访问的信息； ✧ 供应商怎样保护信息； ✧ 合同结束时供应商所拥有的信息返回、毁灭或处置方法； ✧ 供应商只能使用用于商业协议目的的信息和信息资源； ✧ 在合同期间供应商所获得的任何信息都不能用于供应商自己的目的或泄漏给他人。 ■ 应该向综合事务部提供与供应商的合同要点。合同要点能确保供应商符合策略的要求 ； ■ 为供应商分配类型，如 IT 基础组件运维服务、系统维护服务、网络维护服务等； ■ 需定义不同类型供应商可以访问的信息类型，以及如何进行监视和工作访问的权限； ■ 供应商访问信息的人员范围仅限于工作需要的人员，授权需获得综合事务部的批准； ■ 供应商权限人员不得将已授权的身份识别信息和相关设备透露、借用给其他人员，工作结束后应该立即注销访问权限及清空资料； ■ 针对与供应商人员交互的组织人员开展意识培训，培训内容涉及基于供应商类型和供应商访问组织系统及信息级别的参与规则和行为；

	■ 如适合可与供应商就关系中的信息安全签署保密或交换协议； ■ 每一个供应商必须提供在为合同工作的所有员工清单。员工发生变更时必须在 24 小时之内更新并提供； ■ 每一个在组织场所内工作的供应商员工都必须佩带身份识别卡。当合同结束时，此卡应该归还； ■ 可以访问敏感信息资源的每一个供应商员工都不能处理这些信息； ■ 供应商员工应该直接向恰当的人员直接报告所有安全事故； ■ 如果供应商参与安全事故管理，那么必须在合同中明确规定其职责； ■ 供应商必须遵守所有适用的更改控制过程和程序； ■ 定期进行的工作任务和时间必须在合同中规定。规定条件之外的工作必须由相应的管理者书面批准； ■ 必须对供应商访问进行唯一标识，并且对其进行的口令管理必须符合口令实施规范和特殊访问实施规范。供应商主要的工作活动必须形成日志并且在管理者需要的时候可以访问。日志的内容包括但不仅限于：人员变化、口令变化、项目进度重要事件、启动和结束时； ■ 当供应商员工离职时，供应商必须确保所有敏感信息在 24 小时内被收回或销毁； ■ 在合同或邀请结束时，供应商应该将所有信息返回或销毁，并在 24 小时内提交一份返回或销毁的书面证明； ■ 在合同或邀请结束时，供应商必须立即交出所有身份识别卡、访问卡以及设备和供应品。由供应商保留的设备和/或供应品必须被管理者书面授权； ■ 要求供应商必须遵守所有规定和审核要求，包括对供应商工作的审核； ■ 在提供服务时，供应商使用的所有软件必须进行相应的清点并许可。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略

雇员访问策略	
介绍	雇员工作在信息安全区域，工作中需要使用公司的各种信息处理设施，需要访问公司的各种信息资产，因此每一个雇员有义务和责任保护好公司信息资产的安全。
目 的	本策略未访问本公司信息资源的全体雇员，这种访问是出于业务需要的，涉及物理和行政安全管理需求的网络连接、雇员的职责及信息保护的准则。
适用范围	该策略适用于公司的任何雇员，雇员对信息资源的访问，包括信息处理设施设备和技术资源。
术语定义	略
雇员访问策略	■ 雇员必须遵守相应的策略、操作标准以及协议，包括但不仅限于： ✧ 《信息资源保密策略》； ✧ 《病毒防范策略》； ✧ 《可移动代码防范策略》； ✧ 《信息交换策略》； ✧ 《清洁桌面和清屏策略》； ✧ 《网络访问策略》； ✧ 《便携式计算机安全策略》； ✧ 《互联网使用策略》； ✧ 《电子邮件策略》。 ■ 雇员在意识到有安全事件发生时应该第一时间向上层领导报告； ■ 雇员应该直接向恰当的人员直接报告所有安全事故； ■ 雇员必须遵守所有适用的变更管理程序； ■ 当雇员离职时，必须确保所有敏感信息在 24 小时内被收回或销毁； ■ 在合同结束时，雇员应该将所有信息返回或销毁，并在 24 小时内提交一份返回或销毁的书面证明，并由资产责任人签字认可； ■ 在合同结束时，雇员必须立即交出所有身份识别卡、访问卡以及设备和供应品。由雇员保管的设备和 /或供应品的回收必须由资产责任人签字认可；

	■ 要求雇员必须遵守所有规定和审核要求。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
设备及布缆安全策略	
介绍	网络基础设施是向所有信息资源用户提供服务的中心设施。这些基础设施（包括电源馈送和数据传输的电缆以及相关的设备）需要持续不断的发展以满足用户需求，然而同时也要求网络技术高速发展以便将来能够提供功能更强大的用户服务。
目 的	■ 该方针的目的保护设备免受物理的和环境的威胁，减少未授权访问信息的风险。防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断； ■ 为了安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会； ■ 为了保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断，应有足够的支持性设施（供电、供水、通风和空调等）来支持系统； ■ 为了保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听或损坏，电源馈送和数据通讯的电缆必须确保安全； ■ 为了确保设备持续的可用性和完整性，设备应予以正确地维护； ■ 为了对组织非现场设备采取安全措施，要考虑工作在组织场所以外的不同风险； ■ 为了确保涉密信息不泄露，在存储介质销毁之前，任何敏感信息和注册软件已被删除或安全重写； ■ 为了确保涉密信息不泄露，设备、信息或软件在授权之前不应带出组织场所。
适用范围	该方针适用于网络设备设施的建设和维护人员。
术语定义	略

设备及布缆安全策略	■ 设备安置和保护方针 ✧ 设备应进行适当安置，以尽量减少不必要的对工作区域的访问； ✧ 应把处理敏感数据的信息处理设施放在适当的限制观测的位置，以减少在其使用期间信息被窥视的风险，还应保护储存设施以防止未授权访问； ✧ 要求专门保护的部件要予以隔离，以降低所要求的总体保护等级； ✧ 应采取控制措施以减小潜在的物理威胁的风险，例如偷窃、火灾、爆炸、烟雾、水（或供水故障）、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； ✧ 对于可能对信息处理设施运行状态产生负面影响的环境条件（例如温度和湿度）要予以监视； ✧ 所有建筑物都应采用避雷保护； ✧ 应保护处理敏感信息的设备，以减少由于辐射而导致信息泄露的风险； ■ 支持性设施方针 ✧ 支持性设施应定期检查并适当的测试以确保他们的功能，减少由于他们的故障或失效带来的风险。应按照设备制造商的说明提供合适的供电； ✧ 对支持关键业务操作的设备，必须使用支持有序关机或连续运行的不间断电源（UPS）； ✧ 电源应急计划要包括 UPS 故障时要采取的措施。UPS 设备和发电机要定期地检查，以确保它们拥有足够能力，并按照制造商的建议予以测试； ■ 布缆安全方针： ✧ 进入信息处理设施的电源和通信线路宜在地下，若可能，或提供足够的可替换的保护； ✧ 网络布缆要免受未授权窃听或损坏，例如，利用电缆管道或使路由避开公众区域；

✧ 为了防止干扰，电源电缆要与通信电缆分开；

✧ 使用清晰的可识别的电缆和设备记号，以使处理失误最小化，例如，错误网络电缆的意外配线；

✧ 用文件化配线列表减少失误的可能性；

✧ 对于敏感的或关键的系统，更进一步的控制考虑应包括：

＊ 在检查点和终接点处安装铠装电缆管道和上锁的房间或盒子；

＊ 使用可替换的路由选择和/或传输介质，以提供适当的安全措施；

＊ 使用纤维光缆；

＊ 使用电磁防辐射装置保护电缆；

＊ 对于电缆连接的未授权装置要主动实施技术清除、物理检查；

＊ 控制对配线盘和电缆室的访问；

■ 设备维护方针

✧ 要按照供应商推荐的服务时间间隔和规范对设备进行维护；

✧ 只有已授权的维护人员才可对设备进行修理和服务；

✧ 要保存所有可疑的或实际的故障以及所有预防和纠正维护的记录；

✧ 当对设备安排维护时，应实施适当的控制，要考虑维护是由场所内部人员执行还是由外部人员执行；当需要时，敏感信息需要从设备中删除或者维护人员应该是足够可靠的；

✧ 应遵守由保险策略所施加的所有要求。

■ 组织场所外的设备安全方针

✧ 无论责任人是谁，在组织场所外使用任何信息处理设备都要通过管理者授权；

✧ 离开建筑物的设备和介质在公共场所不应无人看管。在旅行时便携式计算机要作为手提行李携带，若可能宜伪装起来；

✧ 制造商的设备保护说明要始终加以遵守，例如，防止暴露于强电磁场内；

✧ 家庭工作的控制措施应根据风险评估确定，当适合时，要施加合

	适的控制措施，例如，可上锁的存档柜、清理桌面策略、对计算机的访问控制以及与办公室的安全通信； ✧ 足够的安全保障掩蔽物宜到位，以保护离开办公场所的设备。安全风险在不同场所可能有显著不同，例如，损坏、盗窃和截取，要考虑确定最合适的控制措施。 ■ 设备的安全处置和再利用方针 ✧ 包含敏感信息的设备在物理上应予以摧毁，或者采用使原始信息不可获取的技术破坏、删除、覆盖信息，而不能采用标准的删除或格式化功能； ✧ 包含敏感信息的已损坏的设备可能需要实施风险评估，以确定这些设备是否要进行销毁、而不是送去修理或丢弃。 ■ 资产移动方针 ✧ 在未经事先授权的情况下，不允许让设备、信息或软件离开办公场所； ✧ 应明确识别有权允许资产移动，离开办公场所的雇员、承包方人员和供应商人员； ✧ 应设置设备移动的时间限制，并在返还时执行符合性检查； ✧ 若需要并合适，要对设备作出移出记录，当返回时，要作出送回记录； ✧ 应执行检测未授权资产移动的抽查，以检测未授权的记录装置，防止他们进入办公场所。这样的抽查应按照相关规章制度执行。应让每个人都知道将进行抽查，并且只能在法律法规要求的适当授权下执行检查。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略

变更管理安全策略	
介绍	信息资源基础设施正在逐步扩大并且越来越复杂。越来越多的人依赖网络、更多的客户服务机构、未升级和扩展的管理系统以及更多应用程序 。由于信息资源基础设施之间的互相依赖程度越来越高，因此有必要加强变更管理过程。 有时每一个信息资源组成部分需要暂停运行，按计划进行升级、维护或调整，另外也可能由于为计划的升级、维护或调整而导致暂停运行。管理这些变更是提供坚固的、有价值的信息资源基础设施的关键组成部分。
目 的	该策略的目的是以一种合理的、可预知的方式管理变更，以便员工和客户能进行相应的计划。变更需要事先严格计划、仔细监控并要进行追踪评价，以降低对用户群的负面影响，增加信息资源的价值。
适用范围	该策略适用于安装、操作或维护信息资源的所有人员。
术语定义	略
变更管理安全策略	■ 对信息资源的每一次变更，如操作系统、计算机硬件、网络以及应用程序都要服从变更管理策略，并且必须遵守变更管理程序； ■ 所有影响计算机环境设备的变更(如空调、水、热、管道、电)需要向变更管理过程的领导者报告，并与之协调处理； ■ 无论是事先有计划的变更还是事先无计划的变更必须都提交书面的变更申请； ■ 所有事先有计划的变更申请必须按照变更管理程序的规定提交，以便综合事务部有足够的时间评审申请，确定并重新评审潜在的失败，并决定申请被批准还是延期执行； ■ 每一个事先计划的变更申请在执行前必须受到综合事务部的正式批准； ■ 指定的综合事务部领导在下列情况下有权拒绝任何申请：不充分的策划、不充分的删除计划、变更的时间等会对关键的业务过程造成负面影响，或者会造成没有充分的资源可用； ■ 在变更管理程序实施前，必须完成对所有客户的通知； ■ 每一次变更必须进行变更评审，无论是计划还是未计划的，成功的还是失败的；

	■ 所有变更必须保留变更管理日志，必须保留的日志包括但不限于下列内容： ✧ 变更的提交和执行日期； ✧ 所有者和保管者信息； ✧ 变更的特性； ✧ 成功或失败的标志。 ■ 所有信息系统必须遵照上述规定进行信息资源的变更。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
病毒防范策略	
介绍	计算机安全事故的数量以及由业务中断服务恢复所导致的费用日益攀升。实施稳固的安全策略，防止对网络和计算机不必要的访问，较早的发现并减轻安全事故可以有效地降低风险以及安全事故造成的费用。
目 的	该策略的目的是描述计算机病毒、蠕虫以及特洛伊木马防御、检测以及清除的要求。
适用范围	该策略适用于使用信息资源的所有人员。
术语定义	略
病毒防范策略	■ 所有连接到局域网的工作站必须使用研发运营部批准的病毒保护软件和配置； ■ 病毒保护软件必须不能被禁用或被绕过； ■ 病毒保护软件的更改不能降低软件的有效性； ■ 不能为了降低病毒保护软件的自动更新频率而对其进行更改； ■ 与局域网连接的每一个文件服务器必须使用研发运营部批准的病毒保护软件，并要进行设置检测、清除可能感染共享文件的病毒； ■ 由病毒保护软件不能自动清除并引起安全事故的病毒，必须向研发运营部报告。

惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
可移动代码防范策略	
介绍	未经授权的移动代码危害信息系统，应实施对恶意代码的监测、预防和恢复控制，以及适当的用户意识培训。
目 的	该策略的目的阻止和发现未经授权的移动代码的引入，实施对恶意代码的监测、预防和恢复控制。
适用范围	该策略适用于使用信息资源的所有人员。
可移动代码防范策略	■ 禁止使用未经授权的软件。 ■ 防范经过外部网络或任何其它媒介引入文件和软件相关的风险，并采取适当的预防措施。 ■ 定期对支持关键业务过程的系统中的软件和数据进行评审；无论出现任何未经验收的文件或者未经授权的修改，都要进行正式调查。 ■ 安装并定期升级防病毒的检测软件和修复软件，定期扫描计算机和存储介质，检测应包括： ✧ 在使用前，对存储媒体，以及通过网络接收的文档进行恶意代码检测； ✧ 在使用前，通过邮件服务器对电子邮件附件及下载文件进行恶意代码检测； ■ 研发运营部负责恶意代码防护、使用培训、病毒袭击和恢复报告。 ■ 为从恶意代码攻击中恢复，需要制定适当的业务持续性计划。包括所有必要的数据、软件备份以及恢复安排。 ■ 研发运营部应制定并实施文件化的程序，验证所有与恶意软件相关的信息并且确保警报公告的内容准确详实。管理员应当确保使用合格的信息资源，防止引入真正的恶意代码。所有用户应有防欺骗的意识，并知道收到欺骗信息时如何处置。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾

	问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
信息备份安全策略	
介绍	电子备份是一项必需的业务要求，能使数据和应用程序在发生意想不到的事件时得以恢复，这些事件包括：自然灾害、系统磁盘故障、间谍活动、数据输入错误或系统操作错误等。
目 的	该策略的目的是设置电子信息的备份和存储职责。
适用范围	该策略适用于组织中负责信息资源安装和支持的所有人员，以及负责信息资源安全的人员和数据所有者。
术语定义	略
信息备份安全策略	■ 信息备份周期和方式必须依据信息的重要性以及数据所有者确定的可接受风险确定； ■ 供应商提供的场所外备份存储必须达到信息存储的最高等级； ■ 场所外备份存储区的物理访问控制的实施必须满足并超过原系统的物理访问控制，另外备份介质必须依据信息存储的最高安全等级进行保护 ； ■ 必须建立并实施对电子信息备份成功与否的验证过程； ■ 必须对场所外备份存储供应商每年进行评审； ■ 为了容易识别介质和 / 或关联系统，备份介质至少应该被标注下列信息： ✧ 系统名； ✧ 创建日期； ✧ 敏感度分级［以相应的电子记录保持法规为基础］； ✧ 包含的信息。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略

技术脆弱性管理策略	
介绍	为防止技术脆弱性被利用，应建立对应技术脆弱性的管理机制，主动补充脆弱性，增加信息安全控制。
目 的	该策略的目的是及时得到现用信息系统技术脆弱性的信息，评价公司对这些脆弱性的暴露程度，并采取适当的措施来处理相关的风险。
适用范围	该策略适用于访问信息资源的所有人。
网络配置安全策略	■ 研发运营部要定义和建立与技术脆弱性管理相关人员，负责脆弱性监视、脆弱性风险评估、打补丁、资产追踪和任意需要的协调责任； ■ 技术脆弱性负责人要制定时间表对潜在的技术脆弱性的通知做出反映； ■ 一旦潜在的技术脆弱性被确定，技术脆弱性负责人要识别相关的风险并采取措施；这些措施可能包括对脆弱的系统打补丁和/或应用其他控制措施； ■ 技术脆弱性负责人应定技术脆弱性需要解决的紧急程度； ■ 如果有可用的补丁，则要评估与安装该补丁相关的风险（脆弱性引起的风险要与安装补丁带来的风险进行比较）； ■ 在安装补丁之前，要进行测试与评价，以确保它们是有效的，且不会导致不能容忍的负面影响；如果没有可用的补丁，要考虑其他控制措施，例如： 1） 关闭与脆弱性有关的服务和功能； 2） 调整或增加访问控制措施，例如在网络边界上添加防火墙（见 13.1）； 3） 增加监视以检测实际的攻击； 4） 提高脆弱性意识； ■ 研发运营部要定期对技术脆弱性管理过程进行监视和评价，以确保其有效性和效率； ■ 处于高风险中的系统要首先解决；
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。

HXYD/SC-0304-2021 信息交换策略	
介绍	在组织之间交换信息和软件应当遵守根据交换协议所制定的正式的交换方针，并且应当服从所有相关的法律。
目 的	保持在组织内部及任何外部机构之间所交换的信息和软件的安全。
适用范围	该策略适用于进行信息交换的所有人员。
术语定义	略
信息交换策略	■ 不能在公共场所或者敞开的办公室、没有屋顶防护的会议室谈论机密信息。 ■ 对信息交流应作适当的防范，如不要暴露敏感信息，避免被通过电话偷听或截取。 ■ 员工、合作方以及任何其他用户不得损害本局的利益，如诽谤、骚扰、假冒、未经授权的采购等。 ■ 不得将包含敏感信息的讯息放在自动应答系统中。 ■ 不得将敏感或关键信息放在打印设施上，如复印机、打印机和传真，防止未经授权人员的访问。 ■ 做应用系统之间接口、协议时，不能影响双方应用的正常运行；在实施之前应充分考虑应用系统的资源是否足够；保证数据交换的权限最小化。 ■ 在进行与相关方信息交换时，需提前指定双方的信息交换人员、交换方式、交换保密方法，以防止信息的泄露。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
运输中物理介质安全策略	
介绍	物理介质是信息资源的载体，在运送过程中必须对其安全进行管理。建立该方针是为了确保包含信息的介质在组织的物理边界以外运送时，防止未授权的访问、不当的使用或毁坏。
目 的	略

适用范围	该方针适用于在组织安全边界外运输组织物理介质的所有人员。
术语定义	略
运输中物理介质安全策略	应考虑下列方针以保护不同地点间传输的信息介质： ➢ 应使用可靠的运输单位或人； ➢ 授权的送信人列表应经管理者批准； ➢ 包装要足以保护信息免遭在运输期间可能出现的任何物理损坏，并且符合制造商的规范（例如软件），例如防止可能减少介质恢复效力的任何环境因素，例如暴露于过热、潮湿或电磁区域； ➢ 若需要，应采取专门的控制，以保护敏感信息免遭未授权泄露或修改；例子包括： ✧ 使用可上锁的容器； ✧ 手工交付； ✧ 防篡改的包装（它可以揭示任何想获得访问的企图）； ✧ 在异常情况下，把托运货物分解成多次交付，并且通过不同的路线发送。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
电子邮件策略	
介绍	信息资源是组织的资产，必须对其进行有效地管理，因而建立该策略是为了： ✧ 确保员工知晓在 Email 过程中的操作方法； ✧ 明确 Email 使用过程中的责任。
目 的	为了建立某公司的 Email 使用规则，保证 Email 的合理发送、收取和存储。
适用范围	该策略适用于被批准的、能够通过 Email 发送、收取和存储信息的所有人员。
术语定义	略

电子邮件策略	■ 下列行为是策略所禁止的： ✧ 发送或者转发虚假、黄色、反动信息； ✧ 发送或者转发宣扬个人政治倾向或者宗教信仰； ✧ 发送或者转发发送垃圾信息； ✧ 发送或者转发能够引起连锁发送的恐吓、祝贺等信息； ✧ 发送口令、密钥、信用卡等的敏感信息； ✧ 用个人信息处理设备收发公司内部 Email ； ✧ 用公司外部账号发送、转发、收取公司敏感信息； ✧ 在非授权情况下以公司的名义发表个人意见； ✧ 发送或者转发可能有计算机病毒的信息； ✧ 使用非授权的电子邮件收发软件； ■ 下列行为是策略所要求的： ✧ 每位员工都有一个 Email 账号，账号密码必须符合口令策略的相关规定； ✧ 用 Email 经过外部网络发送机密信息必须经过加密，加密必须符合加密策略的相关规定； ✧ 发送 Email 必须有清楚的主题； ✧ Email 的处理和存储必须符合信息的分类、标识和存储策略的相关规定； ■ 管理授权 ✧ 公司有权对职员的 Email 进行监视和记录； ✧ 公司有权对 Email 的内容进行存储备份以用于法律目的；
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
信息安全监控策略	
介绍	信息安全监控是确保安全实践和控制被恰当执行和有效实施的一种方法，

	监控活动包括对下列内容的评审： ✧ 防火墙日志 ✧ 用户帐户日志 ✧ 网络扫描日志 ✧ 应用程序日志 ✧ 数据备份和恢复日志 ✧ 其他类型的日志以及出错日志
目 的	该策略是为了确保信息资源控制措施被适当、有效地实施并且不被忽视。安全监控的其中一个好处就是较早的发现破坏行为或新的薄弱点。这样会有助于在破坏发生前阻止破坏行为或薄弱点，最起码能够减小潜在的影响。其他好处包括：审核符合性、服务层监控、业绩测量、划定责 任以及容量策划。
适用范围	适用于负责信息资源安全、现有信息资源的操作以及负责信息资源安全的所有人员。
术语定义	略
信息安全监控策略	■ 自动检测工具会对检测到的破坏行为或薄弱点利用进行实时通知。在可能的地方可以开发安全底线和工具，监控： ✧ 电子邮件通信 ✧ 局域网通信、协议以及设备清单 ✧ 操作系统安全参数 ■ 在检查破坏行为以及薄弱点被利用情况时可以使用下列文件： ✧ 防火墙日志 ✧ 用户帐户日志 ✧ 网络扫描日志 ✧ 系统出错日志 ✧ 应用程序日志 ✧ 数据备份和恢复日志 ✧ 网络打印机和传真日志

	■ 下列内容应该由负责的人员每年至少检查一次： ✧ 口令的难猜测程度 ✧ 未经授权的网络设备 ✧ 未经授权的个人网络服务器 ✧ 未受保护的共享设备 ✧ 未经授权使用的调制解调器 ✧ 操作系统和软件许可 ■ 发现的任何问题都应该向综合事务部报告，进行进一步的调查。 ■ IT 管理员自身的工作由管理者代表进行审查和监督。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
特权访问管理策略	
介绍	与普通用户相比，技术支持人员、安全管理员、IT 管理员可能有特殊的访问账户权限要求。这些管理性的特殊访问账户的访问等级比较高 ，因此对这些账户的批准、控制和监控对于整个安全程序极其重要。
目 的	该策略的目的是为具有特殊访问权限的账号建立创建、使用、控制及其删除的规则。
适用范围	该策略适用于拥有、或者可能会需要信息资源特殊访问权限的所有人员。
术语定义	略
特权访问管理策略	■ 所有管理性的/特殊访问账户在获得账号前，应签署一份不泄密协议； ■ 所有管理性的/特殊访问账户的用户必须接受培训并获得授权； ■ 每一个使用管理性的 / 特殊访问账号的个人都必须避免滥用权力，并且必须在综合事务部的指导下使用； ■ 每一个使用管理性的/特殊访问账号的个人必须以最适宜所执行的工作的方式行使账号权力 ； ■ 每一个管理性的/特殊访问账户必须满足口令策略的要求；

	■ 共有的管理性的/特殊访问账号的口令在人员离职或发生变更时必须更改； ■ 当因内外部审核、软件开发、软件安装或其他规定需求而需要特殊访问账号时，账号： ✧ 必须被授权； ✧ 创建的日期期限必须明确； ✧ 工作结束时必须删除。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
口令控制策略	
介绍	用户授权是控制信息资源访问者的一种方式。对访问进行控制是任何信息资源所必须的。未经授权的人员访问到信息资源可能会引起信息保密性、完整性共和可用性的丢失，导致收入、信誉的损失或经济困难。
目 的	该策略的目的是为用户鉴别机制建立创造、分发、保护、终止以及收回的规则。
适用范围	该策略适用于任何信息资源的使用者。
术语定义	略
口令控制策略	■ 所用用户都必须拥有唯一的、专供其个人使用的用户帐号 ID（用户 ID）； ■ 所有用户不得使用他人的用户进行信息资源的访问； ■ **所有口令，包括计算机登录、文件系统、网络等口令，都必须依据综合事务部规定的下列规则建立和执行：** ✧ 必须定期更改（最长 90 天）； ✧ 必须符合技术部规定的最小长度（6 位字符）； ✧ 必须符合复杂度要求，即数字+字母+特殊符号的组合，例如：203aa# ✧ 必须不能是可以轻易联想到的帐号所有者的特性：用户名、绰号、亲属的姓名、生日等；

	✧ 必须不能用字典中的单词或首字母缩写； ✧ 必须保存历史口令，以防止口令的重复使用。 ■ **服务器、应用系统、网络设备的管理员特殊权限用户的口令除以上要求需要满足外，还有特殊要求：更改周期缩短为 30 天，密码长度不少于 8 位。** ■ 用户的帐号口令必须不能泄露给任何人； ■ 如果怀疑口令的安全性，应立即进行更改； ■ 管理员不能为了使用信息资源规避口令； ■ 用户不能通过自动登录的方式绕过口令登录程序； ■ 计算机设备如果无人值守必须启动口令保护屏保或注销； ■ 用户在首次登录时必须更改口令。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
清洁桌面和清屏策略	
介绍	应该实施清除桌面和清除屏幕方针，以降低对文件、介质以及信息处理设施未经授权访问或破坏的风险。
目 的	该策略的目的是防止对信息和信息处理设施未经授权的用户访问、破坏或盗窃。
适用范围	该策略适用于公司所有员工。
术语定义	略
清洁桌面和清屏策略	■ 含有涉密信息或重要信息的文件、记录、磁盘、光盘或以其它形式存贮的媒体在人员离开时，应锁入文件柜、保险柜等； ■ 所有计算机终端必须设立登录口令，在人员离开时应该锁屏、注销或关机； ■ 在结束工作时，必须关闭所有计算机终端，并且将个人桌面上所有记录有敏感信息的介质锁入文件柜； ■ 应清洁电脑屏幕，确保不放置重要信息在电脑桌面上。

	■ 计算机终端应设置屏幕密码保护， 屏保时间 不大于 5 分钟； ■ 传真机由综合事务部负责管理，并落实责任人。 ■ 打印或复印公司机密信息时，打印或复印设备现场应有可靠人员，打印或复印完毕即从设备拿走。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
互联网使用策略	
介绍	在信息资源管理策略的规定中，信息资源是对组织有价值的重要资产。建立该策略是为了达到下列目的： ✧ 确保符合相应的、与信息资源管理相关的法令、规章以及要求； ✧ 建立谨慎的、合理的互联网使用惯例； ✧ 向使用互联网或者企业内部网络的员工告知他们应负的职责。
目 的	该策略的目的是规范互联网以及公司内部网络的使用，确保信息资源不会被泄漏、篡改、破坏。
适用范围	该策略适用于有权访问任何信息资源而又可以访问互联网以及公司内部网络的所有人员。
术语定义	略
互联网使用策略	■ 提供给授权使用者的互联网浏览软件只能用于公司业务； ■ 互联网访问权限只授权给总经理、副总经理、IT 管理员，其他用户需访问互联网必须在公司公共的上网区域访问互联网，且必须遵守相关规定。 ■ 所有用于访问互联网的软件必须都经过综合事务部批准，并且必须结合卖方提供的安全补丁； ■ 从互联网下载的所有文件必须通过综合事务部批准的病毒检测软件进行病毒扫描； ■ 访问的所有站点都必须符合信息资源使用策略； ■ 对用户在信息资产上的所有活动都必须进行记录并评审；

	■ 所有 Web 站点上的内容都必须符合信息资源使用策略； ■ 不能通过 Web 站点访问攻击性的或骚扰性的资料； ■ 私人的商业广告不能通过 Web 站点发布； ■ 互联网不可以用于个人私利； ■ 在不能确保资料只被授权的人员或组织使用时，数据不能通过 Web 站点获取； ■ 通过外部网络传送的所有敏感资料都必须经过加密； ■ 电子文件必须服从适用其文件类型的保存规则，必须依照部门记录保存方案进行保存； ■ 偶尔使用互联网访问的人员必须仅限于授权用户，不能延伸到家庭成员或其他熟人； ■ 偶尔使用必须不造成费用损失； ■ 偶尔使用必须不能干扰员工的正常工作任务； ■ 文档和文件的发送或接受必须以不引起法律责任或阻碍的方式进行； ■ 所有文档和文件——包括私人文档和文件，必须符合记录公开要求，并且可以依照本策略访问到； ■ 使用互联网应遵循法律法规要求，并不得利用国际联网危害国家安全、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。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
便携式计算机安全策略	
介绍	便携式计算机设备的功能和应用越来越广泛。其小巧的“体型”和强大的功能使人们期望其替代传统的桌面设备。然而，这些设备的便携特性也会给使用他们的组织增加安全暴露。
目 的	该策略的目的是建立移动计算机设备的使用规则及其与互联网的连接规则。

	这些规则是保持信息保密性、完整性和可用性所必需的。
适用范围	该策略适用于使用便携式计算机设备访问信息资源的所有人。
术语定义	略
便携式计算机安全策略	■ 只有被批准的便携式计算机设备才能用来访问信息资源； ■ 便携式计算机设备必须有口令保护； ■ 存储在便携式计算机设备中的重要数据应定期备份； ■ 无线传输设备必须设定复杂化密码，SSID 不广播。 ■ 需要连接互联网的计算机系统必须符合信息服务标准； ■ 对无人看守的便携式计算机设备必须实施物理保护，必须放在带锁的办公室、抽屉或文件柜里，或者锁在桌子或柜子上； ■ 非授权便携式计算机禁止在公司办公区域内使用； ■ 非授权便携式计算机禁止加入公司域；
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
事件管理策略	
介绍	计算机安全事件的数量以及由其导致得业务中断和服务恢复所需的费用日益增长。实施可靠的安全策略，防止对网络和计算机不必要的访问，提高用户的安全意识以及及早检测并减轻安全事件，可有效的降低风险以及安全事件的成本。
目 的	该策略的目的是描述处理计算机安全事件的要求。安全事件包括，但不仅限于：病毒、蠕虫、特洛伊码、未经授权使用计算机账号和计算机 系统以及如在电子邮件策略、信息资源使用策略以及互联网策略中规定的对信息资源不恰当的使用。
适用范围	该策略适用于使用任何信息资源的所有人员。
术语定	略

义	
信息资源保密策略	■ 研发运营部的成员此方面任务和职责的优先权要高于其正常的职责； ■ 在怀疑或确定发生安全事件的任何时候都必须遵循适当的事件管理程序，例如病毒、蠕虫、恶作剧邮件等； ■ 研发运营部负责通知信息安全经理，启动适当的事件管理活动，包括事件管理程序中规定的恢复活动； ■ 在事件调查过程中，研发运营部负责确定要搜集的实物和电子证据； ■ 信息技术小组提供的用于监控安全事件破坏的技术资源应该被维修并降低其潜在的薄弱点； ■ 研发运营部与信息安全经理合作确定是否需要对安全事件进行广泛的沟通，沟通的内容以及怎样最好的将沟通的内容共享； ■ 研发运营部应提供响应的技术资源，用于和系统卖方沟通新问题或薄弱点，并与卖方共同消除或减轻薄弱点； ■ 研发运营部在综合事务部的协助下，负责启动、完成并文件化事件调查过程； ■ 研发运营部负责向下列部门或人员报告： ✧ 信息资源相关部门 ✧ 在有关事件响应的法律、法规和 / 或规章中要求的地方、省、国家有关部门 ■ 综合事务部负责与外部组织以及法规强制部门的协调沟通； ■ 在不牵涉到法律强制的地方，综合事务部可以向信息安全经理建议惩戒措施； ■ 在牵涉到法律强制的地方，综合事务部负责与法律强制部门的联络。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
HXYD/SC-0305-2021 个人信息使用策略	
介绍	对个人信息的隐私加以保护。

目 的	该策略的目的是保护个人信息的隐私，符合相关的法律、法规和合同条款的要求。
适用范围	该策略适用于使用和保存个人信息的人员。
术语定义	略
个人信息使用策略	■ 只对业务上必需的最小限度的信息采取合法且公正的方法进行收集，原则上，在向信息所有者说明使用目的并征得同意后再行收集。 ■ 严禁用于收集目的以外的用途。 ■ 个人信息的所有者要求对自己的个人信息进行明示、修改、删除和停止使用时，在进行严格的本人确认后，应尽快予以施行。 ■ 当将与个人信息有关的事宜对外委托处理时，要求施行与在本公司内同等程度的管理。 ■ 当接受外部委托进行有关个人信息的处理时，要遵守委托方的个人信息管理准则。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
业务信息系统使用策略	
介绍	业务信息系统主要是与我公司业务相关的使用软件系统。
目 的	该策略的目的是为了规范化我们对业务系统的操作，从而降低由此引起的公司财产的损失。
适用范围	该策略适用于所有业务信息系统操作相关的人员。
术语定义	略
业务信息系统使用	■ 加强保护业务信息系统免受网络安全风险的干扰。 ■ 公司业务信息系统的使用人员应该有熟练的操作技巧，对于不熟悉的人员应该尽量避免使用。 ■ 对于不熟悉的人员如果需要使用业务信息系统时，需要进行使用前的培

策略	训。 ■ 对于需要使用业务信息系统的人员需要提出申请，并且通过综合事务部认可后才可以允许使用。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
远程工作策略	
介绍	远程工作是使用通信技术手段使在组织场所外固定地点的人员可以进行远程进入公司网络工作。
目 的	该策略的目的是确保远程工作及设施的信息安全。
适用范围	该策略适用于通过远程工作方式访问任何信息资源的所有人。
术语定义	略
远程工作策略	■ 远程工作的方式必须获得综合事务部的批准，并获得综合事务部的授权，任何部门和个人不得私设可以远程访问的接口； ■ 远程工作应仅限于申请的设备和地点，严禁在公共计算机设备（例如网吧）上进行； ■ 远程工作人员范围仅限于工作需要的人员，内部远程工作人员必须获得部门负责人的书面授权，并获得综合事务部的批准； ■ 远程工作人员不得将远程工作身份识别信息和相关设备透露、借用给其他人员，工作结束后应该立即注销并断开远程连接； ■ 远程工作的相关通信和设备必须接受综合事务部的相关配置和监控； ■ 远程工作的访问权限不允许超过该人员在公司内部网络的正常访问权限，并符合《用户访问控制程序》； ■ 外部供应商需要连接本公司网络进行系统维护或故障诊断应该签订《保密协议》，明确对方的保密责任和相关安全要求；远程访问时要做好记录，维护结束后立即断开连接。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问

	的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
安全开发策略	
介绍	建立软件和系统开发规则，并应用于组织内的开发
目 的	该策略的目的是宜确保进行信息安全设计，并确保其在信息系统开发生命周期中实施。
适用范围	该策略适用于开发管理系统、应用系统过程中，同时开发也可能发生在应用中，例如办公应用、脚本、浏览器和数据库等。
术语定义	略
远程工作策略	■ 保证开发环境的安全，做到开发环境、测试环境、运营环境想隔离，权限单独控制； ■ 制定软件开发周期的安全指南，包括软件开发方法的安全、开发程序的安全编码指南； ■ 收集并编写系统的安全需求； ■ 在软件的里程碑设置时考虑安全的检查点； ■ 建立安全知识库，记录意外开发中遇到的安全问题解决经验； ■ 对开发者就系统开发技术的脆弱性应进行培训，已应对开发过程中遇到是的处理，对培训情况需进行验证。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略
加密控制策略	
介绍	通过密码方法保护信息的保密性、真实性或完整性是一种有效的技术手段。
目的	该策略的目的是使利用密码技术的风险最小化，以及避免不合适或不正确的使用。

适用范围	该策略适用于数据加密的控制，以及进行和使用数据加密技术的人员。
内容	● 根据风险评估的结果，对重要的信息和数据进行加密； ● 通过 VPN 通道进行远程访问，采用 IPSEC 技术进行加密； ● 对于通过拨号设备进行的远程访问，需要进行系统的监控，可不作数据加密处理； ● 对内部网数据通道，作关键点的监控，可不作数据加密处理； ● 对处理重要信息的网段和计算机，采用软件进行数据加密，加密应采用 128 位密钥的 RC4 加密算法。 ● 对离线的计算机,采用软件进行数据加密,加密应采用 128 位密钥的 RC4 加密算法，通过 USB KEY，设置密码，实现离线功能； ● 加密网段的计算机按最大化选择保护模块，设置禁止打印操作，设置禁止截屏操作，开启“允许终端自行加密”功能，凡进入计算机的数据文档均自动加密；关闭“允许终端自行加密”功能，需解密的数据文档由管理员进行。 ● 信息安全员负责加密系统密钥的保管，并建立程序对密钥保护和由于密钥丢失或损毁对加密信息的恢复性控制； ● 数据加密只能使用经国家密码管理部门认可的商用密钥产品，不得使用自行研制的或者境外生产的密码产品。 ● 任何人不得非法攻击密码，不得利用密码危害国家的安全和利益、危害社会治安或者进行其他违法犯罪活动的要求。
惩罚	违背该策略可能导致：员工以及临时工被警告、惩处、解雇、合同方或顾问的雇佣关系终止、实习人员失去继续工作的机会；另外， 这些人员还有可能遭到法律起诉。
引用标准	略