**信息安全管理规划设计咨询服务**

**技术需求书**

## 1. 项目背景

为认真贯彻国家颁布的《网络安全法》、《数据安全法》等法律法规，全面落实国家网络安全方面的重点要点，国家癌症中心/中国医学科学院肿瘤医院拟采购信息安全管理规划设计咨询服务，确保网络安全、数据安全的常态化管理，切实维护重点项目的安全、稳定和高效运行。

## 2.项目服务原则

**（一）安全保密原则**。投标人在提供安全服务的过程中，要严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，服务过程中凡是涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

**（二）最小影响原则**。投标人开展的安全服务工作，要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如不可抗力无法避免，应对风险进行说明。

**（三）规范性原则**。投标人开展的安全服务工作，要由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

**（四）可控性原则**。投标人在开展安全服务工作过程中采用的工具、方法和过程要在双方认可的范围之内，保证用户对于服务过程的可控性。

**（五）质量保障原则**。投标人开展的安全服务工作需特别重视项目质量管理，项目的实施需严格按照项目实施方案和流程进行，并由项目协调小组从中监督、控制项目的进度和质量。

## 3.采购内容和交付成果

### 3.1 采购需求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 需求方案 | 具体技术需求 | 实施方案 |
| 1 | 网络安全体系规划设计咨询 | 依据业界通用安全架构方法论，紧密结合监管方向和客户业务场景，同时考虑数字化转型中新型技术的安全风险，设计出全面完整、整体协同的网络安全架构体系。**咨询内容包括：网络安全治理、网络安全组织、网络安全制度流程、网络安全技术保护体系设计、网络安全运营及网络安全监管等，实现体系化网络安全保障能力。**并分析项目的依赖关系，结合客户实际需求制定网络安全实施路线图。同时依据客户需求，针对云安全、开发安全、安全运营等制定专题规划方案。 | 网络安全体系架构规划建设：对网络安全建设、安全开发建设、应用系统安全建设、资产脆弱性与安全运营等方面进行调研与规划。具体包括以下方面：1.网络安全建设：从网络安全分区分域建设情况、办公内外网隔离情况、区域间安全装置部署情况、区域间安全防护策略情况进行调研，输出安全建设规划；2.云安全规范建设：针对公有云场景与私有云安全建设，对安全管理规范以及安全技术基线等进行调研与风险发现；3.安全开发建设：安全开发流程建设、安全编码规范建设、应用系统上线发布规范、应用间访问关系梳理规范等；4.应用系统安全：身份鉴别机制建设、应用系统间访问控制、系统间账号管理与审计、移动业务安全等方面明确安全标准与制度规范；5.资产与安全运营建设：对外开放资产及相关安全管理要求，供应链关系梳理与安全风险管理，内部南北向、东西向流量监测与加密流量监测及风险发现能力建设；6.安全运维管理：无线安全运维、主机终端运维规范、配置变更等运维流程规范等评审与差距分析。完成以上方面的安全评审与差距分析，针对安全体系方面存在的问题以及安全团队关注的重点安全建设领域提供决策依据，制定专项规划方案。 |
| 2 | 数据安全治理体系规划咨询 | 根据客户的数据治理状况及数据安全管控现状，访谈客户数据使用过程中涉及的相关部门、业务系统、操作人员，调研敏感数据收集、存储、传输、使用和销毁全生命周期，评估敏感数据在技术、流程、管理、人员等各方面存在的数据安全风险。制定数据分级的安全管控策略等。 | 以“合法合规、审计溯源，权责明晰、最小授权，动态防御、环境可信”为基本原则，指导数据安全保障工作有序开展。具体规划内容如下：1.数据全生命周期安全管理要求调研，已国家标准为基础依据，结合主管部门/监管部门发文及要求进行调整，输出可落地的规划调研纲要；2.针对数据处理活动开展风险监测，针对数据处理内容开展数据风险评估，针对流程制度体系等内容开展符合性分析，分析机构在数据安全治理与保护过程中存在的缺陷和不足，对数据安全风险、数据保护策略实施情况、数据安全保护能力等进行综合分析，得出数据全生命周期安全管理差分结论；3.数据安全保护技术体系设计：该阶段完成风险核查阶段技术能力设计（包括漏洞扫描、弱口令检测、极限配置等内容）、数据梳理技术能力设计（统一身份梳理认证、数据资产与敏感数据发现、数据资产分类分级与权限设计扥内容）、数据保护阶段技术能力设计（数据脱敏、数据库水印与溯源技术、API安全、统一身份认证与数据防泄漏技术等）以及监测预警阶段技术能力设计（流量分析、异常行为监控、安全审计与风险控制等）；4.明确数据全生命周期安全管理情况及数据安全技术保护体系缺陷，确定数据安全提升举措，设计数据安全技术规划路线，整合成数据安全治理体系规划设计方案。 |

### 3.2交付成果

* 结合当前信息安全建设现状，通过审计发现、风险分析等手段,查缺补漏并提出优化建议，形成一套契合法律法规要求、符合委托方管理要求的整体信息安全解决方案（制度、流程、资源、工具）。
* 围绕重要数据的管理和应用，从数据采集、传输、存储、处理、交换、销毁的全生命周期出发，建立一套切实可行的数据治理体系（制度、流程、资源、工具）。
* 条件允许的情况下，协助委托方完成信息安全管理体系认证，包括申请、初审、监督审核、再认证审核等工作。（\*此项非必须内容）

## 4.项目实施服务需求

投标人需根据项目的采购、技术规格要求，采用满足要求的服务进行投标，服务必须满足项目采购主要技术规格要求，并保证能对选用服务进行很好的实施，如遇所选服务不能满足项目建设要求或项目中存在缺漏项情况，投标人应承担相应损失，投标总报价不做调整。

投标人需要派遣专业的实施团队，要求经验丰富、高级资质齐全，保证整体项目实施的完整性、安全性、可靠性，保质保量的按时完成。

## 5.资质要求

1）投标人须在《全国网络安全等级测评与检测评估机构目录》中;

2）投标人须在《商用密码应用安全性评估试点机构目录》中;

3）投标人需具有由中国网络安全审查技术与认证中心（CCRC）颁发的信息安全风险评估服务（一级）资质；

4) 投标人近三年内在招标领域内不存在行政或刑事违法、违规行为及不良行为记录。

5) 本项目不接受联合体投标。