**附件**

**2025年度福建省水利数据安全服务项目内容及要求**

一、项目概况

为推进水利数据资产梳理、加强水利行业重要数据安全防护、提升数据安全保障能力，开展2025年度福建省水利数据安全服务工作。

二、项目服务内容及要求

# （一）安全服务范围要求

本次数据安全服务的范围是福建省水利厅本级及厅属单位相关业务系统，业务系统部署在省政务云的政务外网上，业务系统数量不超过20个。

# （二）安全服务时间要求

**自合同签订起一年。**

# 安全服务内容概述

| **序号** | **工作项目** | **数量** |
| --- | --- | --- |
| 1 | **数据资产梳理服务：**持续开展业务数据资产扫描、业务数据资产梳理、业务数据资产血缘关系分析、敏感数据梳理等分析服务，通过对系统发现、识别、梳理，构建完整的数据资产底账，通过自动识别及人工手段敏感数据在系统内的分布，形成敏感数据清单。开展API接口梳理工作，形成API资产清单，根据业务类型、脆弱性、数据流转情况对API接口进行分类管理。 | 1项 |
| 2 | **数据安全风险评估服务：**结合网信等部门要求，开展至少一次全行业数据安全风险评估工作，工作内容包括但不限于：  1、数据安全信息调研：1）数据处理者调研；2）业务和信息系统情况调研；3）数据资产调研；4）数据处理活动调研；5）安全防护措施调研。  2、风险识别：1）已开展测评情况分析；2）数据安全管理风险识别；3）数据处理活动风险识别；4）数据安全技术风险识别；5）个人信息处理风险识别。  3、风险评价 | 1项 |
| 3 | **数据安全日常运营服务：**   1. 依据数据安全应急处置预案开展至少一次数据安全应急演练； 2. 制定数据安全检查方案，开展日常数据安全自查工作； 3. 日常数据安全风险监测、预警、分析与处置， 4. 补充完善数据安全管理制度体系。 | 1项 |
| 4 | **数据库流量与API流量监控服务：**  基于数据库流量及API流量的数据流转监控，通过流量分析还原、深度检测、敏感数据识别等技术手段，深度分析核心业务系统敏感数据流转、业务接口调用、账号访问等行为。监测敏感数据使用风险、应用资产脆弱性、用户异常访问行为，提供风险告警、数据泄露溯源等能力。 | 1项 |
| 5 | **数据库安全运维管理服务：** 集中管理数据库运维行为，提供SQL审批、数据静态脱敏、数据动态脱敏、数据运维操作审批审计等能力，降低数据越权访问、数据泄漏、数据误删除等数据安全风险。 | 1项 |

# （四）安全服务内容要求

**1.数据资产梳理服务**

每年按省水利厅要求，开展至少4次全盘数据资产梳理工作，梳理我厅业务系统重要数据资产目录，通过对系统发现、识别、梳理，构建完整的数据资产底账，借助敏感数据分析模型，自动识别敏感数据在系统内的分布，分析数据库暗资产、脆弱性等方面，评估数据资产在各应用场景面临的威胁及威胁利用脆弱性导致安全事件的可能性，形成《福建省水利厅XXX系统数据资产清单》、《福建省水利厅XXX系统重要数据目录》、《福建省水利厅XXX系统个人信息目录》等。每次资产梳理工作应在任务起一周内完成。依托自动化监控工具发现数据资产变更也应及时更新。

每年开展至少4次全盘API接口梳理工作，通过分析网络流量，从业务类型、脆弱性、数据流转等维度对API接口进行识别及分类，形成《福建省水利厅XXX系统API接口清单》并实现API接口的分类管理。每次资产梳理工作应在一周内完成。依托自动化监控工具发现API资产变更也应及时更新。

**2.数据安全风险评估服务**

依据《中华人民共和国数据安全法》《网络数据安全管理条例》等相关法律法规和条例的具体规定，按照GB/T 45577-2025《数据安全技术 数据安全风险评估方法》，结合网信等部门要求，对我厅业务系统开展至少一次数据安全风险评估工作，评估手段应包括但不限于人员访谈、文档查阅、安全核查、工具测试等方式。工作内容包括但不限于：

**（1）数据安全信息调研**

数据处理者调研：调研收集我厅网络和信息系统的基本情况，包括但不限于业务系统的拓扑结构等信息。

业务和信息系统情况调研：针对业务系统开展基础情况调研，包括网络运行环境、业务基本情况、运营部门、服务对象、数据类别等。

数据资产调研：梳理结构化数据资产（如数据库表等）和非结构化数据资产（如图表文件等），输出《XXX系统数据资产清单》。

数据处理活动调研：梳理业务系统的数据处理活动清单，绘制《XXX系统数据流图》，数据流图包含数据流转各环节（收集、存储、传输、提供、公开、删除、出境等）经过的相关方、信息系统，以及每个流动环节涉及的数据类型等。

安全防护措施调研；针对现有安全措施进行调研验证，包括制度管理体系、技术防护措施有效性、近年发生的网络及数据安全事件情况等。

**（2）风险识别**

已开展测评情况分析：针对业务系统网络安全等级保护测评工作开展情况，遗留风险情况进行分析评估。

数据安全管理风险识别：从数据安全管理制度、安全组织机构、分类分级管理、合作外包管理、安全威胁和应急管理、开发运维管理、云数据安全等方面进行风险识别。

数据处理活动风险识别：需要从数据全生命周期各阶段的处理活动进行风险识别，涉及的数据全生命周期的阶段包括：数据采集、数据存储、数据传输、数据使用和加工、数据提供、数据公开、数据删除等。

数据安全技术风险识别：从网络安全防护、身份鉴别与访问控制、检测预警、数据脱敏、数据防泄漏、数据接口安全、数据备份与恢复、安全审计等方面进行数据安全技术风险。

个人信息处理风险识别：从个人信息处理基本原则、个人信息告知同意、个人信息处理、敏感个人信息处理、个人信息主体权利、个人信息安全义务、个人信息投诉举报等方面识别个人信息保护风险。

**（3）风险评价**

结合数据资产和数据处理活动清单，梳理存在的风险隐患，对可能存在的数据安全风险发生后的影响分析、风险发生可能性分析、风险评价，最终输出《XXX系统数据安全风险评估报告》。

**3.数据安全运营服务**

（1）数据安全应急演练

优化完善我厅现有数据安全应急处置预案，根据处置预案每年至少开展一次数据安全应急演练工作，通过应急演练进一步优化应急处置流程，输出《福建省水利厅数据安全应急演练报告》。

（2）数据安全自查

依据数据安全相关法规条例，从数据全生命周期维度制定数据安全自查项，覆盖数据安全风险管理、数据处理活动（包括但不限于安全管理及技术保障）两方面，每年至少开展两次数据安全自查工作，输出《福建省水利厅数据安全自查报告》。

（3）数据安全风险监测分析

服务期内须持续开展数据安全风险监测分析，分析本周期内我厅重要系统的网络流量，建立完善数据画像，完成应用资产建模，构建目标区域主要应用数据流转路径测绘。对发现的数据流转风险进行分析处置，根据数据流转风险及目标区域业务特点制定风险监测策略，识别潜在的数据流转风险。

（4）补充完善数据安全管理制度体系

依据《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《网络数据安全管理条例》以及《关键信息基础设施保护条例》等相关法律法规和条例的具体规定，在现有已经建立的数据安全管理制度体系的基础上，进一步进行深入优化和全面完善。具体措施包括但不限于对数据安全管理组织机构的结构进行调整和强化，确保其能够更高效地履行职责；同时，对数据安全管理制度体系进行细致的梳理和补充，确保各项制度不仅符合最新的法律法规要求，还能在实际操作中发挥应有的作用，从而全面提升数据安全管理的整体水平和效能。

**4.数据库流量审计与API流量监控服务**

检测数据库及API流量，发现数据库及API风险，及时进行预警处理。须配备系统平台以提供相关监控、预警等服务。每季度输出《数据库流量审计风险跟踪情况表》及《API流量监控风险跟踪情况表》。**数据库流量监控与API流量监控服务配套工具须支持当前云环境以及国产化环境部署，数据库流量监控须支持对国产数据库流量监控。**

（1）数据库流量审计

数据资源画像。通过流量解析对数据资源进行全面测绘形成数据资源画像，内容包括但不限于资源的基础信息：承载环境，部署IP，数据类型、账号数量等；资源的涉敏访问情况，包括日均流入/流出数据量、访问IP数、待处置风险等；资源的安全指标、风险趋势、风险治理/分布、风险主体TOP、接口分布、访问位置分布等内容。分析数据被什么用户使用，通过什么方式使用数据，使用了什么数据等，构建数据流转全景图。

风险检测及预警。通过数据库流量，捕捉操作细节（如执行时间、用户身份和SQL语句），形成审计日志，用于事后追溯和问题定位‌；检测高危操作（如非法删库、越权操作或权限变更）、异常数据传输（如大流量泄露）、数据涉敏以及性能瓶颈分析等，‌并提供实时预警提醒能力（邮件、短信通知等渠道）。

（2）API流量监控

API接口画像。在API资产梳理基础上，结合流量解析对API接口进行全面测绘形成API接口画像，内容包括但不限于接口的基础信息，包括所属应用，承载环境，数据格式，请求/响应数据类型等；接口的涉敏访问情况，包括日均流入/流出数据量、日均访问次数、待处置风险等；接口的安全指标、风险趋势、风险治理分布、数据流动趋势、访问位置分布等内容。分析并记录API接口调用过程，包括数据被什么用户使用，通过什么方式使用数据，使用了什么数据等，构建数据流转全景图。

风险检测及预警。通过流量分析，识别高频调用、异常IP访问、越权操作或注入攻击、异常数据传输等数据安全等风险‌；追踪API调用全链路，记录请求参数、响应结果、用户身份及数据流向，生成可追溯日志；识别API调用过程中重要数据、个人信息使用是否合规，实现API资产与敏感数据的自动关联‌；‌并提供实时预警提醒能力（邮件、短信通知等渠道）。

**5.数据库安全运维管理服务**

为保障业务数据安全，提高数据库运维质量，采购数据库安全运维管理服务。服务商须提供统一数据库访问入口、统一数据库用户身份认证、统一数据库权限管控、统一数据库监控审计，并且提供高危操作告警与拦截等能力，规避数据越权访问、数据泄漏、数据误删除等，保障数据库平稳、高效运行；对单位核心业务系统的数据库进行访问控制、权限控制等，集中提供包括身份验证、权限控制、高危操作阻断、访问时间、执行次数、库表权限、DML权限等在内的细粒度数据库访问控制，数据操作审计记录等安全功能。须配备系统平台提供相关监控、预警等服务（邮件、短信通知等渠道）。

**数据库安全运维管理服务配套工具须支持当前云环境以及国产化环境部署,支持国产数据库适配，并支持按采购人要求接入水利厅统一用户平台。**

每季度输出《数据运维管理安全风险跟踪情况表》。

**（6）开始服务时间要求**

**因提供服务需要在云平台部署相应工具，投标人应在中标后一个月内完成实施部署并开始提供完整服务，并通过采购人确认，否则采购人有权终止合同并按投标人违约处理。**

**（7）服务质量要求**

**中标方须提供7\*24 小时及时响应故障。若发生数据安全预警（包括数据库流量、API审计、数据库运维管理、采购方或云平台发现的预警），中标方须在1小时内做出明确响应和安排。问题协调处理完毕后，24 小时内将情况反馈甲方。**

**投标人须在采购人提供的环境部署提供服务必须的设备及软件系统，若无法支撑正常服务（性能不足、系统安全问题等）须及时进行升级直至服务正常。**

# （五）服务人员要求

**为了保障本项目的服务质量及专业性，对项目团队作以下要求：**

1. **项目经理。须同时具备国家注册信息安全专业人员（CISP）证书及项目管理专业人士（PMP）资格认证。**
2. **项目成员。至少有1名团队成员具备信息安全保障人员认证证书（CISAW证书）。**

**以上要求，须提供相关证书复印件和近6个月内任意1个月的社保缴交证明。**

# （六）真实性要求

**针对本项目提供的服务工具、证明材料进行真实确认核查。投标人在中标后3个工作日内需提供人员证书和社保、数据安全服务能力资质证书等材料备采购人核查，如未能满足本项目要求，采购人有权不予以签订合同,** **并追究其虚假应标相关法律责任。**

# （七）保密要求

1.本条所称“保密信息”指：中标人获得的与本项目有关的、不为公众所知悉的、不宜披露给第三方的任何信息，包括但不限于本项目基本情况、本项目招标文件等。前述保密信息可以以数据、代码、文字及记载上述内容的资料、光盘、软件、图书等有形媒介体现，也可通过法律法规认可的其他介质形式体现。

2.中标人应主动采取加密措施（包括但不限于采取与用于保护自身保密信息同等级别的加密措施）对保密信息进行保护，防止不承担同等保密义务的任何第三者知悉及使用。

3.中标人保证该保密信息仅用于与本项目有关的用途，不得利用保密信息进行项目以外的其他用途。

4.中标人保证未经采购人事先书面授权，不将保密信息的原件、复印件以及对保密信息做出的概括性分析、判断、报告、意见等透露给任何第三方;中标人如因过失泄露保密信息，同样要承担违约责任。

5.中标人不得允许(包括但不限于出借、赠与、出租、转让等行为)或协助不承担同等保密义务的任何第三人使用保密信息。中标人一旦发现或应该发现保密信息被不正当使用或未经授权被使用，应该立即采取合理的措施防止进一步的不正当使用，且应该立即通知采购人。

6.中标人只能在出现以下情形时向特定人员披露保密信息：

（1）根据法律、行政法规、部门规章规定必须披露和公告；

（2）向其法律顾问、财务顾问、审计机构或者其他专业机构披露（前提是该方已与中标人签订同等程度的保密协议）；

（3）采购人书面许可披露或公开；

（4）该信息已被采购人认为不再是保密信息，或已在社会上公开。

7.保密信息的保密期限自本项目合同签订之日起永久有效。

8.倘若本项目合同因任何原因而未生效或失去效力的，中标人及其相关人员仍应当遵守本条的保密义务。如果参与本合同确定业务的中标人员工不再继续参与本项目，则中标人应确保立即终止该员工获得采购人保密信息和信息源的途径。

9.中标人若违反本条约定的承诺，将承担违约行为导致的法律责任，并赔偿由于该违约行为给采购人造成的全部损失（包括但不限于采购人为追索损失而支付的诉讼费、公告费、保全费、律师费等）。

# （八）服务考核

## 1.考核方式和周期

采购人在服务期结束后进行项目考核。

## 2.考核内容

采购人在服务期结束后终验前对服务商进行最终考核，并签订考核表，服务考核内容和考评标准内容如下：

工作考核表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 指标名称 | 分值 | 考核内容及标准 | | 评分 | 备注 |
| 1 | 人员考核 | 20 | 1.合同签订后3天内服务团队人员未到位开展工作的扣5分。（满分5分）  2.服务团队稳定性保障不力，服务期内人员未经甲方同意变动的每次扣5分。（满分5分） | |  |  |
| 甲方对服务人员工作情况和工作满意度打分，采购人及厅相关处室、厅属单位每投诉1次扣1分，扣完为止。(满分10分） | |  |
| 2 | 服务工作考核 | 60 | 1.数据资产梳理服务。未能及时完成资产梳理，或资产梳理不清晰、不符合管理要求的，每次扣2分，扣完为止。(满分10分） | |  |
| 2.数据安全风险评估服务。未能在相关部门时间要求内完成数据安全风险评估服务或评估工作不满足相关部门要求的，每项扣2分，扣完为止。(满分10分） | |  |
| 3.数据安全日常运营服务。预警信息未及时响应和处理的扣3分，数据安全重大风险或故障（如重要数据泄露、个人信息泄露等）未及时发现及处理的一次扣5分，扣完为止。(满分20分） | |  |
| 4.数据库流量与API流量监控服务。未能及时发现安全风险或未解决的，一次扣2分，扣完为止。(满分10分） | |  |
| 5.数据库安全运维管理服务。未能及时发现数据库运维风险导致安全事故的，一次扣5分，扣完为止。(满分10分） | |  |
|  | 保密规定 | 20 | 运维期须严格遵守保密规定，未经许可不得泄露任何数据；只能在甲方许可的系统范围内提供服务，不得利用工作之便非法侵入或尝试侵入其他系统。发生此类事件，该项不得分并追究相关责任。(满分20分） | |  |  |
| 合计 | 100 | 100 |  | |  |  |
| 双方项目管理人员意见 | | | | | | |
| 甲方：    日期： | | | | 乙方：  日期： | | |

## 3考核与结算规则

为确保安全服务能达到采购人的业务实际需求，同时保证服务质量。考核与付款规则要求如下：

（1）考核与扣款

考核根据考核表进行，依据考核得分情况在支付尾款时进行扣款结算，如下：

|  |  |
| --- | --- |
| 考核得分 | 结算依据 |
| 100分 | 全额结算，给予表扬 |
| 90-99分 | 全额结算 |
| 80-89分 | 采购人有权从未支付款项中扣除中标价20%款项 |
| 70-79分 | 采购人有权从未支付款项中扣除中标价50%款项 |
| 69分及以下 | 采购人有权终止合同并追究中标人责任 |

# （九）付款方式

1.合同签订后，采购人在收到中标人提供的正规、足额增值税普通发票之日起15工作日内，采购人向中标人支付合同总额的3**0%。**中标人未及时提供发票的，采购人有权延迟付款。

2.中标人须在一个月内完成实施部署并提供一个月完整服务，经采购人确认后,采购人在收到中标人提供的正规、足额增值税普通发票之日起15工作日内，采购人向中标人支付合同总额的2**0%。**中标人未及时提供发票的，采购人有权延迟付款。

3.服务期满，通过考核验收后，采购人在收到中标人提供的正规、足额增值税普通发票之日起15工作日内，采购人向中标人支付剩余服务款项**，**参照考核标准约定，若存在扣款情况的，采购人将直接在应付款中扣除。中标人未及时提供发票的，采购人有权延迟付款。