福海创石化PTA工厂余热发电项目电力监控系统等级保护测评及安全防护评估与整改加固项目技术规范书

发包签核单

一、项目发包说明：

对福海创石化 PTA 厂余热发电项目进行电力监控系统等级保护测评及安全防护评估与整改加固

发包依据：

1、国网漳州供电公司发电工程竣工验收意见：厂站未进行系统定级、备案、等级保护测评和安全评估

2、国网漳州供电公司关于翔鹭石化余热发电公司供汽余热余压回收利用项目接入系统设计评审意见的函第二点第八条根据《信息安全等级保护管理办法》（公通字[2007]43号）规定，翔鹭余热电厂应开列电力监控系统登记保护测评及安全评估费用，等保测评备案

[illegible]安全[illegible]国家能源局关于印发《电力行业信息安全等级保护管理办法》的通知（国能安全[2014]318号）十三条执行，到所在地市级以上公安机关办理备案手续，并将相关证明报送漳州地调备案。

发包内容详见：《余热发电项目进行电力系统等级保护测评及安全防护评估技术规格书》

二、承揽商资质要求：

为满足电力行业和公安部门的要求，投标方或投标产品应[illegible]

公安部及国家能源局认可的电力行业等级保护测评

中心实验

室或是具有此资质证书的授权单位并提供授权承诺

函证明；

② 投标方或授权商应具有连续2年（2018-2019）在国网福建省[redacted]供电公司等类似测评的经验并提供相应的证明；

③ 投标方或授权商应提供专业技术人员的信息安全专业认证证书，机构内部具有等级保护测评资质人员应包含[redacted]名高级测[redacted]

[redacted]

翔鹭石化余热发电厂

电力监控系统等级保护测评及安全防护评估

1 总则

1.1 引言

为了落实公安部、国家能源局关于电力监控系统安全等级保护[illegible]

络安

基本要

委员会

14]317 号）

度和标准要

护评估技术服务项目的

规范中未规定，但在相关

投标方应按规范应满足的条

是出具说明，则招标方认为投标

执行的标准不一致，投标方应按更

而成为本规范的组成部分。本技术规范与其

求》（电监信息[2012]62 号）、《电力监控系统安全防护规定》（国家发展改革

[2014]第 14 号令）、《电力行业网络与信息安全管理办法》（国能安全[20

和《电力行业信息安全等级保护管理办法》（国能安全[2014]318 号）等制

求，进行本次电力监控系统等级保护测评与安全防护评估。

1.2 适用范围

本技术规范适用于电力监控系统等级保护测评及安全防

采购，包括技术服务要求和验收要求。

1.2.1 本技术规范提出的是最低限度的技术要求。凡本技术规

国家标准、电力行业标准或 IEC 标准中有规定的规范条文，

文进行服务供应说明。

1.2.2 如果投标方没有以书面形式对本技术规范的条文

方提供的服务完全符合本技术规范。

1.2.3 本技术规范所建议使用的标准如与投标方所

严格标准的条文执行或按双方商定的标准执行。

1.3 标准和规范

下列文件中的条款通过本规范的引用

- 《GB/T 25058 信息安全技术 网络安全等级保护实施指南》（正在修订）
- 《GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》
- 《GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南》
- 《GB/T 25070-2019 信息安全技术网络安全等级保护设计技术要求》
- 《关于开展电力行业信息系统安全等级保护定级工作的通知》（电监信息〔2007〕34 号）
- 《电力行业信息系统安全等级保护基本要求》（电监信息[2012]62 号）
- 《电力行业网络与信息安全管理办法》（国能安全[2014]317 号）
- 《电力行业信息安全等级保护管理办法》（国能安全[2014]318 号）
- 《电力监控系统安全防护规定》（国家发展改革委员会[2014]年第 14 号令）
- 《电力监控系统安全防护总体方案》国能安全[2015]36 号
- 《发电厂监控系统安全防护方案》国能安全[2015]36 号
- 《电力监控系统安全防护评估规范》国能安全[2015]36 号

1.4 权利和职责

为切实保障本项目的工作质量，确保测评及评估工作达到预期目标，对招标方及项目实施方双方技术工作责任约定如下：

1.4.1 招标方责任

- 负责测评实施过程中同相关单位和部门的协调。
- 为项目实施方提供良好的工作场地和环境。
- 按工作要求提供相关的资料和信息。
- 准备应急措施，负责实施过程中的紧急情况的处理。

1.4.2 项目实施方责任

- 按照招标方工作章程开展工作。
- 项目内容的变更及时与招标方代表沟通。
- 按照协议要求提供技术服务和成果。
- 确保测评及评估工作质量。
- 配合招标方准备应急预案和实施过程中的紧急情况处理。
- 负责按时完成所有工作。

同时，双方都必须遵循保密要求。

项目概况

本项目属翔鹭石化（漳州）有限公司余热电厂，装机容量[illegible]，设置[illegible]座[illegible]升压站，新增[illegible]台[illegible]主变压器，中压的中性点通过变压器升压后接入220kV总降变VII段母线，数据接入国网漳州电力调控中心。

1.5 项目范围

电力监控系统信息安全等级保护测评与安全防护评估范围如下：

（1）完成电力监控系统定级、信息安全防护系统[illegible]

[illegible]

[illegible]威胁评估、脆弱性评估、

[illegible]一步测算后报价，如有[illegible]程款项。

理和安全运维管理等十个方面的安全测评；

电力监控系统安全防护评估的主要内容包括：资产评估、威胁评估、脆弱性评估、现有安全措施有效性评估等。

注：投标方应到工作现场实际核对工程量（数量）及做遗漏、缺项、计算错误均视为投标方优惠报价，不予追加工

2 技术规范

2.1 测评及设计依据原则

本项目实施方案设计与具体实施应满足以下原则：

2.1.1 保密性原则：项目实施方应与招标方签订保密协议，对测评的过程数据和结果

数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据侵害招标方的权益，否则招标方有权追究投标方的责任。

2.1.2 标准性原则：测评及评估方案的设计与实施应依据国家的相关标准进行。

2.1.3 规范性原则：实施方工作中的过程和文档，应具有规范性，便于项目跟踪和控制。

2.1.4 可控性原则：项目的进度应符合进度安排，保证招标方对测评工作的可控

2.1.5 整体性原则：测评及评估的范围和内容应系统、全面、规范，满足等级保安全防护评估的相关基本要求。

2.1.6 最小影响原则：技术测评及评估工作应尽可能小的影响在线系统和网络的运行，不能对现有运行系统造成影响。在线测评及评估应在招标方许可的条件下

安施方案要点收集材料，签署保密协议，组建测评及评估项目组，并进行进场前、

施前的安全教育工作，同时完成检测工具、装备配置等各项准备工作。

2.2.2.2启动阶段

工作周期：1～2 个工作日

工作内容：项目组进驻被测单位，收集分析信息资产资料、网络资料、业务系统

和信息安全管理制度方针等相关测评所需材料，并召开启动会，就测评及评估工

体事宜进行落实，包括确定测评及评估计划安排、测评及评估范围、测评及

和配合需求等。

整改加固：7个工作日

2.2.2.3现场测评

工作周期：4-5 个工作日

工作内容：项目组从管理和技术两个方面入手，开展被测单位测评及评估工

安全区划分、网络专用、评估管理和制度、基础网络、业务系统、通用服

统、数据库系统、现有安全措施等。

测评及评估方法有顾问访谈、日志审计、人工查看、漏洞扫描等。

现场工作结束后，测评及评估工作组对现场测评情况进行初步

测单位领导和系统管理员等汇报现场阶段工作情况。

2.2.2.4结论分析报告编制阶段

工作周期：3～4 周

工作内容：项目组对测评情况和采集的数据进行分类统计、风险

估，撰写被测单位系统《等级保护测评报告》及《电力监控系统

2.2.2.5整改技术支持阶段

工作周期：根据整改进度而定

工作内容：项目组针对现场测评及评估发现的问题，出具整改

供整改技术咨询支持。

2.2.3 风险控制

测评及评估操作必须遵守现场运行规章制度，确保系统安全稳定运行。如需在线测试，按照相关工作规程，事前申请，并在专责人员的指导和监护下进行。

（2）人员与数据管理

重视保密工作，加强测评及评估过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。

（3）测评对象选择

优先选择备用设备（系统）或测试装置进行测评及评估，避免影响在线系统运行。

（4）制定应急预案

根据被测系统情况，在测评及评估实施前制定应急预案，加强系统安全应急管理能力。

（5）关键业务系统风险控制

生产控制大区在线运行系统禁止采用渗透测试工具进行测评。

2.3 进行整改回查

2.4 等级保护测评内容

根据国家等级保护 2.0 相关标准，本次项目的安全等级保护测评应包括安全通用要求内容：

安全通用要求测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等十个方面的安全测评；

2.4.1 安全通用要求

2.4.1.1 安全物理环境

安全通用要求中的安全物理环境部分是针对物理机房提出的安全控制要求，主要对象为物理环境、物理设备和物理设施等，涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

2.4.1.2 安全通信网络

安全通信网络部分是针对通信网络提出的安全控制要求，主要对象为广域网、城域网和局域网等，涉及的安全控制点包括网络架构、通信传输和可信验证。

2.4.1.3 安全区域边界

全区域边界部分是针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等，涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

2.4.1.4 安全计算环境

安全计算环境部分是针对边界内部提出的安全控制要求。主要对象为边界内部的[illegible]和其他设备等，涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护。

2.4.1.5 安全管理中心

安全管理中心部分是针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理。涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

2.4.1.6 安全管理制度

安全管理制度部分是针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。

2.4.1.7 安全管理机构

安全管理机构部分是针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

2.4.1.8 安全管理人员

安全管理人员部分是针对人员管理格式提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

2.4.1.9 安全建设管理

理。

2.5 安全防护评估内容

根据电力监控系统安全评估相关标准，在系统等级保护测评的基础上，增加如下评估项：资产评估、威胁评估、通用应用评估、基础设施安全评估、体系结构安全评估、系统边界安全评估、各类面安策置评估、安全应急响应评估、现有安装措施有效性评估等。

2.5.1 资产评估

资产评估对象包括：网络、主机、安全防护措施、应用系统等。根据安全防护评估有关技术要求，资产评估主要考虑两个方面的内容：一是信息系统中所存储、处理、传输的主要信息，二是信息系统所提供的主要服务。通过对每一类信息和服务等级分析，最终确定信息系统的重要性级别。资产评估具体步骤包括：资产数据整理与核实、资产重要程度分析。其中，资产数据整理与核实是指对测评前单位提供的资产清单进行资产数据的真实性的查证与确认。资产重要程度分析是根据资产提供的服务，判定资产重要程度的过程。

2.5.2 威胁评估

威胁评估是对被评估单位业务系统、网络与信息系统面临的威胁进行分析的过程。威胁评估根据电力监控系统安全防护评估规范，综合威胁源的动机、能力、手段等因素，对威胁源发生威胁事件的频率进行判断。威胁评估是对被评估单位能够提供防灾信息安全等评估的补充内容。通过威胁评估，要达到明确被评估单位信息及这些威胁的等级的目的。

防火、防静电、防雷击、防盗窃、防破坏措施实施评估。

电力监控系统设备及线缆的部署情况，包括情况、通信线缆和电源线的铺设情况，设备电

2.5.5 体系结构安全评估

体系结构评估应重点检查 16 字方针“安全分区、网络专用、横向隔离、纵向认证”的落实情况，重点针对网络边界防护措施、横向隔离、纵向认证等关键防护措施的执行情况、安全接入设备的设置情况、无线网络防护等。

2.5.6 系统本体安全评估

系统本体安全评估是对电力监控系统自身安全防护情况，包括各种软、硬件使用和策略配置等进行评估：

1. 移动存储介质使用情况，包括硬盘、U 盘或其它存储设备；
2. 操作系统、网络设备、应用系统用户口令使用情况；
3. 操作系统、网络设备、应用系统用户权限分配情况；
4. 主机、交换机、路由器等设备、应用系统的安全策略配置及加固情况，尤其是 Windows 系统、非国产网络及安全设备。
5. 终端检测：主要为抽查被评估单位办公终端和生产终端是否有驻留木马、蠕虫、恶意软件，是否存在自定义共享文件夹，系统补丁是否及时更新安装，关键工作文件存放是否恰当等情况，主要通过人工查看和工具检测两种方式来进行。
6. 外设检测：主要检测带有硬盘、内存或其它存储设备和能够操作系统网络打印机、传真机等智能设备。

2.5.7 全面安全管理评估

全面安全管理评估是从管理角度对单位电力监控系统概况进行评估，重点检查安全防护规定落实情况；

制度建立及主管领导、管理机构和工作人员履职情况，信息安全责任制落实情况；

运维人员的安全管控情况；

电力监控系统等级安全防护评估工作开展情况；

信息安全宣传教育、领导干部及各级人员网络与信息安全基础培训、信息安全人员专业技术培训情况等。

2.5.8 安全应急能力评估

安全应急能力评估是对系统的安全有效性、业务的连续性和备用、灾备能力进行评估。

备用与容灾能力的建设情况，包括系统的冗余设备部署情况，设备配置的备份情

况等；

网络与信息安全应急预案的制定、修订情况，包括应急预案是否健全，是否具有针对性和可操作性等；

应急技术支撑队伍建设、应急演练的执行情况；

重大网络安全事件处置情况。

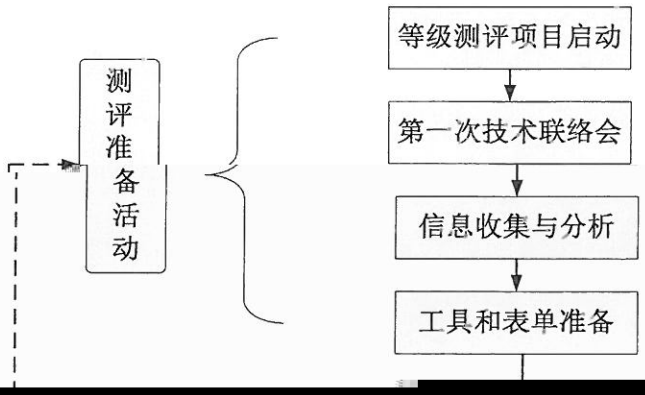
2.5.9 现有安全措施有效性评估

现有安全措施有效性评估是对信息系统中部署的主要安全防护措施进行的审计，以确定这些安全措施的管理和使用情况是否存在重大漏洞和缺陷，明确现有安全措施的有效性程度的活动。现有安全措施的评估主要采用人工检查和访谈的方式进行。主要包括防火墙、防病毒系统、入侵检测防御装置、防病毒网关、单向隔离装置、纵向认证装置等现有安全措施。

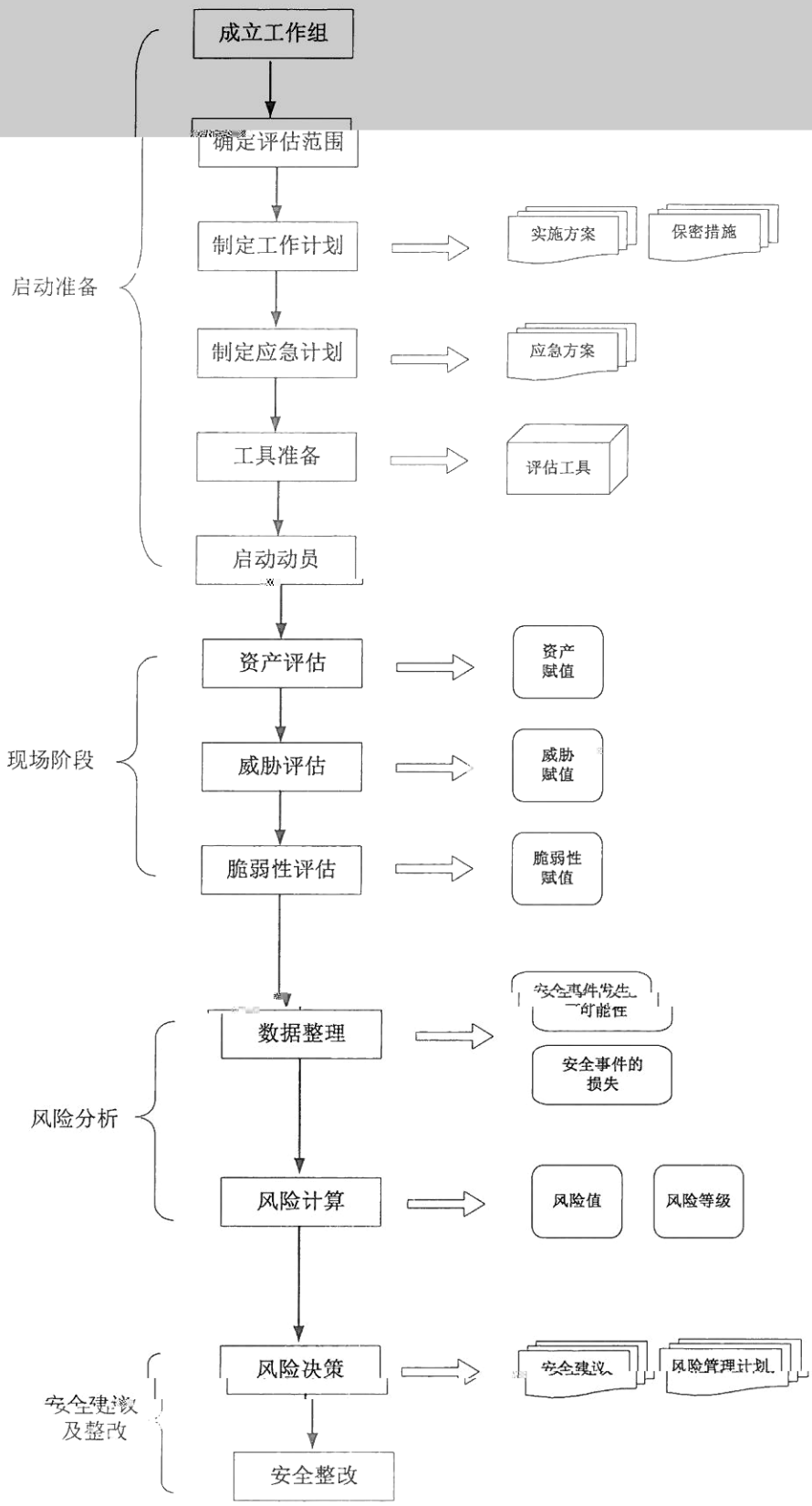
2.5.10 测评及评估流程

根据国家等级保护相关标准，电力监控系统安全等级保护测评流程分为四个阶段：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评完成后，提供整改建议书，配合招标方根据测评范围进行整改实施。

电力监控系统的安全等级保护测评流程如下图所示：


测评准备活动
等级测评项目启动
第一次技术联络会
信息收集与分析
工具和表单准备

范进行，分前期交流和启动准备阶段、现场数据采集和评估阶段、风险计算和分析阶段，以及总结阶段。



3、 项目服务商要求

3.1 服务团队技术要求

投标方应仔细阅读本技术规范书所列的各项规范，所提供的安全服务应满足本技术规范书提出的要求。投标方如可以推荐满足本技术规范的其他方案，但必须对其在技术规范书所描述的差异加以详细说明。若无说明，则按对投标方有利的方面理解。

投标方及投标产品应满足以下要求：

(1) 为满足电力行业和公安部门的要求，投标方或授权商应属于公安部及国家颁发认可的电力行业等级保护测评中心实验室或是具有此资质证书的技术单位并提供授权承诺函证明；

(2) 投标方或授权商应具有连续三年(2018-2020)在国网信息化项目中承担等保测评的经验并提供相应的合同证明；

(3) 投标方或授权商应提供本次项目所涉及安全等级证书的证明，有等级保护测评资质人员应包含 1 名高级测评师和 1 名 CISP 认证测评师；

(4) 投标方或授权商须具有国家信息安全认证中心颁发的《信息安全风险评估服务资质》二级及以上；

(5) 投标方或授权商须具有中国合格评定国家认可委员会颁发的 CNAS 证书。

3.2 驻场服务人员要求

投标方应与招标方签订保密协议，对检测和加固过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据损害招标方的权益，否则招标方有权追究投标方的责任。

投标方在项目实施和控制

重视保密工作，加强测评及评估过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。

（3）测评对象选择

优先选择备用设备下线或测试环境的模拟环境进行测评及评估，避免影响在线系统运行。

（4）制定应急预案

根据被测系统情况，在测评及评估实施前制定应急预案，加强系统在线应急处置能力。

（5）关键业务系统风险控制

生产控制大区在线运行系统禁止采用渗透测试工具进行测评。

4　工程管理

4.1　项目验收

验收应按照招标方确认的验收测试大纲进行，全过程必须由招标方在场见证。

- 等级保护测评及安全防护评估项目启动会后，应出具等级保护测评及安全防护评估报告，该项目收官生一定数量的复审报告。
- 投标方应对所有正式交付件的综合质量负责，指定各交付件的相关人，明确相关职责。
- 投标方应提交验收流程、验收方法和验收依据。
- 投标方应提供交付件归档办法和方式。
- 投标方应提供详细的验收测试大纲或计划，大纲中应明确规定验收须满足的要求。大纲必须经招标方确认后方可生效。
- 验收报告需双方代表签字认可。

4.2　项目文档

4.2.1 投标方提供的资料应使用国际单位制（SI），语言为中文。

4.2.2 资料的组织结构清晰、逻辑性强。资料内容要正确、准确、一致、清晰完整。如所供资料不能达到要求时，投标方应免费给予补充。

4.2.3 投标方资料的出版交货必须在合同规定的日期内。

4.2.4 投标方完成项目后应提供以下文档：

表 3-1　投标方完成项目提供文档列表

序号	文档名称	提交时间	备注
1	《测评方案》	签署合同后1周	电子版
2	《系统自查指南》	签署合同后1周	电子版
3	《系统安全等级保护测评报告》	现场测评后1周	正式版
4	《电力监控系统安全防护评估报告》		

4.3 质量保证

投标方在项目方案设计、实施、验收的各个阶段，均应满足电力监控系统正常稳定运行的要求。

投标方出具的相关报告应得到行业主管单位认定。

4.4 保密要求

投标方承担被测评及评估单位敏感信息的保密责任，在项目实施过程中，双方要妥善保管好提供的各类资料，未经对方书面同意，不得向第三方透露项目和涉及双方企业信息安全、技术等的任何内容。

并将数据内容记录成表，签字确认。

项目结束后，双方必须互相确认测评过程中提供的相关资料，相互归还或销毁。