附件

甲方合同编号：

# 信息系统安全等级测评服务合同

项目名称：榆林职业技术学院网络安全等级测评服务

委 托 方：榆林职业技术学院

受 托 方：陕西慧缘网络科技有限公司

签订时间：2026年 1 月 28 日

签订地点：榆林

有效期限：2年

榆林市网络安全等级保护领导小组办公室印制

# 填表说明

一、本合同为榆林市网络安全等级保护领导小组办公室印制的技术服务合同示范文本，信息系统安全等级保护测评机构及被测单位依照使用。

二、本合同书未尽事项，可由当事人附页另行约定，并作为本合同的组成部分。

三、当事人使用本合同书时约定无需填写的条款，应在该条款处注明“无”字样。

四、测评机构应当在合同签订后10日内向榆林市网络安全等级保护领导小组办公室提交合同原件进行备案。

委托方（甲方）：　　榆林职业技术学院

住所地：　　榆林高新技术产业园区西环路1号

法定代表人：

项目联系人：　　牛文　　白雨

联系方式：　　18091200012　　15109125883

通讯地址：　　榆林职业技术学院信息中心

电话：　　0912-3456108

电子邮箱：　　511050599@qq.com

委托方（乙方）：陕西慧缘网络科技有限公司

住所地：陕西省西安市高新区科技二路软件园示范区秦风阁F301室

法定代表人：蒋卫东

项目联系人：梅巧巧

联系方式：029-88864883 18691868078 15829679119

通讯地址：陕西省西安市高新区科技二路软件园示范区秦风阁F301室

电子邮箱：　　wwg15829259107@163.com

合同甲方委托乙方就榆林职业技术学院网络安全等级测评服务项目进行的专项技术服务，并支付相应的技术服务报酬。双方经过平等协商，在真实、充分表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下协议，并由双方共同恪守。

第一条　双方确定，本合同及相关附件中所涉及的有关名词和技术术语，其定义和解释如下：

1.1**知识产权**：在本合同中，知识产权指任何知识产权，包括但不限于：著作权、集成电路布图设计专有权、任何计算机程序、设计、发明、方法、发现的专利权或非专利技术、商标、商号或其他形式的商业标记等。

1.2**工作成果**：乙方按照本合同第二条约定内容完成，经甲方验收合格并交付给甲方的阶段性工作成果及最终工作成果。

1.3**保密信息**：指接受方因履行本合同而直接或间接的以书面、口头、电子媒介或其他形式从披露方获得的任何非公开信息、资料或数据，这些信息、资料或数据为披露方所有并要求接受方予以保密，包括但不限于技术成果、研究成果、商业计划、客户信息、财务数据、文档模板、业务流程、双方的管理经验、职业个人信息等非公开的信息、资料或数据，但不包括：

1.3.1 任何已出版的或以其它形式处于共有领域的信息，以及在提供该保密信息时接受方通过其它合法途径已获得的信息；

1.3.2 由第三方在不侵犯他人权利及不违反与他人的保密义务的前提下提供给接受方，并且没有附加禁止使用和披露限制的信息；

1.3.3 能够证明是由接受方独立开发的信息；

1.3.4 事先取得披露方书面允许的信息。

第二条　甲方委托乙方进行技术服务的内容如下：

2.1　技术服务目标：完成榆林职业技术学院网络安全等级测评并提交等级测评报告。

2.2　技术服务内容：

| 被测信息系统名称 | 等级 |
| --- | --- |
| 榆林职业技术学院门户网站群管理系统 | 第二级 |
| 榆林职业技术学院教务管理系统 | 第二级 |
| 榆林职业技术学院教学一体化平台系统 | 第二级 |
| 榆林职业技术学院图书馆管理系统 | 第二级 |
| 榆林职业技术学院国资管理系统 | 第二级 |
| 榆林职业技术学院一卡通管理系统 | 第二级 |

其他服务内容：无。

2.3　技术服务依据标准：

2.3.1 国家标准：《信息系统安全等级保护基本要求》GB/T22239-2019

2.3.1 行业标准：无

**第三条** 乙方应该按照下列要求完成技术服务工作：

3.1 技术服务地点：榆林职业技术学院院本部

3.2 技术服务期限：入场测评 三个月（90个日历天）

3.3 技术服务进度：乙方应当按照下列进度要求开展咨询工作并提交相应阶段成果：（具体时间依甲方而定）

第一阶段（测评准备阶段）：2026 年 01 月 29 日至 2026 年 02 月 12 日，进行调研，获取信息系统相关资料；

第二阶段（方案编制阶段）：2026 年 02 月 13 日至 2026 年 03 月 05 日，根据调研情况编制测评方案；

第三阶段（现场测评阶段）：2026 年 03 月 06 日至 2026 年 03 月 20 日，依据测评方案实施现场测评；

第四阶段（分析与报告编制阶段）：2026 年 03 月 21 日至 2026 年 04 月 07 日，根据情况进行分析并编制测评报告；

第五阶段（项目验收阶段）：2026 年 04 月 08 日至 2026 年 04 月 28 日，提交工作成果，准备验收资料，进行项目验收。

**第四条** 为保证乙方有效进行技术服务工作，甲方应当向乙方提供下列工作条件和协作事项。

4.1 提供技术资料；

4.1.1 在测评准备阶段，提供被测信息系统调研所需的系统简介、 设备清单、网络拓扑相关文档等资料；

4.1.2 对测评方案及测评结果进行确认；

4.1.3 网络设备配置文件、相关管理制度；

4.2 提供工作条件：

4.2.1 项目人员入场后，甲方向乙方提供办公场地等工作环境；

4.2.2 网络管理员全程配合。

4.3 其他：无

**第五条** 工作人员安排

5.1 双方确定，在本合同有效期内，甲方指定 白雨 为甲方项目联系人，乙方指定 梅巧巧 为乙方项目联系人。

5.2 乙方应保证其工作人员、专家的稳定性。如果需要更换任何人员，应就调换人员和接替人员事先取得甲方的书面同意， 接替人员的职位、资质应当与调换的人员相当。

第六条　甲方向乙方支付技术服务报酬及支付方式为：

6.1　技术服务费总额为人民币 285000 元（大写：贰拾八万伍仟元整）。

6.2　技术服务费支付方式和时间如下：

6.2.1 服务期满 90 个日历天内，乙方向甲方提交榆林职业技术学院 2 份测评报告以及榆林市公安局颁发的 榆林职业技术学院门户网站群管理系统、榆林职业技术学院教务管理系统、榆林职业技术学院教学一体化平台系统、榆林职业技术学院图书馆管理系统、榆林职业技术学院国资管理系统、榆林职业技术学院一卡通管理系统网络安全备案证。甲方收到报告及备案证后，甲方组织验服务收合格后，乙方提供项目全额发票后，甲方在 30 个工作日内向乙方支付技术服务费总额的 80%，计人民币 228000 元（大写：贰拾贰万捌仟 元整）服务使用期满三个月，使用性能稳定后，无质量问题，经甲方确认后，支付技术服务总额的 20%，计人民币 57000 元（大写：伍万柒仟元整）。

6.2.2 乙方开户银行名称、地址和账号为：

开户银行：重庆银行股份有限公司西安分行营业部

地址：陕西省西安市高新区科技二路软件园示范区秦风阁F301室

账号：870101040014642

6.2.3 乙方将自行承担本合同涉及的所有税款。

第七条　双方确定以下方式对乙方的技术服务工作成果验收：

7.1　乙方完成技术服务工作的形式：乙方向甲方提交信息系统安全等级测评项目计划，信息系统安全等级测评方案以及信息系统安全等级测评报告。

7.2　验收方式：甲方以会议形式组织整体项目验收。

第八条　双方确定因履行本合同应遵守的保密义务请参照本合同附件《保密协议》内容。

第九条　工作成果及相关资料的权利归属：

9.1　本合同项下的工作成果及其他相关资料的一切权利（包括但不限于所有权和知识产权）均归甲方享有。

9.2　乙方在服务工作过程中产生工作底稿的所有权及知识产权归甲方所。

第十条　本合同的变更必须由双方协商一致，并以书面形式确定。

第十一条　双方确定，按以下约定承担各自违约责任：

11.1　乙方的违约责任

11.1.1 延迟交付：如因乙方自身原因导致未能如期交付工作成果，则每延期 1 日，应向甲方支付应付款项的1%作为违约金，最高不超过合同总额 5 %。

11.1.2 泄密：乙方或其员工违反本合同的保密义务，给甲方造成损失，乙

方应赔偿甲方遭受的实际损失（包括但不限于经济损失、律师费、诉讼费及其它相关的合理费用）。

11.2　甲方的违约责任

甲方无正当理由未按照合同的约定如期支付应付款项的，则每延期__/__日，应向乙方支付应付款项的__/__%作为违约金，最高不超过合同总额的__/__%。

**第十二条**　侵权责任

12.1　乙方保证其提交的工作成果不侵犯任何第三方的商业秘密、 所有权和知识产权及其他合法权益。

12.2　若乙方违反 12.1 条约定导致甲方受到任何来自第三方的起诉或索赔的，乙方应当负责与第三方进行直接交涉，为甲方进行抗辩，并承担一些责任后果，由此产生任何费用均由乙方自行承担。甲方也可以自行对此提出抗辩，乙方应全力协助甲方，若甲方因此受到任何损失，乙方应当予以全部赔偿。

**第十三条**　不可抗力

13.1　不可抗力指在本合同期限内发生的不可预见（或可预见，但其发生或后果不可避免）、非任何乙方所能控制且任何乙方无法完全履行本合同的国家政策、法律、法规的限制、地震、台风、火灾、水灾、战争、罢工、暴动、黑客攻击或任何其他社会、政治动荡造成的灾难。

13.2　如果出现不可抗力，双方在本合同中的义务在不可抗力影响范围及其持续期间内将中止履行。经另外一方确认的不可抗力影响时间，不计入本合同执行时间。本合同期限可根据中止的期限作相应延长，但需双方协商一致。任何乙方均不会因此而承担责任。

13.3　声称遭受不可抗力的一方应在不可抗力发生后不迟于5日内通知另一方，并随附经有关部门确认的不可抗力书面证明，而尽可能减少不可抗力所产生之影响。

13.4　如果发生不可抗力，双方应立即协商解决问题的方案。不过不可抗力持续60日以上，且致使合同目的无法实现的，则任何一方均可解除本合同。

13.5　在发生不可抗力时，双方各自控制下的设备、资料负有保管责任，对未受不可抗力影响并且可以继续履行的合同义务应继续履行。

**第十四条**　双方因履行本合同而发生的争议，应协商、调节解决。协商、调节不成的，甲方依法向__甲方所在地__人民法院起诉。

**第十五条**　与履行本合同有关的下列技术文件，经双方确认后，为本合同的有效组成部分，与本合同具有同等法律效力：

15.1　《保密协议》；

15.2　《技术规范书》；

15.3　投标文件《榆林职业技术学院网络安全等级测评服务项目竞争性谈判响应文件》。

第十六条　其他事项

16.1　甲、乙双方确认，本合同首页关于双方通讯地址、电话、传真均系真实有效，如有变更，变更方应在变更后24小时内通知对方。因一方变更前述通讯地址、电话、传真而未通知对方，造成对方无法发出通知的，由此造成的损失由变更方负责。

16.2　因本合同履行所发出的（包括但不限于）通知等文件均应采用书面形式，即邮寄信件或手递信件。上述通知等文件的送达，如以邮寄方式送达的，信件发出后第七日为送达日；以手递方式送达的，手递日为送达日。

第十七条　合同的生效及终止

本合同自双方法定代表人或授权代理人签字盖章之日起生效，至甲乙双方履行完本合同项下全部义务之日终止。

第十八条　转让

本合同任何一方未经双方书面同意不得将本合同规定的任何权利和义务转让给任何第三方。

第十九条　适用法律

本合同的签署、执行等有关事项均适用于中华人民共和国法律。

第二十条　合同共计23页，一式 8 份，甲方 4份，乙方 4 份，具有同等法律效力。

甲方：（盖章）榆林职业技术学院　　乙方：（盖章）陕西慧缘网络科技有限公司

法定代表人（授权代理人）：　　法定代表人（授权代理人）：

（签字）　　（签字）梅巧巧

日期：2026 年 1 月 28 日　　日期：2026 年 1 月 28 日

附件 1

# 保密协议

甲方（委托方）：榆林职业技术学院

乙方（受托方）：陕西慧缘网络科技有限公司

按照甲乙双方签订的《网络安全等级保护测评技术服务合同》规定，甲乙双方约定，乙方向甲方提供网络安全技术服务，甲、乙双方本着平等自愿、公平诚信的原则，依据《中华人民共和国劳动法》、《中华人民共和国反不正当竞争法》订立本保密协议，甲乙双方达成如下协议：

**第一条 保密信息定义**

1. 项目实施过程中涉及的技术信息和技术资料：包括但不限于 IP 地址规划、网络架构、网络拓扑、软件系统架构、源代码、配置信息、应用系统数据、系统说明书、维护手册，以及项目实施过程中的会议文件、变更、传真、邮件等相关资料；
2. 项目实施过程中各有关当事人拥有的商业秘密、敏感信息、知识产权等，已经公开的知识产权信息除外；
3. 经营信息：包括客户名称、客户地址及联系方式、需求信息、营销计划、采购资料、定价政策、进货渠道、产销策略、招投标中的标底及标书内容、项目组人员构成、费用预算、利润情况及不公开的财务资料等；
4. 项目实施过程中产生的新技术信息和技术资料；
5. 甲乙双方之间工作往来的人员电话、即时通讯、传真，信函，电子邮件等；
6. 经甲乙双方在项目实施过程中确认的需要保密的其他信息；

**第二条 乙方责任**

7. 乙方应将甲方信息系统涉及的保密信息仅用于本测评项目的调研、方案编制、现场测评和报告编制工作；

8. 乙方对从甲方处获得的技术信息和技术资料负有保密责任，未经甲方同意不得提供给任何第三方；
9. 乙方为承担本协议约定的保密责任，应妥善保管有关的文件和资料，未经甲方的书面许可，不对其复制，仿造等；
10. 乙方应对有关人员进行有效管理，以确保本协议的履行。在本协议约定的保密期限内，乙方如发现有关保密信息被泄露，应及时通知甲方，并采取积极的措施避免损失的扩大；
11. 乙方在实施相关工作过程中，需要向本项目的有关方面（包括：承担相关工作的其他成员、聘请的专家、政府主管部门）提供保密信息时，必须取得甲方的书面许可，或者由甲方负责提供；

**第三条 违约责任**

违反本协议的约定，由违约方承担相应法律责任，并赔偿由此产生的一切损失。双方在履行协议中产生的纠纷，应通过友好协商解决。如协商不成，双方约定的纠纷裁决地点为乙方所在地人民法院；

**第四条 保密期限**

本协议保密期限自盖章之日或者自双方中的一方取得有关文件、资料之日起，以时间在前的为准。

附件 2

# 榆林职业技术学院
# 网络安全等级测评服务购置清单

| 序号 | 设备名称 | 服务内容 | 数量 | 单价（元） | 总价（元） | 备注 |
|---|---|---|---|---|---|---|
| 1 | 门户网站群管理系统 | 网络安全等级测评服务 | 1 | 47500.00 | 47500.00 | 第二级 |
| 2 | 教务管理系统 | 网络安全等级测评服务 | 1 | 47500.00 | 47500.00 | 第二级 |
| 3 | 教学一体化平台 | 网络安全等级测评服务 | 1 | 47500.00 | 47500.00 | 第二级 |
| 4 | 图书馆管理系统 | 网络安全等级测评服务 | 1 | 47500.00 | 47500.00 | 第二级 |
| 5 | 国资管理系统 | 网络安全等级测评服务 | 1 | 47500.00 | 47500.00 | 第二级 |
| 6 | 一卡通管理系统 | 网络安全等级测评服务 | 1 | 47500.00 | 47500.00 | 第二级 |
| 合计：小写：285000.00 元　　大写：贰拾捌万伍仟元整 | | | | | | |

附件 3

# 榆林职业技术学院
# 2025年网络安全等级测评服务技术参数

## 一、工作目标

为深入贯彻落实习近平总书记关于网络安全工作的重要指示精神，根据《中华人民共和国网络安全法》、《信息系统安全等级保护管理办法》以及《关于开展全国重要信息系统安全等级保护定级工作的通知》等文件要求，对我单位信息系统及网络实施等级保护测评工作，找出网络信息系统存在的安全漏洞及隐患，为后续建设和整改工作提供建议和决策依据，进一步提高我单位网络信息系统整体安全防护水平。

## 二、工作内容

本项目是对我院信息系统在“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、安全运维管理”等方面的开展测评工作。

服务内容包括：协助定级备案、编制测评方案、进行现场测评、形成测评报告。

1. 工作对象：

| 序号 | 信息系统名称 | 自定安全保护等级 | 数量 |
|---|---|---|---|
| 1 | 门户网站群管理系统 | 第二级 | 1 项 |
| 2 | 教务管理系统 | 第二级 | 1 项 |
| 3 | 教学一体化平台 | 第二级 | 1 项 |
| 4 | 图书馆管理系统 | 第二级 | 1 项 |
| 5 | 国资管理系统 | 第二级 | 1 项 |
| 6 | 一卡通管理系统 | 第二级 | 1 项 |

2. 实施要求或注意事项

（1）服务商在测评过程中，不得影响系统使用户单位的正常使用；

（2）服务商需确保项目质量符合国家和行业质量标准；

（3）服务商需配备相应的等保测评工程师，项目经理必须为高级测评师，项目经理和项目组其他成员均具有等保测评的资质认证；

（4）服务商在合同签订后 3 个月内完成所有的项目内容。

（5）服务商在实施过程中接触到的用户单位的涉密信息需严格保密并签订保密协议；

（6）服务商须提供网络安全等级测评服务的《风险规避实施方案》。

## 三、工作依据

- 《中华人民共和国网络安全法》
- 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）
- 《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）
- 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
- 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
- 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070- 2019）
- 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
- 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）
- 《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627- 2018）
- 《信息安全技术 网络安全等级保护安全管理中心技术要求》（GB/T 36958-2018）

## 四、二级测评指标

| 安全层面 | 安全控制点 | 测评指标（2.0） |
|---|---|---|
| 安全物理环境 | 物理位置选择 | 1.机房场地应选择在具有防震、防风和防雨等能力的建筑内； |
| | | 2.机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 |
| | 物理访问控制 | 1.机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。 |
| | 防盗窃和防破坏 | 1.应将设备或主要部件进行固定，并设置明显的不易除去的标记； |
| | | 2.应将通信线缆铺设在隐蔽处。 |
| | 防雷击 | 1.应将各类机柜、设施和设备等通过接地系统安全接地。 |

| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| | 防火 | 1. 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； |
| | | 2. 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。 |
| | 防水防潮 | 1. 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； |
| | | 2. 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。 |
| | 防静电 | 1. 应采用防静电地板并采用必要的接地防静电措施。 |
| | 温湿度控制 | 1. 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 |
| | 电力供应 | 1. 应在机房供电线路上配置稳压器和过电压防护设备； |
| | | 2. 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。 |
| | 电磁防护 | 1. 电源线和通信线缆应隔离铺设，避免互相干扰。 |
| 安全通信网络 | 网络架构 | 1. 应划分不同的网络区域，并按照方便管理和控制的原则为各个网络区域分配地址； |
| | | 2. 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。 |
| | 通信传输 | 1. 应采用校验技术保证通信过程中数据的完整性。 |
| | 可信验证 | 1. 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 安全区域边界 | 边界防护 | 1. 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。 |
| | 访问控制 | 1. 应在网络边界或区域之间访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； |
| | | 2. 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； |

| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| | | 3. 应对源地址、目标地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； |
| | | 4. 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。 |
| | 入侵防范 | 1. 应在关键网络节点处监视网络攻击行为。 |
| | 恶意代码防范 | 1. 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。 |
| | 安全审计 | 1. 应在网络边界，重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| | | 2. 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |
| | | 3. 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| | 可信验证 | 1. 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 安全计算环境 | 身份鉴别 | 1. 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| | | 2. 应具有登录失败处理功能，应配置并启用结束会话、限制非法登陆次数和当登录连接超时自动退出等相关措施； |
| | | 3. 当进行远程管理时，应采取必要的措施防止鉴别信息在网络传输过程中被窃听。 |
| | 访问控制 | 1. 应对登录的用户分配账户和权限； |
| | | 2. 应重命名或删除默认账户，修改默认账户的默认口令； |
| | | 3. 应及时删除或停用多余的、过期的账户，避免共享账户的存在； |
| | | 4. 应授予管理用户所需的最小权限，实现管理用户的权限分离。 |

| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| | 安全审计 | 1. 应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| | | 2. 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |
| | | 3. 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| | 入侵防范 | 1. 应遵循最小安装的原则，仅安装需要的组件和应用程序； |
| | | 2. 应关闭不需要的系统服务、默认共享和高危端口； |
| | | 3. 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| | | 4. 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。 |
| | | 5. 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| | 恶意代码防范 | 1. 应安装方恶意代码软件或配置具有相应功能的软件，并及时更新防恶意代码软件版本和恶意代码库。 |
| | 可信验证 | 1. 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| | 数据完整性 | 1. 应采用校验技术保证重要数据在传输过程中的完整性。 |
| | 数据备份和恢复 | 1. 应提供重要数据的本地数据备份与恢复功能； |
| | | 2. 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 |
| | 剩余信息保护 | 1. 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。 |
| | 个人信息保护 | 1. 应仅采集和保存业务必需的用户个人信息； |
| | | 2. 应禁止未授权访问和非法使用用户个人信息。 |

| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| 安全管理中心 | 系统管理 | 1. 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； |
| | | 2. 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 |
| | 审计管理 | 1. 应对安全审计员进行身份鉴别，只允许通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； |
| | | 2. 应通过安全审计员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询。 |
| 安全管理制度 | 安全策略 | 1. 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。 |
| | 管理制度 | 1. 应对安全管理活动中的主要管理内容建立安全管理制度； |
| | | 2. 应对管理人员或操作人员执行的日常管理操作建立操作规程。 |
| | 制定和发布 | 1. 应指定或授权专门的部门或人员负责安全管理制度的制定； |
| | | 2. 安全管理制度应通过正式、有效的方式发布，并进行版本控制。 |
| | 评审和修订 | 1. 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足需要改进的安全管理制度进行修订。 |
| 安全管理机构 | 岗位设置 | 1. 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； |
| | | 2. 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 |
| | 人员配备 | 1. 应配备一定数量的系统管理员、审计管理员、安全管理员等。 |
| | 授权和审批 | 1. 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； |
| | | 2. 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。 |

| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| | 沟通和合作 | 1. 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理信息安全问题； |
| | | 2. 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； |
| | | 3. 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 |
| | 审核和检查 | 1. 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 |
| 安全管理人员 | 人员录用 | 1. 应指定或授权专门的部门或人员负责人员录用； |
| | | 2. 应对被录用人的身份、安全背景、专业资格或资质等进行审查。 |
| | 人员离岗 | 1. 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。 |
| | 安全意识教育和培训 | 1. 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。 |
| | 外部人员访问管理 | 1. 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； |
| | | 2. 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户，分配权限，并登记备案； |
| | | 3. 部人员离场后应及时清除其所有的访问权限。 |
| 安全建设管理 | 定级和备案 | 1. 应以书面的形式说明保护对象的安全保护等级及确定安全保护等级的方法和理由； |
| | | 2. 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定； |
| | | 3. 应保证定级结果经过相关部门的批准； |
| | | 4. 应将备案材料报主管部门和公安机关备案。 |
| | 安全方案设计 | 1. 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； |

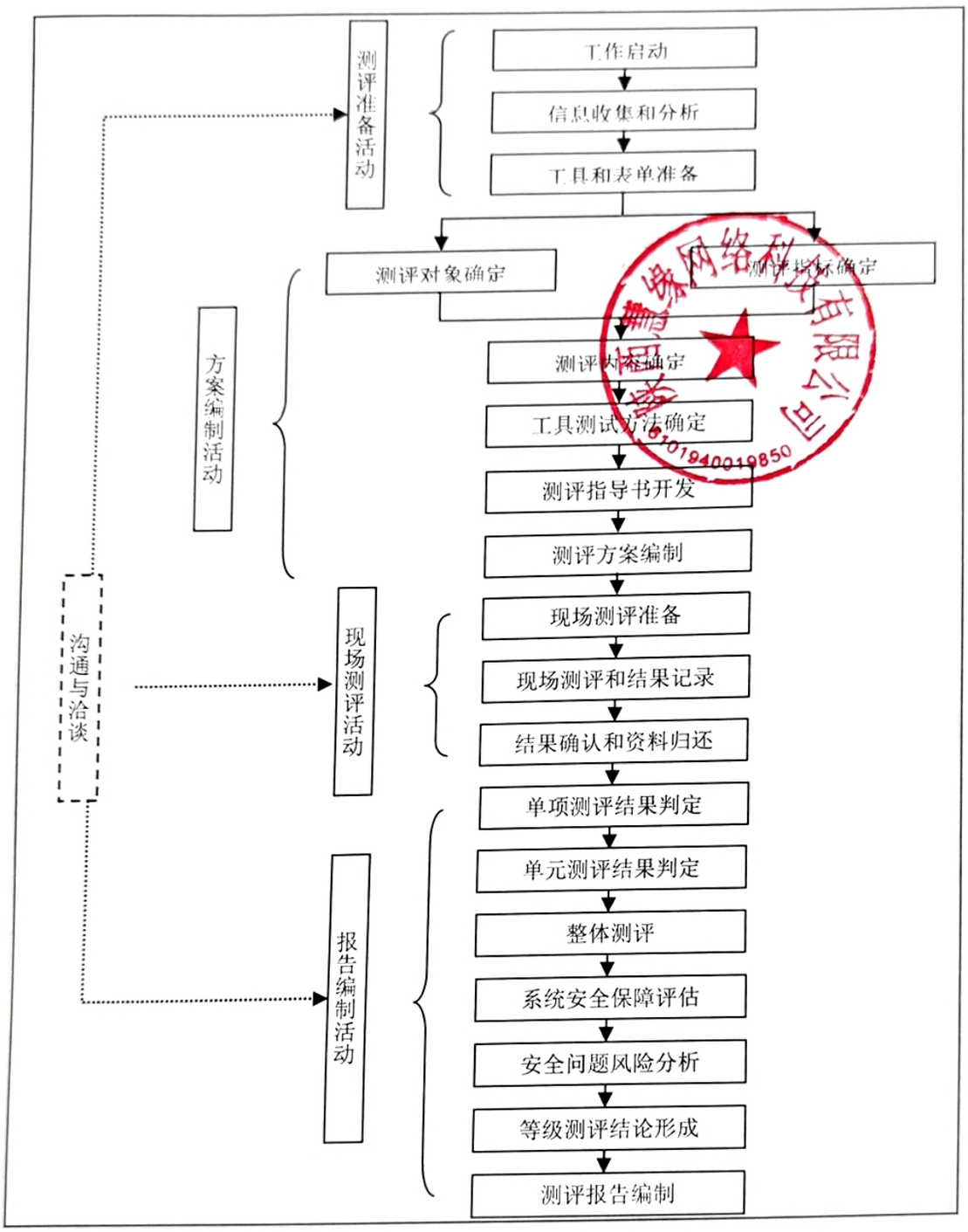
| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| | | 2. 应根据保护对象的安全保护等级进行安全方案设计； |
| | | 3. 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。 |
| | 产品采购和使用 | 1. 应确保网络安全产品的采购和使用符合国家的有关规定； |
| | | 2. 应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。 |
| | 自行软件开发 | 1. 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； |
| | | 2. 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。 |
| | 外包软件开发 | 1. 应在软件交付前检测其中可能存在的恶意代码； |
| | | 2. 应保证开发单位提供软件设计文档和使用指南。 |
| | 工程实施 | 1. 应指定或授权专门的部门或人员负责工程实施过程的管理； |
| | | 2. 应制定安全工程实施方案控制工程实施过程。 |
| | 测试验收 | 1. 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； |
| | | 2. 应进行上线前的安全性测试，并出具安全测试报告。 |
| | 系统交付 | 1. 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； |
| | | 2. 应对负责系统运行维护的技术人员进行相应的技能培训； |
| | | 3. 应提供系统建设过程文档和运行维护文档。 |
| | 等级测评 | 1. 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； |
| | | 2. 在发生重大变更或级别发生时进行等级测评； |
| | | 3. 应确保测评机构的选择符合国家相关规定。 |

| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| | 服务供应商管理 | 1. 应确保服务供应商的选择符合国家的有关标准； |
| | | 2. 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。 |
| 安全运维管理 | 环境管理 | 1. 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； |
| | | 2. 应对机房的安全管理作出规定，包括物理访问，物品进出和环境安全等； |
| | | 3. 应不在重要区域接待来访人员，不随意放置包含敏感信息的纸质文件和移动介质等。 |
| | 资产管理 | 1. 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。 |
| | 介质管理 | 1. 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理并根据存档介质的目录清单定期盘点； |
| | | 2. 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录。 |
| | 设备维护管理 | 1. 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； |
| | | 2. 应对配套设施、软硬件维护管理作出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。 |
| | 漏洞和风险管理 | 1. 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。 |
| | 网络和系统安全管理 | 1. 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； |
| | | 2. 应指定专门的部门或人员进行账户管理，对账户申请，建立账户、删除账户等进行控制； |
| | | 3. 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； |

| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| | | 4. 应制定重要设备的配置和操作手册，依据操作手册对设备进行安全配置和优化配置等； |
| | | 5. 应详细记录运维操作日志，包括日常巡检工作，运行维护记录、参数的设置和修改的内容。 |
| | 恶意代码防范管理 | 1. 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； |
| | | 2. 应对防恶意代码防范要求作出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等； |
| | | 3. 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。 |
| | 配置管理 | 1. 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。 |
| | 密码管理 | 1. 应遵循密码相关的国家标准和行业标准； |
| | | 2. 应使用国家密码管理局认证核准的密码技术和产品。 |
| | 变更管理 | 1. 应明确认变更需求，变更前根据变更需求制定变更方案、变更方案经过评审、审批后方可实施。 |
| | 备份与恢复管理 | 1. 应识别需要定期备份的重要业务信息、系统数据及软件系统等； |
| | | 2. 应规定备份信息的备份方式、备份频度、存储介质和保存期等； |
| | | 3. 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份程序和恢复程序。 |
| | 安全事件处置 | 1. 应及时向安全管理部门报告所发现的安全弱点和可疑事件； |
| | | 2. 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； |
| | | 3. 应在安全事件和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。 |

| 安全层面 | 安全控制点 | 测评指标（2.0） |
| --- | --- | --- |
| | 应急预案管理 | 1. 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； |
| | | 2. 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。 |
| | 外包运维管理 | 1. 应确保外包运维服务商的选择符合国家有关规定； |
| | | 2. 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。 |

## 五、测评流程




## 六、工作成果

最终交付成果包括但不限于以下内容：

《网络安全等级保护测评对象基本情况调查表》

《网络安全等级测评项目计划书》

《网络安全等级测评方案》

《网络安全等级测评报告》