**北京市市级部门信息系统升级改造项目**

**申报书编写说明**

**各项目申报单位应根据本部门顶层设计成果，结合信息化建设的实际情况，根据拟申报项目建设内容，选择申报书参考模板中的相关章节，如实填写，申报材料必须真实、准确、完整。**

**申报书可附带相关的证明材料。（如专家论证意见、领导批示、上级主管单位发文等）**

# 第一部分申报书封面说明

**项目名称：**

**对于新建类项目，项目名称一般为：主责单位简称 + XXXX + “建设项目”， XXXX应为新建信息系统的名称，如“北京市经信委办公系统建设项目”。对于分期建设的项目，可在项目后加上X期。**

**对于升级改造类项目，项目名称一般为：主责单位简称 + XXXX + “升级改造项目”，其中XXXX为要被改造的原信息系统名称，如“北京市经信委办公系统升级改造项目”。对于只对局部进行升级改造的，可在原系统名称后增加限定词以示区别，如“北京市经信委办公系统安全体系升级改造项目”。对于分期升级改造的项目，可在项目后加上X期。**

**如果信息系统名称中能体现所属行业或委办局，主责单位简称可省略。**

**申报单位（盖章）：**

**一般为市级部委办局或市级直属机构，原则上不接受下属机构或部门越过上级主管部门直接申报的项目。**

**申报单位项目联系人：**

**一般为申报单位信息化工作主管部门具体负责该项目的人员。**

**联系电话：**

**一般为固定电话，为便于及时联系沟通，最好同时留存移动电话。**

**申报时间： 年 月 日**

**采用阿拉伯数字填写，为正式递交申报书的日期，对于修改后重新提交的申报书，应填写重新提交时的日期。**

# 第二部分申报书内容编写说明

# 一、背景、现状和必要性

## （一）背景

**概述本项目立项的背景情况和依据，其中立项背景情况包括项目来源、立项论证过程、对拟支撑业务的重要性和紧迫性等；立项依据包括市委市政府领导批示、市政府办实事项目、折子工程、规划范围的等。**

**如果属于升级改造类项目，还应说明本次要升级改造的原系统名称、原建设目标、建设内容、建设时间、终验时间、投入运行时间、投资规模及运行情况等。如果该系统之前已经过升级改造，还应说明历次升级改造的相关情况。**

## （二）现状

**属于系统升级改造类项目，应说明原系统的现状。如果属于多系统整合类项目，应说明本次申报项目所涉及的各系统的现状。主要包括以下内容：**

**1.业务应用方面：重点说明原系统在业务支撑范围、业务处理的实时性和响应时间、业务高峰期在线用户数及并发用户数、业务协同程度等方面的设计能力和实施状况。**

**2.原系统情况：系统采用的技术路线和系统架构，重点说明在软件环境（系统软件品牌和版本）、硬件配置（硬件设备品牌型号）、数据库、数据存储系统的技术和容量、网络及安全等方面的设计能力和实际配置，网络和设备连接图（与相关网络的连通情况及出口带宽）。安全风险评估；安全等级保护工作；安全体系建设；容灾体系建设等。**

**3. 原系统运行效果**

**1）概括说明原系统业务应用是否正常、软硬件运行负荷状况等。所支撑业务的实际数据平均流量和峰值流量。**

**2）系统产生的社会效益和经济效益（投入/产出情况），公共服务覆盖率、用户满意度，资源共享、协同办公等效果，资金等资源配置的合理程度等。**

**4.信息化资产情况。**

**参照《北京市市级信息系统升级改造项目决算报告（参考模版）》的“决算02－1表” 和“决算02－1表”格式说明相关的信息化资产现状。**

**5.存在问题**

**应从原系统的业务应用、支撑服务，软件系统、硬件系统及信息安全体系等方面，分析存在的问题、风险及其原因等。**

**（1）原系统哪些功能和性能不能满足业务发展或信息资源共享等方面需求，需要进行功能完善和扩展；原系统存在哪些较大缺陷，需进行完善或进行技术架构改造等。**

**（2）原系统没有整体信息安全保障措施，需要增加信息安全体系建设；原系统信息安全保障措施需要进行哪些更新和升级；原系统的信息安全等级提高等情况导致需要对原有信息安全体系进行加固建设（不含信息安全体系正常运维保障）等。**

**（3）需要进行版本升级的软件产品（如，操作系统、数据库系统、中间件等）的情况；因服务协议到期需进行更换的软件产品；因设备老化、系统软件对硬件的要求提升、网络流量增加等原因需对网络设备和计算机等硬件设备进行更换或升级的具体情况；因业务发展而需扩充硬件设备配置和软件产品的配置具体情况等。**

**属于新建项目，应说明与新建项目相关的业务系统情况，包括实现方式、工作效率、需要解决的问题等。**

## （三）项目必要性

**概述项目建设的必要性，一般按以下几个方面进行说明：**

**1．推动业务发展，说明拟支撑业务符合部门“三定方案”要求，进行信息化建设对支撑本部门业务工作目标有价值。**

**2．概括存在的问题，说明需要进行升级改造。**

**3．市委、市政府领导批示，政府办实事项目，政府折子工程。**

**4．上级主管单位发文，要求完成的建设任务，或配套建设的项目。**

**5．其它需要说明的必要性。**

# 二、需求分析

## （一）业务需求

**在充分梳理、优化业务流程的基础上，详细描述申报项目拟建设系统所支撑业务需求，包括业务边界、业务模式、业务频度、业务规模等方面内容。**

**并说明系统的最终用户及管理用户，每类用户在业务流程中所对应的角色、权限等方面需求。**

## （二）功能需求

**基于信息系统整合的基础上，根据业务需求，分析申报项目中拟建设系统的功能需求。可从业务应用软件系统、信息资源建设、设备、网络、机房环境等多个方面进行分析、整理和归纳。**

**如果涉及业务协同需求，应用明确本系统和部门内其他系统、其他部门业务系统的功能对接需求，即本系统和外部系统的接口关系。**

**如果存在对共享交换平台、政务云计算服务平台、移动政务平台、物联网平台等全市统筹建设的共性平台使用需求，应说明需要调用哪个共性平台的哪些共性服务。**

## （三）数据需求

**若项目方案中涉及政务信息资源时，应在信息资源梳理分析的基础上，说明本项目采集、共享、整合或者获取哪些数据及这些数据的更新频率，并说明数据采集、数据加工处理、数据存储等方面需求。**

**如果存在跨部门、跨层级资源共享需求，应说明需要共享哪些部门的数据，并具体列出数据内容、共享方式、更新频率等。**

**如果存在部门内部信息资源的整合需求，应说明需要整合哪些系统，并具体列出这些系统中已经形成的信息资源等。**

## （四）性能需求

**说明系统支持的在线用户数、并发用户数、响应时间、访问速度、可靠性等。**

## （五）安全需求

**分析政策法规要求、相关技术规范要求、安全风险，说明系统主要安全需求，及系统在安全等保方面的需求、网站方面的特定安全要求（参见GB/T 31506-2015）等。**

**安全为满足相关标准以及等级保护三级的安全要求，从以下几点满足需求：**

** 加强网络安全防护建设，保障信息系统安全稳定的运行。开展渗透测试和漏洞扫描工作，检测应用系统、网络系统、主机系统和数据库系统的安全情况，为下一步安全整改工作提供合理有效的依据，保障已有信息系统的安全运行。另一方面确保新上线系统的安全性。通过不断优化安全配置和策略，加强信息系统业务连续性建设，确保信息系统安全、有效的运行。**

** 及时发现安全隐患，快速响应确保系统安全运营。通过建立全面监测系统，及时发现安全隐患，一旦发生信息安全事件，能够快速响应并在最短时间内把事故影响面控制到最小。**

** 抵御来自互联网的黑客攻击与威胁，保障合法用户正常访问公司网站及对外业务系统，维护工作业务稳健、持续运营。**

** 通过加强网络安全监测，明确网络安全责任，加强网络安全科技风险防范工作，满足监管部门合规性要求。**

** 健全安全体系文档，并提供相关安全服务，包括技术支持和培训等。**

# 三、建设目标

## （一）业务目标

**业务流程梳理和规范化目标，改进服务和提高效率的绩效目标，业务和信息资源管理机制完善目标等。**

**１．要有对现有业务流程进行梳理和规范化的目标；**

**２．详细说明升级改造后改进服务和提高效率的绩效目标；**

**３．为保证目标实现所采取的完善业务和信息资源管理机制的措施。**

**4．对信息资源建设目标成果的应用说明。**

## （二）技术目标

**软件、硬件、信息资源、安全、运维等目标。**

**从以下几方面论证说明为实现业务目标所必须达到的技术目标。**

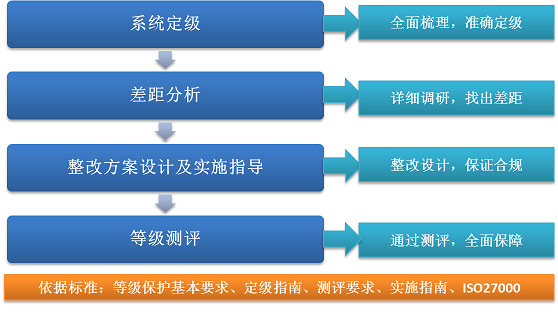
**1．软件的功能、性能、易用性、兼容性、可靠性、健壮性等及支持自主创新的目标；**

**2．信息资源采集、共享、整合和应用的目标；**

**3．网络、存储、主机、机房设备等硬件的性能、兼容性等及支持自主创新的目标；**

**4．根据系统安全风险，依据相应安全等级保护要求在物理、网络、主机、应用、数据备份等方面及支持自主创新的目标；**

**系统安全风险控制按照以下顺序对业务系统进行安全风险的挖掘和规避：**



**依照系统定级及备案指导-》差距分析-》整改方案设计及实施指导-》等级测评，**公安部关于信息系统等级保护定级的相关法规和标准，**实现满足公安部对等级保护的要求目标，以及国家相关标准对业务系统的安全要求目标。**

**5．技术保障运行、支撑业务和数据维护、应急保障等运维方面的目标。**

在应急保障中涉及到系统安全的事件中，依照以下流程处理：



需要现场紧急处理的安全应急响应保障，依照以下流程处理：



## （三）预期绩效

**预期项目实施后所产生的社会综合效益和经济效益两部分，要求对两部分内容分别阐述。**

**1.项目的社会效益主要指项目实施后对本单位公共服务水平提高的作用，对促进社会发展的作用，以及对本单位社会地位和社会影响的提高。**

**2.项目的经济效益主要指项目实施后能产生的收益性成果，可提供量化指标进行说明。**

# 四、建设方案

## （一）建设原则

**说明系统设计、建设时，所应遵循的原则，如统筹规划分步实施、充分利用现有资源等。**

## （二）设计依据

**列出系统设计所依据国家和北京地方的法律法规、标准、规范、指南等。**

## （三）总体建设任务与分期建设内容

**列出项目的建设内容，如应用软件开发、网络建设、安全加固、机房及环境建设等。**

**如果项目内容较多，需要分期实施，在概括总体建设任务的基础上，应详细列出本期的建设内容。**

## （四）总体框架

**列出项目采用的的技术路线、体系架构、拓扑结构、设备部署等，并辅以文字说明。**

**应说明该项目与本部门信息化总体框架的关系，或与相关系统的关系。**

## （五）技术方案

**根据项目设计的内容选择相关内容编写**

### 1. 应用软件开发

**根据需求分析和建设目标，在梳理业务流程和数据流、优化整合相关资源的基础上，制定应用软件开发的解决方案，设计应用软件系统的功能，明确说明哪些功能是新增或完善。**

**应详细描述软件功能中，每个组成部分实现业务处理或数据处理的相关工作，描述业务应用系统与其它系统的接口或数据共享方案。**

**如果涉及跨部门业务协同，应根据需求分析，明确本系统和其他部门业务系统的对接方案，包括系统接口方案等。**

**如果应用软件开发的工作中涉及到共享交换平台、政务云计算服务平台、移动政务平台、物联网平台等全市统筹建设的共性平台，应明确与共性平台的关系，并明确利用共性平台提供的哪些共性服务以及对接方案。如不利用共性平台的服务，而是自行开发类似功能，应说明理由。**

### 2. 信息资源建设

**（1）信息资源概述**

**请简要描述项目（系统）信息资源建设的目标、内容和思路。**

**（2）信息资源建设方案**

**请以目录表格形式明确本项目建设过程中部门内部整合的，及项目建成后形成的数据资源（见表1）。其中，数据资源名称、数据类型、来源方式、更新周期、数据资源共享、数据资源开放为必填项。**

**表1项目数据资源目录**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **数据资源名称** | **数据资源描述** | **数据项** | **数据类型** | **来源方式** | **更新周期** | **数据资源共享** | | | **数据资源开放** | | | **备注** |
| **共享类型** | **共享方式** | **不能向其他政务部门共享的依据** | **开放方式** | **拟开放时间** | **不能向社会开放的依据** |
|  |  |  |  | **□数据库**  **□表格**  **□文本**  **□图片**  **□音视频**  **□地理空间**  **□其它：\_\_\_** | **□数据采集**  **□内部整合**  **□数据共享**  **□其他方式\_\_\_\_\_\_** | **□实时**  **□每日**  **□每周**  **□每月**  **□每季度**  **□每年**  **□其它：\_\_\_\_\_** | **□无条件共享**  **□有条件共享**  **□不共享** | **□北京市大数据管理平台**  **□其他：\_\_\_\_** | ***（如果为空，默认可向其他政府部门共享）*** | **□北京市政务数据资源网**  **□其它：** | **年月** | ***（如果为空，默认可向社会开放）*** |  |

**填表说明：**

**①序号：项目中涉及的数据资源的序号。**

**②数据资源名称：数据资源的名称，如“人口基础信息”。**

**③数据资源描述：对数据资源名称的解释或进一步描述，如数据资源的用途等。**

**④数据项：明确到字段，可叠加。**

**⑤数据类型：数据资源的类型，在对应项打√。选择“其他”应具体说明。**

**⑥来源方式：数据资源的来源方式，在对应项打√。选择“其他方式”应具体说明。**

* **数据采集：指部门自行组织采集或购买数据，应单独进行说明，包括数据采集内容、采集方式、采集频度、更新渠道和长效保障机制等，并详细说明自行采集的理由。**
* **内部整合：指部门内部数据资源的整合，应明确数据整合方案，主要包括拟整合的系统名称、拟整合的数据资源内容、整合技术方式、内部协调情况、保障机制等内容。**
* **数据共享：指从其他政务部门获取数据资源。**

**⑦更新周期：数据资源的更新频率，在对应项打√。选择“其他”应具体说明。**

**⑧数据资源共享：可向其他政务部门共享的数据资源，填写“共享范围”和“共享方式”；不能向其他政务部门共享的数据资源，填写“不能向其他政务部门共享的依据”。**

* **共享类型：“无条件共享”指数据资源通过北京市大数据管理平台汇聚，并可提供给所有政务部门共享使用。“有条件共享”指数据资源通过北京市大数据管理平台汇聚，并可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用。选择“不共享”应具体说明。**
* **共享方式：原则上，政务部门之间的数据资源共享应通过北京市大数据管理平台开展，选择“其他”应具体说明。**
* **不能向其他政务部门共享的依据：应明确上位法或相关文件依据。如果为空，默认可向他政务部门共享。**

**⑨数据资源开放：可向社会开放的数据资源，填写“开放方式”和“拟开放时间”；不能向社会开放的数据资源，填写“不能向社会开放的文件依据”。**

* **开放方式：原则上，可开放的数据资源应通过北京市政务数据资源网向社会开放，选择“其他”应具体说明。数据资源可多渠道开放。**
* **拟开放时间：数据资源预计向社会开放的时间。**
* **不能向社会开放的依据：应明确上位法或相关文件依据。如果为空，默认可向社会开放。**

**（3）需要从其他政务部门获取数据资源，应填写表2。其中，“共享方式”原则上应通过北京市大数据管理平台开展，若选择“其他”应具体说明。**

**表2 需从其他政务部门获取的数据资源目录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **数据资源名称** | **数据资源描述** | **来源部门** | **共享周期** | **共享方式** | **沟通协调情况及保障机制** | **备注** |
|  |  | ***（数据资源的格式、用途等）*** |  | **□实时**  **□每日**  **□每周**  **□每月**  **□每季度**  **□每年**  **□其它：\_\_\_** | **□北京市大数据管理平台**  **□其他：\_\_\_\_\_\_** | ***（可附文字说明）*** |  |

### 3. 主机系统硬件和软件配置

**根据系统性能和信息流流量对主机系统硬件的需求，提出硬件设备配置方案，应明确说明哪些硬件设备是新增、扩容、升级或更换。**

**根据应用软件系统和办公计算机等对主机系统软件产品的需求、服务期限、可更换的产品等，提出软件产品配置方案，应明确说明哪些软件产品是新增、升级或更换，及软件产品部署情况。**

### 4. 网络及综合布线

**根据信息系统的建设目标，按照相关的标准、规范和要求，设计网络系统的整体结构、与其它网络的接口、VLAN划分规划、路由和IP地址分配、网络管理系统等。**

**根据工作区信息点数量和网络需求和建设目标，按照相关的标准、规范，设计水平配线、垂直干线、配线间、机房以及建筑物间的综合布线方案。**

### 5. 安全

**根据现有安全体系现状、需求、风险评估要点、信息安全等级保护和安全目标等因素，按照物理安全、网络安全、主机系统安全、应用安全和数据安全等不同层面，提出信息安全体系建设或加固方案。原则上，要求每个系统都要说明信息安全等级保护的定级。**

**根据提出的信息安全建设或加固方案，简要说明信息安全测评计划。**

* **物理安全测评**

物理安全测评将通过访谈和检查结合的方式评测被测信息系统的物理安全保障情况。主要涉及对象为机房。

* **网络安全测评**

网络安全测评将通过访谈、检查和测试的方式评测信息系统的网络安全保障情况。主要涉及对象机房的网络设备、网络安全设备以及网络拓扑结构等三大类对象。

* **主机安全测评**

主机系统安全测评将通过访谈、检查和测试的方式评测信息系统的主机系统安全保障情况。

* **应用安全测评**

应用安全测评将通过访谈、检查和测试的方式评测信息系统的应用安全保障情况。为信息系统整体安全性进行综合风险评价做准备。

* **数据安全测评**

数据库安全测评将通过访谈、检查和测试结合的方式评测信息系统的数据安全保障情况。本次测评重点检查系统的数据在采集、传输、处理和存储过程中的安全。

* **安全管理机构测评**

安全管理机构测评将通过访谈、检查的方式，评测信息系统管理机构的安全保障情况。主要涉及访谈对象是安全主管。

* **安全管理制度测评**

安全管理制度测评将通过访谈、检查的方式，评测信息系统的安全管理制度是否能保证信息安全的适宜性、充分性和有效性。主要涉及访谈对象是安全主管。

* **人员安全管理测评**

人员安全管理测评将通过访谈、检查的方式，评测信息系统的人员安全管理保障情况。主要涉及访谈对象是安全主管、人事负责人，人事工作人员、安全管理人员、系统管理员和网络管理员。

* **系统建设管理测评**

系统建设管理测评将通过访谈、检查的方式，评测信息系统建设管理的安全措施。主要涉及访谈对象是安全主管和系统建设负责人。

* **系统运维管理测评**

系统运维管理测评将通过访谈、检查的方式，评测信息系统的安全运行维护。主要涉及访谈对象是安全主管、物理负责人、资产管理员、系统运维负责人、系统管理员和审计员。

### 5. 存储备份系统

**根据需要存储备份数据的容量、增量、保存时间和数据操作方式等，选择存储备份系统的解决方案。主要内容包括备份设备、备份介质、备份策略、存储容量、备份软件、存储技术的选择和网络设计等。**

### 7. 安防系统

**根据需要采取的安防措施，分别说明安防系统所包含的子系统，如周界报警系统、视频监控系统等，参考相关的标准、规范，进行方案设计。**

### 8. 机房

**根据机房建设的需求，参考相关的标准、规范，设计机房中的配电、UPS系统、防雷接地、空调、消防、环境监控、门禁等子系统的方案，给出各类设备的型号、数量、作用和连接图，并说明计算依据。**

机房要求

* 机房包括交换机机房、控制室、辅助室等（如无条件，机房与控制室可合并）；
* 机房及有关走廊等地段的土建工程已全部竣工，室内墙壁已充分干燥；
* 机房地面负荷：每平方米不小于450Kg；
* 机房净高：2.70～3.00米；
* 机房主要门的大小应满足设备的搬运需要，房门锁和钥匙齐全；
* 具备通风设备；
* 机房顶棚、墙、门、窗、地面应不脱落，不易起尘，不易积灰，并能防尘砂侵入。屋顶严格要求不漏水、不掉灰，装饰材料应用非燃烧材料或难燃烧材料；
* 各种沟槽应采取防潮措施，其边角应平整，地面与盖板应缝隙严密，照明与电力管线应尽量采用暗铺设；
* 机房颜色：地板一般不采用带花纹图案材料，墙、顶的颜色一般以明朗淡雅为宜，涂料应为无光漆或不含硅化物的油漆；
* 机房地板：推荐铺防静电活动地板。单元活动地板系统电阻值应符合《计算机机房用活动地板技术条件》。地板板块铺设严密坚固，每平米水平误差应不大于2mm。没有活动地板时，应铺设导静电地面(体积电阻率应为1.0×107--1.0×1010Ω)。导静电地面或活动地板必须进行静电接地，可以经限流电阻及连接线与接地装置相连，限流电阻阻值1MΩ。
* 地板绝缘电阻要求如下表：

|  |  |  |
| --- | --- | --- |
| **阻值要求分档** | **每档绝缘电阻值** | **说明** |
| 最小绝缘电阻 | 25×103 Ω |  |
| 最大绝缘电阻 | 1×106 Ω | 对新地板要求 |
| 最大绝缘电阻 | 1×1010 Ω | 地板寿命终了时 |

* 机房地面平整光洁，预留暗管、地槽和孔洞的数量、位置、尺寸均应符合工艺设计的要求；
* 机房的防震加固应符合下列规定:单独建设机房时，机房主楼应按当地基本设计烈度提高一度；设备的安装(尤其是采用活动地板的机房)应按当地基本设计烈度进行抗震加固。
* 机房内要满足国家二级防火标准；

空间要求

为了便于散热和设备维护，建议设备机柜前后与墙面或其它设备的距离不应小于1米，左右可以与其他设备并列，但与墙体之间的距离不能小于0.8米。

线缆要求

* 电缆一般应布放于沟槽中，并采取防潮、防鼠、防火等措施。
* 信号电缆不应和电源电缆混在一起布放，以免受到干扰。
* 局方在设备安装之前完成网线的布放。
* 尾纤的布放。如果工程中配有光接口模块，用户在工程安装之前完成局点间光缆的布放，光纤配线架ODF或线盒ODBF的安装，并把光纤接到ODF/ODB上。
* 网线的布放。 用户在工程安装前完成网络交换机到局域网双绞网线的布放。
* 传输系统的准备：用户在工程前安装好相应的传输设备，并调试好。
* 标签：对所用到的电缆要贴上标签，标签要正确清晰。

安全要求

* 机房必须配备适用的消防器材，如有感烟感温等告警装置，性能应良好。
* 机房内不同的电压插座，应有明显标志。
* 机房内严禁存放易燃、易爆等危险品。
* 楼板预留孔洞应配有安全盖板。
* 根据国家《建筑设计防火规范》中关于“民用建筑的防火间距”规定:通信建筑作为重点防火单位，其设计耐火等级为二级和一级（高层建筑），建筑物之间防火间距不少于6米；而相邻单元建筑物为三，四级时，则其间距不少于7米。

#### 机房环境要求

防电磁干扰要求

各种干扰源，无论是来自设备或应用系统外部，还是来自内部，都是以电容耦合、电感耦合、电磁波辐射、公共阻抗（包括接地系统）耦合和导线（电源线、信号线和输出线等）的传导方式对设备产生影响。

为此应注意：

设备机房应具有抗外界电磁干扰的屏蔽效应。

设备要有良好的接地，铺设防静电地板，或铺贴有半导电材料的地板革，要以铜箔在若干点处接地(水泥地与半导电地板之间压贴铜箔并与地线相连)。

设备本身受到的外界电磁波干扰应严格限制在0.01~10000MHz频率范围内，场强应小于140dBV/m。

设备的交流、直流电缆和信号电缆受到的外界电磁波干扰应满足下表要求：

|  |  |
| --- | --- |
| **频率范围（MHz）** | **最大线路感应电流（dB V/m）** |
| 0.01~0.8 | -21.05lgf+67.9 |
| 0.8~100 | 70 |

额定电磁波干扰表

* （1） 要对供电系统采取有效的防电网干扰措施；
* （2） 设备工作地最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些；
* （3） 远离强功率无线电发射台、雷达发射台、高频大电流设备；
* （4） 与其他设备间的互连电缆（电源线除外）尽量采用屏蔽电缆；
* （5） 必要时采取电磁屏蔽的方法。

防静电要求

尽管网络设备在防静电方面作了大量的考虑，采取了多种措施，但当静电超过一定容限时，仍会对电路乃至整机产生巨大的破坏作用。

在与设备连接的通信网中，静电感应主要来自两个方面：一是室外高压输电线、雷电等外界电场；一是室内环境、地板材料、整机结构等内部系统。因此为防止静电的破坏，应做到：

* （1）设备及地板良好接地；
* （2）室内防尘；
* （3）保持适当的温湿度条件；
* （4）当人体接触电路板时，应戴防静电手腕，穿防静电工作服。

防尘要求

灰尘对设备的运行安全是一大危害。室内灰尘落在机体上，可以造成静电吸附，使金属接件或金属接点接触不良。尤其是在室内相对湿度偏低的情况下，更易造成这种静电吸附，不但会影响设备寿命，而且容易造成通信故障。对机房内灰尘含量及粒径要求如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **最大直径（μm）** | **0.5** | **1** | **3** | **5** |
| 最大浓度（每立方米所含颗粒数） | 1.4 × 107 | 7 × 105 | 2.4 × 105 | 1.3 × 105 |

除灰尘外，设备机房对空气中所含的盐、酸、硫化物也有严格的要求。这些有害气体会加速金属的腐蚀和某些部件的老化过程。机房内应防止有害气体如SO2、H2S、NO2、NH3，CL2等的侵入，其具体限制值如下表所示：

|  |  |  |
| --- | --- | --- |
| **气 体** | **平均（mg/m3）** | **最大（mg/m3）** |
| 二氧化硫 SO2 | 0.2 | 1.5 |
| 硫化氢 H2S | 0.006 | 0.03 |
| 二氧化氨 NO2 | 0.04 | 0.15 |
| 氨 NH3 | 0.05 | 0.15 |
| 氯气 CL2 | 0.01 | 0.3 |

**建议机房防尘的措施：**

* 门、窗均加密封。外窗加双层玻璃并密封，门加防尘密封条。理想的条件是天窗密封机房，加尘埃过滤装置；
* 保持工作服及拖鞋清洁，经常更换；
* 操作设备尽量设在外间，避免经常进出人员及经常开闭机房门；
* 在允许的范围内使机房的相对湿度高一些，这样可以减少尘埃的静电吸附；
* 机房的墙面及顶棚按规定必须是刷漆或贴壁纸。而以刷无光漆的效果为好。

温湿度要求

为保证设备正常工作和延长使用寿命，机房内需维持一定的温度和湿度。若机房内长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，有时也易发生材料机械性能变化、金属部件锈蚀等现象；若相对湿度过低，绝缘垫片会干缩而引起紧固螺丝松动，同时在干燥的气候环境下，易产生静电，危害设备上的电路；温度过高则危害更大，它会使设备的可靠性大大降低，长期高温还会影响其寿命，过高的温度将加速绝缘材料的老化过程。 设备对温湿度的要求如下所示。

|  |  |  |  |
| --- | --- | --- | --- |
| **温度** | | **相对湿度** | |
| 长期工作 | 短期工作 | 长期工作 | 短期工作 |
| 15℃～30℃ | 0℃～45℃ | 40%～65% | 10%～40% |

空调温度最佳范围为20℃--25℃。

空调湿度最佳范围为50％--60％。

注1：设备正常工作环境下，温、湿度的测量点系指：在地板以上2米和设备前方0.4米外测量的数值(机架前后没有保护板时测量)。

注2：短期工作条件系指连续不超过48小时和每年累计不超过15天。一般有条件单位就应考虑配置空调。

注3：极端恶劣工作环境，一般指机房空调系统出现故障时可能出现的环境温度和湿度值。每次不应超过5小时能恢复正常工作范围。

接地要求

接地的良好是设备稳定工作的基础，是接入网防止雷击、抵抗干扰的首要保证条件。请按设备接地规范的要求，认真检查安装现场的接地条件，并根据实际情况把接地工作做好。

设备对接地的要求如下：

接地端子的接触电阻要小于0.1Ω（通过12V/25A的试验）；

要求机房接地电阻阻值<1Ω ；

接地线（PGND）应该是黄绿相间的导线，接地线截面积必须≥25mm2，工程施工时连接线尽量短；

应对接地端子采取必要的措施以防止腐蚀；

保护接地端子应用防松组合螺钉加固。

### 9. 其它

**不在上述范围内的其它类建设内容。**

## （六）设备选型原则及关键技术指标

**说明主要设备，如操作系统、中间件、数据库系统、服务器、交换机、路由器等系统软硬件选型时，在标准化、成熟度、兼容性、性价比、技术服务能力等方面的考虑，及其选型依据。**

**说明主要设备的关键技术指标。**

**设备选型依照性价比最高原则进行，对比各家云服务商，在单位运算能力内价格最低的服务商优先考虑。**

**操作系统仅限于linux中的unbutu和centos中选择。其中ubuntu版本不得低于14，centos版本不得低于6.7.**

**云服务商选择时还应考虑服务商售后支持的能力，包括但不限于云服务商的售后技术支持能力，应急响应和介入的效率，对一般事件的处理能力，对三方事件的协调和解决能力等。**

## （二）监理（聘请第三方监理）

**本项目是否需要监理，按照项目性质，重点说明需要监理范围、监理工作内容。**

不需要监理

## （三）安全测评及软件测评

**本项目是否需要安全测评及软件测评，按照项目性质，重点说明需要安全测评及软件测评范围、工作内容。**

* + - * 1. 整体测评

国标GB/T22239-2008 中的要求项，是为了对抗相应等级的威胁或具备相应等级的恢复能力而设计的，但由于安全措施的实现方式多种多样，安全技术也在不断发展，信息系统的运行使用单位所采用的安全措施和技术并不一定和 GB/T 22239-2008的要求项完全一致。因此，需要从信息系统整体上是否能够对抗相应等级威胁的角度，对单元测评中的不符合项和部分符合项进行综合分析，分析这些不符合项或部分符合项是否会影响到信息系统整体安全保护能力的缺失。信息系统的整体测评，就是在单元测评的基础上，评价信息系统的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。

信息系统整体测评从安全控制点间、层面间和区域间等方面进行安全分析和测评，并最后从系统结构安全方面进行综合分析，对系统结构进行安全测评。

安全控制点间安全测评是指对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

层面间安全测评是指对同一区域内的两个或者两个以上不同层面的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

区域间安全测评是指对两个或者两个以上不同物理或逻辑区域间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

* **安全控制间安全测评**

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。安全功能上的削弱会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性。例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

在测评安全控制间的增强和补充作用时，应先根据安全控制的具体实现和部署方式以及信息系统的实际环境，分析出位于物理安全、网络安全、主机系统安全、应用安全和数据安全等同一层面内的哪些安全技术控制间可能存在安全功能上的增强和补充作用，分析出处在安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等同一方面内的哪些安全管理控制间可能存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断安全控制相互作用后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评安全控制间的削弱作用时，应先根据安全控制的具体实现方式和部署方式以及信息系统的实际环境，分析出位于物理安全、网络安全、主机系统安全、应用安全和数据安全等同一层面内的哪些安全技术控制间可能会存在安全功能上的削弱作用，分析出处在安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等同一方面内的哪些安全管理控制间可能存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程进行测评验证。最后根据测评分析结果，综合判断安全控制相互作用后，一个安全控制是否影响另一个安全控制的功能发挥或者给其带来新的脆弱性，使其功能削弱。

如果安全控制间优势互补，使单个低等级安全控制发挥的安全功能达到信息系统相应等级的安全要求，则可认为该安全控制没有影响信息系统的整体安全保护能力。如果安全控制间存在削弱作用，使某个安全控制的功能等级降低到其安全功能已不能达到信息系统相应等级的安全要求，则可认为该安全控制影响到信息系统的整体安全保护能力。

* **层面间安全测评**

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。安全功能上的增强和补充可以使两个不同层面上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个层面上的安全控制影响另一个层面安全控制的功能发挥或者给其带来新的脆弱性。

在测评层面间的功能增强和补充作用时，先根据层面的整合集成方式和信息系统的实际环境，重点研究不同层面上相同或相似的安全控制（如主机系统层面与应用层面上的身份鉴别之间的关系），以及技术与管理上各层面的关联关系，分析出哪些安全控制间可能会存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断层面间整合后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评层面间的功能削弱作用时，应先根据层面的整合集成方式和信息系统的实际环境，分析出哪些安全技术层面间和安全管理方面可能存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断不同层面整合后，一个层面是否影响另一个层面安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

如果层面间安全功能增强或优势互补，使单个或部分低等级安全控制发挥的安全功能达到信息系统的安全要求，则可认为这些安全控制没有影响信息系统的整体安全保护能力。如果层面间存在削弱作用，使某个或某些安全控制的功能等级降低到其安全功能已不能满足信息系统相应等级的安全要求，则可认为这些安全控制影响到信息系统的整体安全保护能力。

* **区域间安全测评**

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。例如，流入某个区域的所有网络数据都已经在另一个区域上做过网络安全审计，则可以认为该区域通过区域互连后具备网络安全审计功能。安全功能上的增强和补充可以使两个不同区域上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个区域上的安全功能影响另一个区域安全功能的发挥或者给其带来新的脆弱性。

在测评区域间的功能增强和补充作用时，先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析出哪些区域间可能会存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断区域间互连互通后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评区域间的功能削弱作用时，先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析出哪些区域间可能会存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断不同区域互连互通后，一个区域是否影响另一个区域安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

如果区域间安全功能增强或优势互补，使单个或部分低等级安全控制发挥的安全功能达到信息系统的安全要求，则可认为这些安全控制没有影响信息系统的整体安全保护能力。如果区域间存在削弱作用，使某个或某些安全控制的功能等级降低到其安全功能已不能满足信息系统相应等级的安全要求，则可认为这些安全控制影响到信息系统的整体安全保护能力。

* **系统结构安全测评**

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。例如，由于信息系统边界上的网络入侵防范设备的管理接口连接方式不当，可能使网络访问控制出现旁路，出现信息系统整体安全防范不当。测评分析信息系统整体结构的安全性，主要是指从信息安全的角度，分析信息系统的物理布局、网络结构和业务逻辑等在整体结构上是否合理、简单、安全有效。测评信息系统整体安全防范的合理性，主要是指从系统的角度，分析研究信息系统安全防范在整体上是否遵循纵深防御的思路，明晰系统边界，确定重点保护对象，在适当的位置部署恰当的安全技术和安全管理措施等。

在测评分析信息系统整体结构的安全性时，应掌握信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等各种情况，结合业务数据流分析物理布局与网络拓扑之间、网络拓扑与业务逻辑之间、物理布局与业务逻辑之间、不同信息系统之间存在的各种关系，明确物理、网络和业务系统等不同位置上可能面临的威胁、可能暴露的脆弱性等，考虑信息系统的实际情况，综合判定信息系统的整体布局是否合理、主要关系是否简单、整体是否安全有效等。

在测评分析信息系统整体安全防范的合理性时，应熟悉信息系统安全保护措施的具体实现方式和部署情况等，结合业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等，参照纵深防御的要求，识别信息系统的安全防范是否突出重点、层层深入，综合判定信息系统的整体安全防范是否恰当合理等。

* + - * 1. 测评报告编制阶段

通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成测评报告文本。主要任务包括：

1. 针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据，形成初步单项测评结果。
2. 将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果。
3. 针对单项测评结果的不符合项，采取逐条判定的方法，从安全控制间、层面间和区域间出发考虑，给出整体测评的具体结果，并对系统结构进行整体安全测评。
4. 测评人员依据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。
5. 测评人员在测评结果汇总、风险分析和评价的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。
6. 测评报告编制。

工作过程如下：

测评报告编制阶段工作过程表

| **项目工作内容** | **工作详细任务** | **实施人员** | **输出** |
| --- | --- | --- | --- |
| 1.单项测评结果判定 | 分析测评项所对抗威胁的存在情况 | 项目经理  管理测评组  系统测评组  网络测评组 | 《等级测评报告》的单项测评结果部分 |
| 分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较 |
| 综合判定单个测评项的测评结果 |
| 2.单元测评结果判定 | 汇总每个测评对象在每个测评单元的单项测评结果 | 《等级测评报告》告的单项测评结果汇总分析部分 |
| 判定每个测评对象的单元测评结果 |
| 3.整体测评 | 分析不符合和部分符合的测评项与其他测评项（包括安全控制间、层面间、区域间、系统结构）之间的关联关系及对结果的影响情况 | 《等级测评报告》的系统整体测评分析部分 |
| 分析被测系统整体结构的安全性对结果的影响情况 |
| 4.风险分析 | 整体测评后的单项测评结果再次汇总 | 《等级测评报告》的风险分析部分 |
| 分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性 |
| 分析威胁利用安全问题后造成的影响程度 |
| 为被测系统面临的风险进行赋值 |
| 评价风险分析结果 |
| 5.等级测评结论形成 | 统计再次汇总后的单项测评结果为部分符合和不符合项的项数 | 等级测评报告的等级测评结论部分 |
| 形成等级测评结论 |
| 6.测评报告编制 | 概述测评项目情况 | 《等级测评报告》  提交用户 |
| 描述被测系统情况 |
| 描述测评范围和方法 |
| 描述整体测评情况 |
| 汇总测评结果 |
| 描述风险情况 |
| 给出等级测评结论和整改建议 |

* + 1. 交付成果

《系统等级保护测评报告》

## （四）相关保障措施

**针对项目实施过程中，对可能存在的质量、进度、人员、运维等方面的问题，提出相应的应对措施和风险管理计划。**

## 项目管理体系

### 项目管理组

项目管理组由各专项小组组长组成，负责项目的时间、进度、资源、时间的分配和把握总体管理，保障项目质量。人员应具有丰富的系统设计、开发和项目管理能力。

人员构成：

由具有丰富项目管理经验的人员组成，出一名高级管理人员担任组长。

职责：

1、草拟项目管理的各项制度。

2、对项目过程中的质量管理进行监控，对发现的质量隐患进行监督。

3、协助项目评审小组对项目进行阶段评审。

4、定期提交项目实施监控报告，指出存在问题，提出解决方案。

5、协调项目组内人员的分工合作，资源分配。

6、保存项目过程中的相关文件和数据。

7、为优化项目管理提出建议。

### 项目评审组

项目评审小组由公司技术专家委员会的委员组成。主要职责如下：

1、对实施计划和阶段报告进行评审。

2、对重大技术方案进行评审。

3、在里程碑阶段对整个项目进行总体评审和评估。

4、项目结束时，对项目总结报告进行评审。

## 项目实施体系

根据本项目的特点与分工不同，项目实施体系可分成总体组、安全实施组、技术文档管理组和项目质量保障组五部分。具体职能如下：

### 总体组

由资深系统分析人员和资深系统集成人员组成。主要职责如下：

1、负责方案的总体把握，具体负责系统方案设计，设备选型、采购和验收网络互连调试过程中的技术指导。

2、提出并确立业务整体需求，指导完成系统分析和系统结构设计。

3、负责制定阶段验收标准和最终验收标准，报领导小组审批。

### 安全实施组

安全实施组，承担整个安全系统建设的现场施工监督、网络互连设备的安装、调试、维护与培训等各项任务，安全实施组可以根据施工过程中的具体情况向总体组提出方案更改与调整意见。

人员构成：

由的技术人员和项目涉及的供货商的工程技术人员共同组成。担任组长。

职责：

1、负责谈判采购的相关安全设备的到货、清点验货、自检、安装、调试。

2、按照总体设计的要求进行设计、施工，并且在需要时根据总体设计的变更来调整具体设计和施工。

3、进行项目的验货、设备安装调试。

4、参与验收。

5、根据各阶段的工程安排，有组织地对一卡通公司的工程技术人员进行技术培训。

### 标准规范体系组

本小组负责本期工程标准规范体系的需求调研、编制、推广和完善，项目小组设置小组长、工程师。小组长向项目经理汇报。

职责

1、需求调研

2、标准规范编制

3、标准规范推广

4、标准规范完善

5、协助验收

### 技术文档管理组

人员构成：

由熟悉安全工程和国家文档编制规范的管理人员组成。

职责：

1、制定项目的文档计划。

2、依照项目实施计划，进行文档标识和追踪。将整个工程中的每一变化情况纳入受控状态，使项目各实施小组都能及时得到项目进行的最新资料。

3、按照各类文档产生期限收集整理各类文档。控制文档格式，编制文档清单，管理文档版本等。

4、与一卡通公司进行文档的交接。

### 质量保障组

项目测试小组由有丰富开发经验和测试经验的技术人员组成，负责整个系统的测试和质量保证工作。

## 项目支持体系

### 项目协调组

解决项目实施中出现的问题、完成项目所需的商务界面。由的资深客户经理、厂商、用户代表组成。

职责

1、负责本项目所需产品的采购、定货、验货和送货。并保证按时、按质提供本项目所需产品，与供货商沟通确保供货商为一卡通公司提供优质的技术支持与服务。

2、在项目实施过程中及早筹款，按时提供项目所需系统软件。

3、为实施人员在通讯、交通、工作联系、工程施工等方面提供便利条件。

### 培训组

人员构成：

由专门资深技术人员组成。

职责：

1、策划、组织现场安装调试培训。

2、安排具体的技术培训课程。

3、负责根据培训计划对用户进行各类培训。

## 项目协调体系

人员构成：

由的资深销售经理、资深项目经理、资深系统工程师、一卡通公司代表组成。

职责：

1、负责本项目所需产品的采购、定货、验货和送货。并保证按时、按质提供本项目所需产品，为一卡通公司提供优质的技术支持与服务。

2、在项目实施过程中及早筹款，按时提供项目所需设备及系统软件。

3、为实施人员在通讯、交通、工作联系、工程施工等方面提供便利条件。

## 项目过程管理

项目管理主要分为五大程序组，包括项目的启动，计划，执行，控制和总结。项目管理应用多领域管理技巧包括项目时间管理、项目范围管理、项目成本管理、项目质量管理、项目人力资源管理、项目交流管理、项目风险管理、项目采购管理和项目整合管理。

项目管理的基础是PMI的项目管理体系和系统安全工程成熟度模型SSE－CMM。

SSE-CMM的目的是建立和完善一套成熟的、可度量的安全工程过程。该模型定义了一个安全工程过程应有的特征，这些特征是完善的安全工程的根本保证。这个安全工程对于任何工程活动均是清晰定义的、可管理的、可测量的、可控制的并且是有效的。SSE-CMM模型及其评定方法汇集了业界常见的实施方法，提供了一套业界范围内（包括政府及产业）的标准度量体系，确保了在处理硬件、软件、系统和组织安全问题的工程实施活动后，能够得到的一个完整意义上的安全结果。

PMI的项目管理知识体系则把项目管理归纳为范围管理、时间管理、成本管理、质量管理、人力资源管理、风险管理、采购管理、交流管理和整合管理九大知识领域。PMI知识体系为信息安全设备采购项目管理提供了指南。

项目管理方法则整合了PMI的项目管理体系和SSE－CMM系统安全工程成熟度模型，强调分布于整个工程生命周期中各个环节的安全工程活动，包括概念定义、需求分析、设计、开发、集成、安装、运行、维护及更新项目，并不断改进工程实施的现状，达到提高系统安全、产品安全和工程服务安全的质量和可用性并降低成本，充分体现了在工程管理和实施方面的工程能力。

对于本次项目，建议可通过建立工作细分结构（Work Breakdown Structure，WBS）明确项目的工作内容，这样不仅定义了工作内容，同时也定义了工作任务之间的关系，明确了工作界面。项目的WBS是对工作计划、进度、费用、技术状态进行部署和跟踪控制等管理活动的基础。

1. 项目管理

有效的项目管理机制是顺利开展等级测评工作的基础，同时可加快项目进度，提高项目质量，顺利达到项目预期目标。等级测评项目重点在于等级测评结果的质量上，有效的项目进度控制、变更管理与项目沟通是等级测评项目实施质量的基础保障。

项目进度管理

采用科学的方法将用户实施的要求与项目各阶段的工作内容相结合制定切实可行的工程实施计划，将每一项工作细分到每一人，且每一项细分的工作周期都不大于一周，每一项工作都有明确的检验标准。项目经理每周都应该进行项目进展回顾，发现问题，解决问题。以确保项目严格按计划执行。

为了保证项目进度的要求，的项目相关人员会做到：

1. 项目经理定期提交一份项目进度安排，经项目领导小组批准；
2. 在每次项目例会上，项目经理需要与相关负责人员讨论项目进度情况，对不能按时完成的部分要及时制定方案，及时处理；
3. 在每次项目例会上，项目经理必须汇报项目进度情况，如果有严重的延时，则需要向项目领导小组汇报，以便寻求解决办法；
4. 更改后的项目计划必须经管理委员会通过方可实施。

项目变更管理

项目变更将按照“项目变更控制流程”执行。

1. 项目变更管理的内容包括项目的变更申请、变更评估、申请审批、变更实施（如若通过审批）。
2. 项目的任何参与方（者）在确定变更的必要性时需要填写《变更申请表》向项目经理或项目领导提出变更申请。请求的范围可涉及项目的内容、时间计划、交付物、资源、技术规范和标准等诸多方面。申请人可是测评方的项目组成员，或者委托方项目组成员。
3. 项目测评变更影响应考虑所有受到影响的项目的各个方面，如：

* 对交付物影响
* 对进度的影响
* 对成本的影响
* 对风险的影响
* 对资源的影响
* 对付款进度的影响

1. 项目经理依据以下变更批准权限范围来进行相应的上升报告和获取相应的审批，并将变更记录存放于项目文档中，如下表所示：

**项目变更范围权限管理**

|  |  |
| --- | --- |
| **变更范围** | **变更批准权限** |
| 项目工作局部调整，项目工作范围不变 | 项目经理 |
| 项目工作范围变化，不影响工期、成本、交付物 | 项目领导小组 |
| 项目工作范围变化，影响工期、成本、质量、交付内容 | 项目领导小组 |
| 项目工作局部调整，项目工作范围不变 | 项目经理 |
| 问题处理执行人 | 解决问题，记录问题处理状态，解决后及时反馈给问题负责人 |

1. 项目变更申请不管得到批准还是拒绝，都意味着各方对批准或拒绝后的影响有了共识并决定接受。各方将协调调整项目计划和其他影响到的项目文件，安排资源，确定变更行动计划和责任人，实施此变更，并填写变更实施报告和存档。测评方项目经理将变更申请、变更批准和变更实施报告存放于在项目文档中。

项目质量管理

质量管理包括两个方面：项目实施过程、项目实施的交付成果。本项目是咨询、服务类项目，主要交付物是文档资料，包括：各类过程文件和阶段性报告等，通过文档评审活动来完成质量保证。

本项目文档评审活动包括三个层面：

*  项目组评审
*  管理层评审
*  专家评审

具体可参见项目内容与方案中各阶段的说明。项目经理和质量监督员定期跟踪项目实施过程的各项任务的执行及其质量，检查和督促各项评审活动的执行，及时发现项目工作中的问题，并通过评审总结报告、项目周报等形式向各项目组成员汇报质量活动的结果。

项目沟通管理

本项目的沟通方式主要包括：

1. 会议：

**项目沟通管理-会议**

|  |  |  |
| --- | --- | --- |
| **会议类型** | **参加者** | **会议主要目的** |
| 项目开工大会 | 委托方项目组全体（领导小组和项目小组）  委托方用户代表  实施方项目组、项目经理、主要成员 | 对项目目标、项目完成的衡量标准、项目主要交付物等达成是共识  审查通过项目计划  得到双方高层对资源投入的承诺  达成就沟通模式和策略的共识 |
| 项目进程每月例会 | 委托方领导小组、组长、主要成员、项目组全体 | 报告项目进程、阶段性成果  解决在项目层面不能解决的问题  确定项目需要改进的方面  确定纠正措施并指定责任人 |
| 项目进程每周例会 | 实施方/委托方项目组全体成员 | 总结项目的现状、协调项目工作、沟通交流工作结果  分析项目风险，提出应对措施。  审阅、评估、批准项目变更请求，检查已批准变更请求之实施状态。 |
| 阶段结束回顾会议 | 项目领导小组主要成员 | 审核、确定项目组提交的相关交付材料、阶段成果、下阶段工作计划  在阶段结束时回顾项目进程、分析项目趋势，决定项目进度计划基础值是否需要调整  进行阶段性验收 |
| 项目结束会议 | 项目组全体（包括委托方、 实施方项目组全体） | 总结项目绩效  总结项目经验教训  确认项目遗留问题，决定跟进计划和责任人 |
| 问题解决会议  变更处理会议 | 项目组相关人员 | 已解决问题为宗旨，分析问题原因，寻求解决方案，在必要时升级问题  分析变更影响，处理变更 |

1. 在每次会议之后，相关责任人将发出会议纪要，对会议中达成的共识、讨论或未解决的问题、行动计划予以记录。
2. 报告：

项目主要将采用的报告类型如下表。报告的正式语言为中文。

**项目沟通管理-报告**

|  |  |
| --- | --- |
| **报告类型** | **分发群体** |
| 周报告 | 项目本阶段的成员 |
| 月报告 | 全体项目组成员 |
| 项目总结报告 | 全体项目组成员 |
| 会议纪要 | 应参加会议的人员（包括缺席者） |

1. 日常通信：

项目采用电子邮件和传真为正式的日常沟通手段。正式语言为中文。

1. 风险规避措施

系统等级保护建设项目的主要任务是由安全测评服务人员来完成，根据项目特点，项目风险主要来源于安全测评的服务人员。通过风险控制措施、安全测评与安全加固风险规避措施可有效降低项目实施过程中产生的风险问题，降低风险发生的机率。

检查风险规避

在本次检查中可能存在的技术风险有：

* 工具扫描策略集配置不当

由于在系统中存在不同的主机、网络设备及安全设备，且网络关系复杂。因此，为了降低扫描工具对业务及网络的影响，应当根据具体的检查对象类型从扫描策略上就进行策略集的最优配置。

* 网络应用脆弱

在进行网络设计和实施过程中，由于缺乏安全性、可靠性和扩展性的考虑，使得网络的核心设备和支撑网络难以满足不断扩展的业务需求。基于以上的检查风险的分析，可以采取以下措施进行风险规避。

* 检查时间的选择

执行工具扫描检查需要避开业务的高峰时段，从而减小检查对业务的影响。

* 扫描测试

在可能的情况下，对扫描对象测试机进行预检查。检查方式上采用分类扫描和单台扫描。对不同的检查对象执行不同的扫描策略；对存在备份关系的设备，可以进行单台扫描。

* 减缓扫描速度

通过减少并发线程来降低被扫描主机所承受的压力，在几次测试后得出适中的并发线程数量及扫描方式。

* 优化扫描策略配置

扫描策略的最优配置原则是：分类扫描：对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的弱点测试。

针对扫描对象细化扫描策略配置：对于不同类型的主机或者设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。经过对扫描策略的优化，即降低了流量，又减少了不必要的弱点测试给业务带来的风险。

* 厂商协作

厂商需要提供各应用程序的名称、版本、协议、进程名和相应的端口号等信息，在检查之前，由甲方与检查服务商以及业务厂商共同分析检查对业务可能造成的风险，分析可能存在的问题。在检查过程中尽量规避这些风险。

## 安全加固风险规避

为保证系统的正常运行，安全加固过程中对网络系统造成的异常情况降到最低点，应对加固对象运行的操作系统和应用系统进行调研，制定合理的、复合系统特性的安全加固方案，实施严格按照安全加固方案所确定内容和步骤进行，确保每一个操作步骤都对在线系统没有损害。

另外为了防止在安全加固过程中出现异常情况，防止安全加固对互联网接入系统造成损害，保证网络系统在诸如此类的灾难发生后能及时的恢复与运转，确保系统的正常运行或异常情况的发生降到最低点

## （五）其它相关内容

**针对复杂或规模较大的项目，应包括人员培训方案，培训方案中应说明培训人员类型、数量、培训方式和培训内容等。**

### 培训目的

组织技术培训的主要目的是希望通过规范和完整的培训过程，让公司的技术人员对项目中涉及的安全产品有一个直观的认识和感受。通过技术培训可帮助公司的技术人员利用安全产品来进一步完善计算机网络系统的管理，对目前建设中的系统体系结构、主要使用的技术手段及其工具有一个系统的了解。

### 培训内容

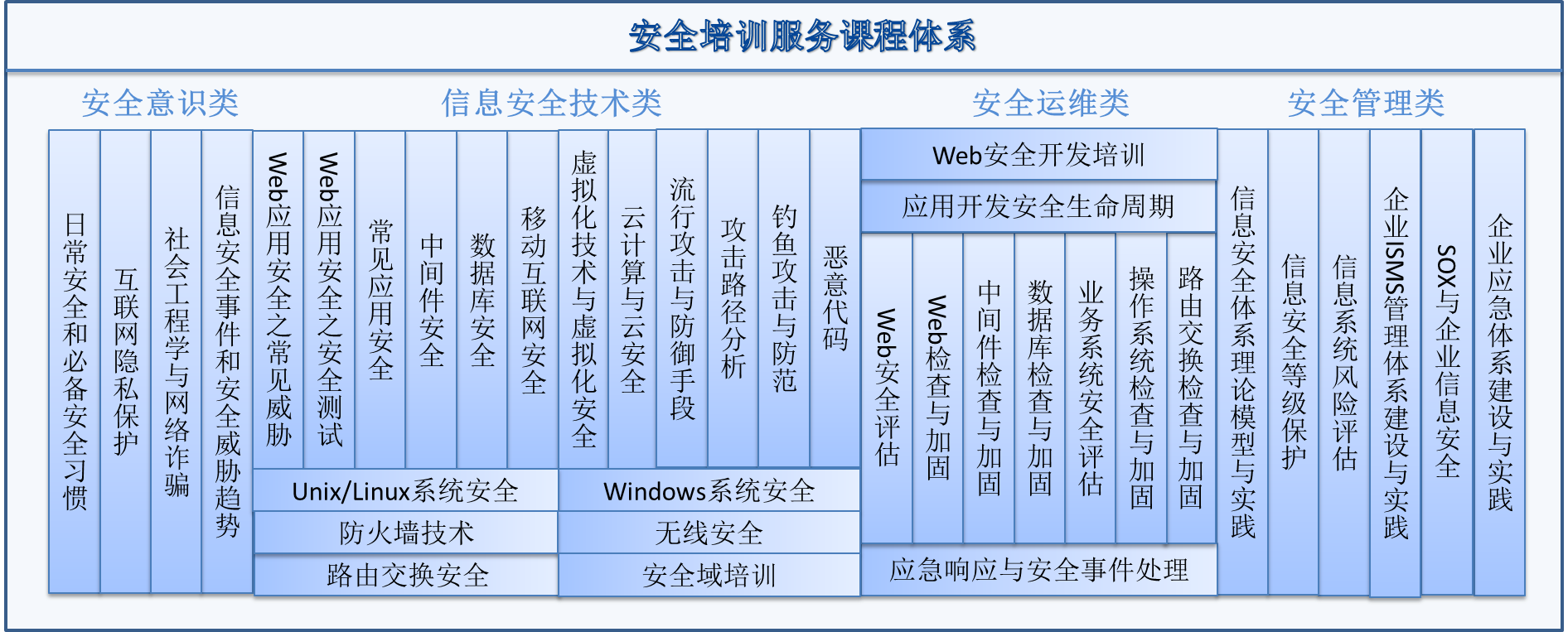
培训由负责师资、教材的提供并负责组织实施，公司可根据实际需求与协商定制化课程内容，具体培训内容如下：

培训课程概述

安全攻防技术培训和安全开发培训。其中，安全攻防技术培训内容又可细分为两块：流行攻击与防御手段和Web应用安全之安全测试。安全开发培训部分也可细分为两块：Web安全开发培训和应用开发安全生命周期培训。

应公司要求，此次安全培训采用企业内训形式提供安全培训服务，讲师集中当面授课，课后答疑。此外，提供每堂的随堂练习，协助学员进行知识回顾，发现知识吸收中不足的问题并及时回复学员的提问。

四大类课程分类



按照课程内容将所提供安全培训服务课程分成下面四大类课程：

* 安全意识类
  + 意识培训
  + 安全趋势培训
* 信息安全技术类
  + 应用技术培训
  + 操作系统技术培训
  + 网络技术培训
  + 攻击与防范培训
* 安全运维类
  + 安全开发培训
  + 安全防护培训
  + 安全演练培训
  + 安全事件处理培训
* 安全管理类
  + 安全标准课程培训
  + 体系建设课程培训

**针对复杂或规模较大或涉及建设多家单位的项目，还应提供运维方案，包括运维费评估。**

**成立领导协调小组，运维方案作为项目建设后期服务交互的组成部分，由小组整体提交。**

## （三）投资编制说明

**说明集成费、监理费、测评费等费用的核算依据。**

# 附加说明：

**申报书应附加用EXCEL编写的经费明细表，主要包括预算总表、产品购置、应用软件开发、配套工程和其它相关费用等五个子表，申报单位应按需填写，具体形式和内容请参考“经费明细表”的模板。**