` **记录编号：$项目编号$-GD01**

**信息系统基本情况调查表**

|  |  |
| --- | --- |
| **系统名称：** | **$项目名称$** |
| **被测单位：** | **$被测单位$** |
| **测评单位：** | **上海计算机软件技术开发中心** |
| **填写日期：** | **$测评准备末日$** |

目录

[表1-1.单位基本情况 1](#_Toc36656955)

[表1-2.安全相关人员名单 3](#_Toc36656956)

[表1-3.物理环境情况 4](#_Toc36656957)

[表1-4.信息系统基本情况 5](#_Toc36656958)

[表1-5.信息系统承载业务（服务）情况 6](#_Toc36656959)

[表1-6.信息系统网络结构（环境）情况 7](#_Toc36656960)

[表1-7.外联线路及设备端口（网络边界）情况 8](#_Toc36656961)

[表1-8.网络设备情况 9](#_Toc36656962)

[表1-9.安全设备情况 10](#_Toc36656963)

[表1-10.服务器/存储设备情况 12](#_Toc36656964)

[表1-11.终端/感知设备/现场设备情况 14](#_Toc36656965)

[表1-12.数据库管理系统情况 15](#_Toc36656966)

[表1-13.系统软件情况 16](#_Toc36656967)

[表1-14.应用系统软件/系统管理平台/中间件情况 17](#_Toc36656968)

[表1-15.关键数据类别 18](#_Toc36656969)

[表1-16.数据备份情况 21](#_Toc36656970)

[表1-17.安全管理中心情况 22](#_Toc36656971)

[表1-18.密码产品情况 23](#_Toc36656972)

[表1-19.应用系统软件处理流程（多表） 24](#_Toc36656973)

[表1-20.业务数据流程（多表） 25](#_Toc36656974)

[表1-21.管理文档情况调查 26](#_Toc36656975)

[表1-22.安全服务 32](#_Toc36656976)

[表1-23.安全威胁情况表 33](#_Toc36656977)

[表1-24 被测系统的最新网络结构图（拓扑图） 35](#_Toc36656978)

# 表1-1.单位基本情况

填表人： 日期：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 单位全称 | $被测单位$ | | | | | 简称 | |  | |
| 单位情况简介 | -- | | | | | | | | |
| 系统简介 | $系统简介$  插入系统相关图片 | | | | | | | | |
| 单位所属类型 | **□**政府机关 **□**国家重要行业、重要领域或重要企事业单位 🗸一般企事业单位 **□**其它类型 | | | | | | | | |
| 单位地址 | $被测单位地址$ | | | | | | | | |
| 邮政编码 | $被测单位邮编$ | | | | | | | | |
| 负责人姓名 | $负责人$ | 办公电话 | $负责人办公电话$ | 部门 | $负责人部门$ | | 职位 | | $负责人职位$ |
| 手机号 | $负责人手机号$ | 邮件地址 | $负责人邮箱$ | | | | |
| 联系人 | $联系人$ | 办公电话 | $联系人办公电话$ | 部门 | $联系人部门$ | | 职位 | | $联系人职位$ |
| 手机号 | $联系人手机号$ | 邮件地址 | $联系人邮箱$ | | | | |
| 上级主管部门 |  | | | | | | | | |

注：情况简介栏，请填写与被测评系统有关的机构内容。

# 表1-2.安全相关人员[[1]](#footnote-1)名单

填表人： 日期：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **人员姓名** | **所属部门** | **负责范围** | **岗位/角色** | **联系方法** |
|  |  |  |  |  |  |

# 表1-3.物理环境[[2]](#footnote-2)情况

填表人： 日期：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **物理环境名称(机房名)** | **物理位置** | **重要程度** | **涉及信息系统** |
|  |  |  |  |  |

# 表1-4.信息系统基本情况

填表人： 日期：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **信息系统名称** | **安全保护等级** | **业务信息安全保护等级** | **系统服务安全保护等级** | **承载业务应用** |
|  | $项目名称$ | $安全保护等级$ | $业务信息安全保护等级$ | $系统服务安全保护等级$ |  |

# 表1-5.信息系统承载业务（服务）情况

填表人： 日期：

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **业务（服务）名称** | **业务描述** | **业务处理信息类别** | **用户数量** | **用户分布范围** | **涉及的应用系统软件** | **是否24小时运行** | **是否可以脱离系统完成** | **重要程度** | **责任部门** |
|  | $项目名称$ |  |  |  |  |  |  |  | 非常重要 |  |

注：1、用户分布范围，写全国、全省、本地区、本单位

2、业务信息类别，写国家秘密信息、非密敏感信息（机构或公民的专有信息）、可公开信息

3、重要程度，写非常重要、重要、一般

# 表1-6.信息系统网络结构（环境）情况

填表人： 日期：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **网络功能区域名称** | **主要功能和作用描述** | **IP网段地址** | **服务器数量** | **终端数量** | **与其连接的其它网络区域** | **网络区域之间的边界设备（互联设备）** | **重要程度** | **备注**  **（责任部门）** |
|  |  |  |  |  |  |  |  |  |  |

注：重要程度填写非常重要、重要、一般

# 表1-7.外联线路及设备端口（网络边界）情况

填表人： 日期：

| **序号** | **外联线路名称**  **(边界名称)** | **所属网络区域**[**[[3]](#footnote-3)**] | **连接对象名称** | **接入线路种类** | **传输速率（带宽）** | **线路接入设备** | **承载主要业务应用** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |

# 表1-8.网络设备情况

填表人： 日期：

| **序号** | **网络设备名称** | **是否虚拟设备** | **系统及版本** | **品牌** | **型号** | **主要**  **用途** | **数量 (台/套)** | **重要程度** | **IP地址** | **是否热备** | **物理**  **位置** | **所属网络区域**[**[[4]](#footnote-4)**] | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

注：重要程度填写非常重要、重要、一般

操作系统填写version信息

# 表1-9.安全设备情况

填表人： 日期：

| **序号** | **安全**  **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌** | **型号** | **主要用途** | **数量 (台/套)** | **重要程度** | **IP地址** | **物理**  **位置** | **所属网络区域**[**[[5]](#footnote-5)**] | **是否热备** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

注：系统及版本信息填写version信息

# 表1-10.服务器/存储设备情况

填表人： 日期：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称**[[6]](#footnote-6) | **是否虚拟设备** | **操作系统**  **及版本** | **应用系统/平台名称** | **数据库管理系统** | **中间件及版本** | **数量** | **重要程度** | **设备型号** | **物理位置** | **IP地址** | **所属网络区域**[**[[7]](#footnote-7)**] | **涉及数据** | **是否热备** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

注：1、重要程度填写非常重要、重要、一般

2、包括数据存储设备

# 表1-11.终端/感知设备/现场设备情况

填表人： 日期：

| **序号** | **终端设备名称** | **是否虚拟设备** | **操作系统/控制软件** | **设备类别和用途** | **数量 （台/套）** | **重要程度** | **型号** | **安装应用系统软件名称** | **涉及数据** | **所属网络区域** | **物理位置** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |

注：1、重要程度填写非常重要、重要、一般

2、包括业务管理终端、业务终端、运维终端，如：专用终端设备以及网管终端、安全设备控制台等

# 表1-12.数据库管理系统情况

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **是否虚拟设备** | **数据库管理系统及版本** | **应用系统/平台名称** | **所属操作系统及名称** | **中间件及版本** | **重要程度** | **软件厂商** | **硬件平台** |
|  |  |  |  |  |  |  |  |  |  |

# 表1-13.系统软件情况

填表人： 日期：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统软件名称** | **版本** | **软件厂商** | **硬件平台** | **涉及应用系统** |
|  |  |  |  |  |  |

注：包括**操作系统、数据库系统**等软件

# 表1-14.应用系统软件/系统管理平台/中间件情况

| **序号** | **应用系统**  **/平台名称** | **主要功能** | **应用软件及版本** | **开发厂商** | **重要程度** | **硬件/软件平台** | **C/S或**  **B/S模式** | **涉及数据** | **现有用户数据** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |

填表人： 日期：

注：包括**中间件、应用系统**等软件

# 表1-15.关键数据类别

填表人： 日期：

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** | **重要程度** | **主要存储设备** | **数据作用** | | | | | | **涉及业务应用** | **是否加密/加密算法** | **数据总量及日增量** | **涉及存储系统及处理设备** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **采集** | **存储** | **处理** | **应用** | **流动** | **销毁** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

注：1、数据安全性要求每项填写“高”、“中”、“低”

2、如本页不够，请续页填写

# 表1-16.数据备份情况

填表人： 日期：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **备份数据名** | **介质类型** | **备份周期** | **保存期** | **是否异地保存/备份场地** | **过期处理方法** | **所属备份系统** |
|  |  |  |  |  |  |  |  |

注：“备份数据名”与表1-14的“数据名称”一致

# 表1-17.安全管理中心情况

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **功能描述** | **系统管理** | **审计管理** | **安全管理** | **集中管控** | **重要程度** |
|  |  |  |  |  |  |  |  |

# 表1-18.密码产品情况

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **生产厂商** | **商密型号** | **密码算法** | **用途** | **数量** |
|  |  |  |  |  |  |  |

# 表1-19.应用系统软件处理流程（多表）

填表人： 日期：

|  |
| --- |
|  |
|  |

注：1、重要应用系统软件应该描述处理流程图，说明主要处理步骤、过程、流向、涉及设备和用户。  
2、如本页不够，请续页。

# 表1-20.业务数据流程（多表）

填表人： 日期：

|  |
| --- |
|  |
|  |

注：1、重要数据应该描绘数据流程图，从数据产生到传输经过的主要设备，再到存储设备等流程。  
2、如本页不够，请续页。

# 表1-21.管理文档情况调查

**a、制度类文档**

填表人： 日期：

| **序号** | **文档主要内容** | **相关文档名称** | **备注** |
| --- | --- | --- | --- |
|  |  |  |  |

注：请在相关文档名称栏填写对应的文档名称，如果相关内容在多个文档中涉及，填写多个文档名称。

**b、记录类文档**

| **序号** | **记录类文档要求** | **备注** |
| --- | --- | --- |
|  | 机房出入登记记录（包括第三方人员） | 有 □无 |
|  | 机房基础设施维护记录 | 有 □无 |
|  | 各类会议纪要或记录（部门内、部门间协调会、领导小组） | 有 □无 |
|  | 各类评审和修订记录（安全管理制度评审和修订记录、体系评审记录等） | 有 □无 |
|  | 人员考核、审查、培训记录（人员录用、人员定期考核）、离岗手续 | 有 □无 |
|  | 各项审批和批准执行记录（来访人员进入机房审批、介质/设备外带审批、系统外联审批等） | 有 □无 |
|  | 安全管理制度收发登记记录 | 有 □无 |
|  | 产品的选型测试结果记录 | 有 □无 |
|  | 系统验收测试记录、报告 | 有 □无 |
|  | 介质归档、查询等的登记记录 | 有 □无 |
|  | 主机系统、网络、安全设备等的操作日志和维护记录 | 有 □无 |
|  | 机房日常巡检记录 | 有 □无 |
|  | 对主机、网络设备和应用软件等的监控记录和分析报告 | 有 □无 |
|  | 恶意代码检测、升级记录和分析报告 | 有 □无 |
|  | 备份过程记录 | 有 □无 |
|  | 变更方案评审记录和变更过程记录 | 有 □无 |
|  | 安全事件处理过程记录 | 有 □无 |
|  | 应急预案培训、演练、审查记录 | 有 □无 |
|  | 其他记录文档 | 有 □无 |

**c. 证据类文档**

| **序号** | **证据类文档要求** | **备注** |
| --- | --- | --- |
|  | 资产清单 | 有 □无 |
|  | 机构安全管理人员岗位名单 | 有 □无 |
|  | 外联单位联系列表 | 有 □无 |
|  | 人员保密协议 | 有 □无 |
|  | 关键岗位安全协议 | 有 □无 |
|  | 候选产品名单 | 有 □无 |
|  | 信息系统定级报告或定级建议书 | 有 □无 |
|  | 系统备案材料 | 有 □无 |
|  | 近期和远期安全建设工作计划、总体建设规划书 | 有 □无 |
|  | 详细设计方案 | 有 □无 |
|  | 工程实施方案 | 有 □无 |
|  | 系统验收测试方案 | 有 □无 |
|  | 系统测试、验收报告 | 有 □无 |
|  | 系统交付清单 | 有 □无 |
|  | 变更方案 | 有 □无 |
|  | 变更申请书 | 有 □无 |
|  | 信息系统定期安全检查的检查表和安全检查报告 | 有 □无 |
|  | 主要设备漏洞扫描报告 | 有 □无 |
|  | 系统异常行为审计分析报告 | 有 □无 |
|  | 机房安全设计和验收方面的文档 | 有 □无 |
|  | 总体安全策略等配套文件的专家论证文档 | 有 □无 |
|  | 与安全服务商或外包开发商签订的服务合同和安全协议 | 有 □无 |
|  | 软件开发设计和用户指南等相关文档（目录体系框架或交换原型系统）、软件测试报告 | 有 □无 |

# 表1-22.安全服务

| **序号** | **安全服务名称[[8]](#footnote-8)** | **安全服务商** | **服务开始日期** | **服务终止日期** |
| --- | --- | --- | --- | --- |
| 1 | 安全测评 | 上海计算机软件技术开发中心 |  |  |

# 表1-23.安全威胁情况表

填表人： 日期：

| **序号** | **安全事件调查** | **调查结果** |
| --- | --- | --- |
|  | 是否发生过网络安全事件 | √没有 □1次/年 □2次/年 □3次以上/年 □不清  安全事件说明：（时间、影响） |
|  | 发生的网络安全事件类型（多选） | □感染病毒/蠕虫/特洛伊木马程序 □拒绝服务攻击 □端口扫描攻击  □数据窃取 □破坏数据或网络 □篡改网页 □垃圾邮件  □内部人员有意破坏 □内部人员滥用网络端口、系统资源  □被利用发送和传播有害信息 □网络诈骗和盗窃 □其它  √其它说明：未发生网络安全事件 |
|  | 如何发现网络安全事件（多选） | √网络（系统）管理员工作检测发现 □通过事后分析发现  √通过安全产品发现 √有关部门通知或意外发现  √他人告知 □其它  其它说明：未发生网络安全事件 |
|  | 网络安全事件造成损失评估 | □非常严重 □严重 □一般 √比较轻微 □轻微 □无法评估 |
|  | 可能的攻击来源 | □内部 √外部 □都有 √病毒 □其他原因 □不清楚  攻击来源说明：未发生网络安全事件 |
|  | 导致发生网络安全事件的可能原因 | □未修补或防范软件漏洞 □网络或软件配置错误  □登录密码过于简单或未修改 □缺少访问控制 √攻击者使用拒绝服务攻击  □攻击者利用软件默认设置 □利用内部用户安全管理漏洞或内部人员作案  □内部网络违规连接互联网 □攻击者使用欺诈方法  □不知原因 □其它  其它说明：未发生网络安全事件 |
|  | 是否发生过硬件故障 | □有 （注明时间、概率） √无  造成的影响是： |
|  | 是否发生过软件故障 | □有 （注明时间、概率） √无  造成的影响是： |
|  | 是否发生过维护失误 | □有 （注明时间、概率） √无  造成的影响是： |
|  | 是否发生过因用户操作失误引起的安全事件 | □有 （注明时间、概率） √无  造成的影响是： |
|  | 是否发生过物理设施/设备被物理破坏 | □有 （注明时间、概率） √无  造成的影响是： |
|  | 有无遭受自然性破坏（如雷击等） | □有 （注明时间、概率） √无  有请注明时间、时间后果 |
|  | 是否发生过莫名其妙的故障 | □有 （注明时间、概率） √无  有请注明时间、时间后果 |

# 表1-24 被测系统的最新网络结构图（拓扑图）

1） 拓扑图

网络结构图要求：

* 应该表示出网络设备、服务器设备和主要终端设备及其名称
* 应该表述出服务器设备的IP地址
* 应该表示网络区域划分等情况
* 应该表示网络与外部的连接等情况
* 应该能够对照网络结构图说明所有业务流程和系统组成

2）拓扑描述：包括拓扑区域划分、边界主要安全防护措施、运维管理方式等

1. 与被测系统有关的管理人员如安全负责人、安全员、安全审计员，技术人员如机房管理员、数据库管理员、系统管理员、应用管理员、网络管理员、系统运维人员，业务人员如业务操作员，其他如人力资源负责人等 [↑](#footnote-ref-1)
2. 物理环境包括主机房、辅机房、办公环境等 [↑](#footnote-ref-2)
3. [] 所属网络区域，需要与表1—6中的‘网络功能区域名称’相对应 [↑](#footnote-ref-3)
4. [] 所属网络区域，需要与表1—6中的‘网络功能区域名称’相对应 [↑](#footnote-ref-4)
5. [] 所属网络区域，需要与表1—6中的‘网络功能区域名称’相对应 [↑](#footnote-ref-5)
6. 设备名称在本报告中应唯一，如xx业务主数据库服务器或xx-svr-db-1。 [↑](#footnote-ref-6)
7. [] 所属网络区域，需要与表1—6中的‘网络功能区域名称’相对应 [↑](#footnote-ref-7)
8. 安全服务包括系统集成、安全集成、安全运维、安全测评、应急响应、安全监测等所有相关安全服务。 [↑](#footnote-ref-8)