**信息系统等级保护测评调研记录**

# 1单位基础信息调查表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 01**单位名称** |  | | | | | | |
| 02单位地址（营业执照上的地址） |  | | | | | | |
| 03**邮政编码** |  | | | 04**行政区划代码** | |  | |
| 05**单位**  **负责人** | 姓 名 |  | | 职务/职称 | |  | |
| 办公电话 |  | | 电子邮件 | |  | |
| 06**责任部门** |  | | | | | | |
| 07**责任部门**  **联系人** | 姓 名 |  | | 职务/职称 | |  | |
| 办公电话 |  | | 电子邮件 | |  | |
| 移动电话 |  | |
| 08**隶属关系** | □1中央 □2省(自治区、直辖市) □3地(区、市、州、盟)  □4县（区、市、旗） □9其他 | | | | | | |
| 09**单位类型** | □1党委机关 □2政府机关 □3事业单位 □4企业 □9其他 | | | | | | |
| 10**行业类别** | □11电信 □12广电 □13经营性公众互联网  □21铁路 □22银行 □23海关 □24税务  □25民航 □26电力 □27证券 □28保险  □31国防科技工业 □32公安 □33人事劳动和社会保障 □34财政  □35审计 □36商业贸易 □37国土资源 □38能源  □39交通 □40统计 □41工商行政管理 □42邮政  □43教育 □44文化 □45卫生 □46农业  □47水利 □48外交 □49发展改革 □50科技  □51宣传 □52质量监督检验检疫  □99其他 | | | | | | |
| 11**信息系统**  **总数** | 个 | 12**第二级信息系统数** | 个 | | 13**第三级信息系统数** | | 个 |
| 14**第四级信息系统数** | 个 | | 15**第五级信息系统数** | | 个 |

# 2 系统基础信息调查表

## 2.1 信息系统情况

**注**：1，主管部门是指对备案单位信息系统负领导责任的行政或业务主管单位或部门。

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 01系统名称 | |  | | | | | | 02系统编号 | | |  |
| 03系统  承载  业务  情况 | 业务类型 | □1生产作业 □2指挥调度 □3管理控制 □4内部办公  □5公众服务 □9其他 | | | | | | | | | |
| 业务描述 |  | | | | | | | | | |
| 04系统  服务  情况 | 服务范围 | □10全国 □11跨省（区、市） 跨个  □20全省（区、市） □21跨地（市、区） 跨个  □30地（市、区）内  □99其它 | | | | | | | | | |
| 服务对象 | □1单位内部人员 □2社会公众人员 □3两者均包括 □9其他 | | | | | | | | | |
| 05系统  网络  平台 | 覆盖范围 | □1局域网 □2城域网 □3广域网 □9其他 | | | | | | | | | |
| 网络性质 | □1业务专网 □2互联网 □9其它 | | | | | | | | | |
| 06系统互联情况 | | □1与其他行业系统连接 □2与本行业其他单位系统连接  □3与本单位其他系统连接 □9其它 独立系统 | | | | | | | | | |
| 07关键产品使用情况 | | 序号 | 产品类型 | 数量 | 使用国产品率 | | | | | | |
| 全部使用 | 全部未使用 | | | 部分使用及使用率 | | |
| 1 | 安全专用产品 |  | □ | □ | | | □ % | | |
| 2 | 网络产品 |  | □ | □ | | | □ % | | |
| 3 | 操作系统 |  | □ | □ | | | □ % | | |
| 4 | 数据库 |  | □ | □ | | | □ % | | |
| 5 | 服务器 |  | □ | □ | | | □ % | | |
| 6 | 其他 |  | □ | □ | | | □ % | | |
| 08系统采用服务情况 | | 序号 | 服务类型 | | 服务责任方类型 | | | | | | |
| 本行业（单位） | | 国内其他服务商 | | | 国外服务商 | |
| 1 | 等级测评 | □有□无 | □ | | □ | | | □ | |
| 2 | 风险评估 | □有□无 | □ | | □ | | | □ | |
| 3 | 灾难恢复 | □有□无 | □ | | □ | | | □ | |
| 4 | 应急响应 | □有□无 | □ | | □ | | | □ | |
| 5 | 系统集成 | □有□无 | □ | | □ | | | □ | |
| 6 | 安全咨询 | □有□无 | □ | | □ | | | □ | |
| 7 | 安全培训 | □有□无 | □ | | □ | | | □ | |
| 8 | 其它 | | □ | | □ | | | □ | |
| 09等级测评单位名称 | | 成都卓越华安信息技术服务有限公司 | | | | | | | | | |
| 10何时投入运行使用 | |  | | | | | | | | | |
| 11系统是否是分系统 | | □是 √否（如选择是请填下两项） | | | | | | | | | |
| 12上级系统名称 | |  | | | | | | | | | |
| 13上级系统所属单位名称 | |  | | | | | | | | | |

## 2.2 信息系统定级情况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 01确定  业务  信息  安全  保护  等级 | 损害客体及损害程度 | | | 级别 |
| □仅对公民、法人和其他组织的合法权益造成损害 | | | □第一级 |
| □对公民、法人和其他组织的合法权益造成严重损害  √对社会秩序和公共利益造成损害 | | | □第二级 |
| □对社会秩序和公共利益造成严重损害  □对国家安全造成损害 | | | □第三级 |
| □对社会秩序和公共利益造成特别严重损害  □对国家安全造成严重损害 | | | □第四级 |
| □对国家安全造成特别严重损害 | | | □第五级 |
| 02确定  系统  服务  安全  保护  等级 | □仅对公民、法人和其他组织的合法权益造成损害 | | | □第一级 |
| □对公民、法人和其他组织的合法权益造成严重损害  √对社会秩序和公共利益造成损害 | | | □第二级 |
| □对社会秩序和公共利益造成严重损害  □对国家安全造成损害 | | | □第三级 |
| □对社会秩序和公共利益造成特别严重损害  □对国家安全造成严重损害 | | | □第四级 |
| □对国家安全造成特别严重损害 | | | □第五级 |
| 03信息系统安全保护等级 | | □第一级 □第二级 □第三级 □第四级 □第五级 | | |
| 04定级时间 | |  | | |
| 05专家评审情况 | | □已评审 □未评审 | | |
| 06是否有主管部门 | | □有 □无（如选择有请填下两项） | | |
| 07主管部门名称 | |  | | |
| 08主管部门审批定级情况 | | □已审批 □未审批 | | |
| 09系统定级报告 | | □有 □ 无 附件名称\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| 填表人： | | | 填表日期：年月日 | |

## 2.3第三级以上信息系统提交材料情况

|  |  |
| --- | --- |
| 1. 系统拓扑结构及说明 | □有 □无 附件名称 |
| 1. 系统安全组织机构及管理制度 | □有 □无 附件名称 |
| 1. 系统安全保护设施设计实施方案或改建实施方案 | □有 □无 附件名称 |
| 1. 系统使用的安全产品清单及认证、销售许可证明 | □有 □无 附件名称 |
| 1. 系统等级测评报告 | □有 □无 附件名称 |
| 1. 专家评审情况 | □有 □无 附件名称 |
| 1. 上级主管部门审批意见 | □有 □无 附件名称 |

# 3 信息系统网络拓扑图

**注：**1、请提供信息系统的最新网络结构图（拓扑图）。

2、请标识出网络设备、服务器设备和主要终端设备品牌和型号。

4、请标识出网络功能区域划分等情况。

5、请标识网络与外部的连接等情况。

6、对照网络结构图说明所有业务流程和系统组成（即对网络拓扑图详细描述）。

7、系统投入时间

8、系统开发公司

9、安全运维公司

# 4 系统功能描述

该系统的功能是：XXXXXXX

# 5 系统业务描述

该系统的业务是：XXXXXX

# 6 运维人员调查表

**注**：以列表形式给出与被测信息系统安全相关的人员，描述项目包括姓名、岗位/角色和联系方式。人员包括但不限于安全主管、系统建设负责人、系统运维负责人、网络（安全）管理员、主机（安全）管理员、数据库（安全）管理员、应用（安全）管理员、机房管理人员、资产管理员、业务操作员、安全审计人员等。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **人员姓名** | **职务/职称** | **所属部门** | **负责范围** | **联系方法** | **备注** |
| 例 | xxx | 系统管理员 | 信息部 | 系统管理监督 | 028-xxxx |  |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |

# 7 机房基础信息

| **序号** | **机房名称** | **物理位置** |
| --- | --- | --- |
| 1 | XX机房 | Xx省xx市xx路xx号xx大楼xx层 |
| 2 |  |  |
| 3 |  |  |

# 8 主机设备及数据库基础信息

**注**：

1.“设备名称”处请填写该设备名称，如：XX系统应用服务器。

2.“操作系统/数据库管理系统”处请填写服务器主机操作系统、数据库操作系统（包括版本），如：AIX6.0，DB2 9.0。

3.请把数据库和数据库服务器分开列出。

4.“重要程度”处请根据实际情况填写：关键、重要或者一般。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **编号** | **设备名称** | **操作系统/数据库管理系统** | **版本** | **数量**  **（台/套）** | **IP地址** | **安装应用软件名称** | **主要业务应用** | **是否热备** | **重要程度** |
| **例** | **Xx服务器** | **Windows server** | **2008** | **x台** | **1.1.1.1** | **是** | **重要** |  |  |
| **例** | **Xx数据库服务器** | **Windows server** | **2008** |  | **1.1.1.2** |  |  |  |  |
| **例** | **Xx数据库** | **SQL**  **server** | **2008** |  | **1.1.1.2** |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

# 9 网络设备基础信息（系统部署在云上这个不用填写）

| **序号** | **设备名称** | **品牌** | **型号** | **物理/逻辑区域** | **IP地址** | **主要用途** | **是否热备** | **数量**  **（台/套）** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 例 | 数据网核心交换机 | 华为 | CLOUDENGINE-12800 | 中心机房/网络核心处 |  |  | 是 | 2 | 非常重要 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

# 10 安全设备基础信息及安全产品销售许可证

注：需要提供每一个安全产品的安全许可证（安全产品：防火墙、vpn、IDS、IPS、上网行为审计、日志审计、堡垒机（运维审计系统）、数据库审计、UTM、防病毒墙、WEB应用防火墙（WAF）、漏洞扫描、加密机、网页防篡改、网闸、抗DDos）

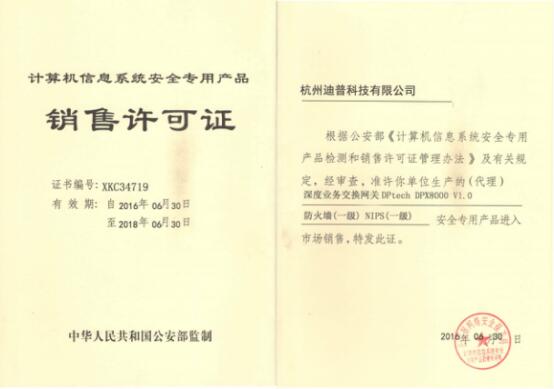
## 10.1 安全产品清单（系统部署在云上这个不需要填写）

| **序号** | **设备名称** | **品牌** | **型号** | **IP地址** | **主要用途** | **部署方式** | **数量**  **（台/套）** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 例 | 防火墙 | DP | DPX8000 | 192.168.1.2 |  |  | 2 | 非常重要 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## 10.2 安全服务产品（针对系统上云）

| **序号** | **安全服务名称** | **安全服务商** | **服务起止时间** | **主要服务内容** |
| --- | --- | --- | --- | --- |
| 例 | 安骑士 | 阿里云 | 2018.01-2019.01 | ECS主机防护 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 10.2 安全产品许可证

例

# 11 应用系统基础信息

| **编号** | **名称** | **主要功能** | **系统架构** | **开发厂商** | **IP地址** | **域名** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 例 | OA系统 | 该系统主要功能是： | B/S | Xx公司 | x.x.x.x | www.xxx.com |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

注意：C/S架构的域名要填写系统域名（即服务器出口的域名一般只有一个）

# 12 管理文档基础信息

制度最基本覆盖面：文件控制、安全检查、人力资源及培训、设备管理、软件开发/外部开发项目管理、机房安全管理、信息分类及管理、网络安全管理、系统安全管理、恶意代码管理、变更控制、备份及介质管理、事件管理、应急预案

## 12.1 制度类文档

|  |  |  |
| --- | --- | --- |
| **序号** | **文档要求** | **文档应具备主要内容** |
| 1 | 机构总体安全方针和政策方面的管理制度 |  |
| 2 | 部门设置、岗位设置及工作职责定义方面的管理制度 |  |
| 3 | 授权审批、审批流程等方面的管理制度 |  |
| 4 | 安全审核和安全检查方面的管理制度 |  |
| 5 | 管理制度、操作规程修订、维护方面的管理制度 |  |
| 6 | 人力资源及安全管理培训制度 | 制度应包括：人员的录用资料调查和保密协议、离岗后的权限访问、安全技能和安全认知的考核、安全意识教育和培训、外部人员访问管理等内容 |
| 7 | 工程实施过程管理方面的管理制度 |  |
| 8 | 产品选型、采购方面的管理制度 |  |
| 9 | 软件开发/外部开发项目管理制度 |  |
| 10 | 测试、验收方面的管理制度 |  |
| 11 | 机房安全管理方面的管理制度 |  |
| 12 | 办公环境安全管理方面的管理制度 |  |
| 13 | 资产、设备、介质安全管理方面的管理制度 |  |
| 14 | 信息分类、标识、发布、使用方面的管理制度 |  |
| 15 | 配套设施、软硬件维护方面的管理制度 |  |
| 16 | 网络和系统安全管理制度 | 网络安全管理制度应包括：对网络安全的配置、网络设备漏洞扫描、日志保存时间、安全策略、升级与打补丁、口令跟新周期等内容。  系统安全管理制度应包括：对系统安全策略、安全配置、系统漏洞扫描、日志管理和日常操作流程等内容。 |
| 17 | 病毒防范方面和密码使用管理制度 | 制度应包括：防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面内容 |
| 18 | 系统变更管理制度 |  |
| 19 | 备份和恢复方面的管理制度 | 制度应包括：备份方式、频度、介质和保存期等内容 |
| 20 | 安全事件报告和处置管理制度 |  |
| 21 | 应急响应方法、应急响应计划等方面的文件 |  |
| 22 | 安全检查制度 | 制度应包括：检查程序、检查周期、检查内容（检查安全技术措施的有效性，安全配置与安全策略的一致性，安全管理制度的执行情况，用户账号情况，系统漏洞情况，系统审计情况） |

## 12.2 记录类文档

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **记录类文档要求** | **相关文档名称** | **主要内容** |
| 1 | 机房出入登记记录（包括第三方人员） |  |  |
| 2 | 机房基础设施维护记录 |  |  |
| 3 | 各类会议纪要或记录（部门内、部门间协调会、领导小组） |  |  |
| 4 | 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） |  |  |
| 5 | 人员考核、审查、培训记录（人员录用、人员定期考核）、离岗手续 |  |  |
| 6 | 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） |  |  |
| 7 | 安全管理制度收发登记记录 |  |  |
| 8 | 产品的选型测试结果记录 |  |  |
| 9 | 系统验收测试记录、报告 |  |  |
| 10 | 介质归档、查询等的登记记录 |  |  |
| 11 | 主机系统、网络、安全设备等的操作日志和维护记录 |  |  |
| 12 | 机房日常巡检记录 |  |  |
| 13 | 对主机、网络设备和应用软件等的监控记录和分析报告 |  |  |
| 14 | 恶意代码检测、升级记录和分析报告 |  |  |
| 15 | 备份过程记录 |  |  |
| 16 | 变更方案评审记录和变更过程记录 |  |  |
| 17 | 安全事件处理过程记录 |  |  |
| 18 | 应急预案培训、演练、审查记录 |  |  |
| 19 | 其他记录文档 |  |  |

## 12.3 证据类文档

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **证据类文档要求** | | **相关文档名称** | **主要内容** |
| 1 | 资产清单 | |  |  |
| 2 | 机构安全管理人员岗位名单 | |  |  |
| 3 | 外联单位联系列表 | |  |  |
| 4 | 人员保密协议 | |  |  |
| 5 | 关键岗位安全协议 | |  |  |
| 6 | 候选产品名单 | |  |  |
| 7 | 信息系统定级报告或定级建设书 | |  |  |
| 8 | 系统备案材料 | |  |  |
| 9 | 近期和远期安全建设工作计划、总体建设规划书 | |  |  |
| 10 | 详细设计方案 | |  |  |
| 11 | 系统建设项目 | 工程实施方案 |  |  |
| 12 | 系统验收测试方案 |  |  |
| 13 | 系统测试、验收报告 |  |  |
| 14 | 系统交付清单 |  |  |
| 15 | 变更方案 | |  |  |
| 16 | 变更申请书 | |  |  |
| 17 | 信息系统定期安全检查的检查表和安全检查报告 | |  |  |
| 18 | 主要设备漏洞扫描报告 | |  |  |
| 19 | 系统异常行为审计分析报告 | |  |  |
| 20 | 机房安全设计和验收方面的文档 | |  |  |
| 21 | 总体安全策略等配套文件的专家论证文档 | |  |  |
| 22 | 与安全服务商或外包开发商签订的服务合同和安全协议 | |  |  |
| 23 | 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形系统）、软件测试报告 | |  |  |

# 13 系统备案申请表

|  |  |
| --- | --- |
| 单位名称 |  |
| 网站域名 |  |
| 负责人 |  |
| 联系方式 |  |
| 办公地址 |  |
| 定级申请 |  |
| 接入商 |  |
| 接入机房及IP |  |
| 机房联系方式 |  |
| 系统内容 | 公章  年 月 日 |
| 审批意见 | 初审意见： |
| 复审意见： |
| 部门意见： |

注意：B/S架构网站域名正常填写，C/S架构这里填写系统名称

# 14 安全威胁情况

| **序号** | **安全事件调查** | **调查结果** |
| --- | --- | --- |
| **1** | 是否发生过网络安全事件 | □没有 □1次/年 □2次/年 □3次以上/年 □不清楚  安全事件说明：（时间、影响） |
| **2** | 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： |
| **3** | 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： |
| **4** | 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 |
| **5** | 可能的攻击来源 | □内部 □外部 □都有 □病毒 □其他原因 □不清  攻击来源说明： |
| **6** | 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： |
| **7** | 是否发生过硬件故障 | □有 （注明时间、概率） □无  造成的影响是： |
| **8** | 是否发生过软件故障 | □有 （注明时间、概率） □无  造成的影响是： |
| **9** | 是否发生过维护失误 | □有 （注明时间、概率） □无  造成的影响是： |
| **10** | 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： |
| **11** | 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： |
| **12** | 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 |
| **13** | 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 |