### 项目编号：（DJCP201XXXX）-XXXXX

**XXX 大学全流程数字化业务系统等级**

**保护对象基本情况调查表**

北京 XXXX 信息技术有限公司2020 年 10 月

**目录**

1. [基本信息表 1](#_bookmark0)
   1. [单位基本信息 1](#_bookmark1)
   2. [被测评单位简介 2](#_bookmark2)
   3. [等级保护对象基本情况 2](#_bookmark3)
2. [机房 3](#_bookmark4)
3. [网络结构 4](#_bookmark5)
   1. [网络拓扑结构图 4](#_bookmark6)
   2. [网络区域划分与功能描述 4](#_bookmark7)
4. [网络互联设备 7](#_bookmark9)
5. [安全设备 9](#_bookmark11)
6. [服务器/存储设备（每个系统设备写在一起） 11](#_bookmark12)
7. [承载的业务情况及业务应用软件 12](#_bookmark13)
   1. [应用软件基本情况 12](#_bookmark14)
   2. [主要业务流程 14](#_bookmark20)
   3. [系统软件基本情况 15](#_bookmark22)
8. [密码产品 16](#_bookmark23)
9. [业务数据情况 16](#_bookmark24)
10. [安全相关人员 17](#_bookmark25)
11. [安全管理文档 18](#_bookmark27)
12. [安全服务 19](#_bookmark28)
13. [安全威胁情况 20](#_bookmark29)

# 基本信息表

## 单位基本信息

#### 填表人：XXX 填表日期：2020 年 10 月 26 日

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **被测评单位** | | | | |
| **单位名称** | XXX 大学 | | | |
| **上级主管部门** | 教育部 | | | |
| **单位地址** |  | | **邮政编码** | 100029 |
| 联系人 | **姓 名** | XXX | **职务/职称** | 工程师 |
| **所属部门** | XXX | **办公电话** | XXX |
| **移动电话** | XXX | **电子邮件** | XXX |

* 1. **被测评单位简介**

XXX 大学创办于 1958 年，原名 XXX 学院

* 1. **等级保护对象基本情况**

**填表人：XXX 填表日期：2020 年 10 月 26 日**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **等级保护对象** | | | | |
| **定级对象 1** | **名称** | XXX 大学全流程数字化业务系统 | **安全保护等级** | 第二级 |
| **业务信息安全保护**  **等级** | 第二级 | **系统服务安全保护等**  **级** | 第二级 |
| **功能描述** | XXX | **备案证书编号** | XXX |

# 机房

**填表人：XXX 填表日期：2020 年 10 月 26 日**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **机房名称** | **物理位置** | **重要程度** |
| 1 | 某校区信息中心机房 | XXXX | 非常重要 |
| 2 | 某校区信息中心机房 | XXX | 非常重要 |

1. **网络结构**[**1**](#_bookmark8)
   1. **网络拓扑结构图:**
   2. **网络区域划分与功能描述**

**填表人：XXX 填表日期：2020 年 10 月 26 日**

表 3-1 网络结构情况

1. 填表说明
2. 网络拓扑示意图应标注目标系统的外部边界连接情况，包括外联系统（如互联网、第三方单位相关系统、下属单位前置系统等）、接入设备及边界防护设备，以及接入链路类型， 并在拓扑图下方以文字形式对外部边界情况进行补充说明，描述相关系统、设备、链路的具体信息（如链路带宽）。
3. 网络拓扑示意应标注安全（功能）区域的划分（如 DMZ 区、核心数据区、用户区、网管区等）以及主要的网络互联及隔离设备的部署情况，并在拓扑图下方以文字形式描述对网络内部结构情况进行补充说明，如区域间采取的安全防护策略等。
4. 网络拓扑示意应标注不同类型服务器（如应用服务器、数据库服务器等）在安全区域中的部署情况，并在拓扑图下方以文字形式描述各区域以及部署的主要服务器设备功能（承载的业务应用软件，参见第六章）与数量。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **网络区域名称** | **区域功能描述** | **IP 网段地址** | **服务器数**  **量** | **终端数量（管**  **理）** | **与其连接的其他网络区域** | **网络区域边界设备** | **重要程度** | **责任部门** |
| 1 | 外联区 | 部署防火墙设 备，实现数据接入和访问控制功  能 | XXXX | - | - | 核心区 | 防火墙 | 非常重要 | 信息中心 |
| 2 | 核心区 | 部署核心交换机，提高核心区  数据交换能力 | XXXX | - | - | 服务器区DMZ 区 | 交换机 | 非常重要 | 信息中心 |
| 3 | DMZ 区 | 部署 Web 应用防火墙和反代服务器，提供 Web 服务，保障内部网  络的安全 | XXXX | 1 | - | 核心区 | 防火墙 | 非常重要 | 信息中心 |
| 4 | 安全监控区 | 部署上网行为管理设备和入侵检测设备，实现上网行为监控和入  侵攻击行为检测的功能 | XXXX | - | - | 核心区 | 交换机 | 非常重要 | 信息中心 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **网络区域名称** | **区域功能描述** | **IP 网段地址** | **服务器数**  **量** | **终端数量（管**  **理）** | **与其连接的其他网络区域** | **网络区域边界设备** | **重要程度** | **责任部门** |
| 5 | 运维管理区 | 部署接入交换 机、堡垒机、漏洞扫描设备、日志审计设备，实现运维管理、漏洞扫描和日志审  计功能 | XXXX | - | 1 | 核心区 | 交换机 | 非常重要 | 信息中心 |
| 6 | 办公区 | 部署运维终端 | XXXX | - | 1 | 核心区 | 交换机 | 非常  重要 | 信息中心 |
| 7 | 服务器区 | 部署服务器设备 | XXXX | 2 | - | 核心区 | 防火墙 | 非常  重要 | 信息中心 |

#### 填表人：XXX 填表日期：2020 年 10 月 26 日

表 3-2 网络外联情况

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序**  **号** | **外联线路名称** | **所属网络区域** | **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** |
| 1. | 教育网-IPV4 | 外联区 | 防火墙 | 互联网 | 1G | 防火墙 | XXX 大学全流程数  字化业务系统 |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 联通 | 外联区 | 防火墙 | 互联网 | 2G | 防火墙 | XXX 大学全流程数  字化业务系统 |  |
| 3 | 教育网-IPV6 | 外联区 | 防火墙 | 互联网 | 1G | 防火墙 | XXX 大学全流程数  字化业务系统 |  |

# 网络互联设备

**填表人：XXX 填表日期：2020 年 10 月 26 日**

表 4-1 网络互联设备基本情况表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **拓扑图中对应**  **序列号** | **设备名称**[**2**](#_bookmark10) | **是否虚拟**  **设备** | **用途** | **网络区域** | **物理区域** | **品牌** | **型号** | **IP 地址** | **数量（ 台/套）** | **重要程度** | **是否热备** |
| 1 | - | 核心交换机 | × | 数据交换 | 核心区 | 某校区 | 华为 | XXX | XXXX | 1 | 非常重要 | 是 |

**填表说明**

1. 可参考如下命名规则：区域\_功能描述\_设备类型\_序号（可选），如互联网接入区边界路由器\_1，或简记为互联网接入路由器。

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **拓扑图**  **中对应序列号** | **设备名称2** | **是否**  **虚拟设备** | **用途** | **网络区域** | **物理区域** | **品牌** | **型号** | **IP 地址** | **数量（ 台/套）** | **重要程度** | **是否热备** |
| 2 | - | 某校区汇聚交换机 | × | 数据交换 | 服务器区 | 某校区 | H3C | XXX | XXXX | 1 | 非常重要 | 是 |
| 3 | - | 服务器接入交换机 | × | 数据交换 | 服务器区 | 某校区 | H3C | XXX | XXXX | 1 | 非常重要 | 是 |
| 4 |  | 运维区接入交换机 | × | 数据交换 | 服务器区 | 某校区 | H3C | XXX | XXXX | 1 | 重要 | 是 |
| 5 | - | 办公区接入交换机 | × | 数据交换 | 办公区 | 某校区 | H3C | XXX | XXXX | 1 | 重要 | 是 |

# 安全设备

#### 填表人：XXX 填表日期：2020 年 10 月 26 日

表 5-1 安全设备基本情况表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **拓扑图中对应序列**  **号** | **设备名称** | **是否虚拟设备** | **用途** | **网络区域** | **物理区域** | **品牌** | **型号** | **IP 地址** | **数量（ 台/套）** | **重要程度** | **是否热备** |
| 1 | - | 出口防火墙 | × | 访问控制 | 外联区 | 某校区 | 迪普 | XXX | XXX | 2 | 非常重要 | 否 |
| 2 | - | 上网行为管理 | × | 上网行为管控 | 安全监控区 | 某校区 | 网康 | XXX | XXX | 1 | 非常重要 | 否 |
| 3 | - | 入侵检测 | × | 入侵行为检测 | 安全监控区 | 某校区 | 启明星辰 | XXX | XXX | 1 | 非常重要 | 否 |
| 4 | - | 服务器区防火墙 | × | 访问控制 | 服务器区 | 某校区 | 启明星辰 | XXX | XXX | 1 | 非常重要 | 否 |
| 5 | - | Web 应用防火墙 | × | 应用层防护 | DMZ 区 | 某校区 | 启明星辰 | XXX | XXX | 1 | 非常重要 | 否 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | - | 堡垒机 | × | 运维管理 | 运维管理区 | 某校区 | 网瑞达 | XXX | XXX | 1 | 非常重要 | 否 |
| 7 | - | 漏洞扫描 | × | 漏洞扫描 | 运维管理区 | 某校区 | 铱迅 | XXX | XXX | 1 | 重要 | 否 |
| 8 | - | 日志审计 | × | 运维管理 | 运维管理区 | 某校区 | 网瑞达 | XXX | XXX | 1 | 重要 | 否 |

# 服务器/存储设备（每个系统设备写在一起）

**填表人：XXX 填表日期：2020 年 10 月 26 日**

表 6-1 主机/存储设备基本情况表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **定级系统** | **设备名称** | **是否虚拟**  **设备** | **物理/逻辑区域** | **操作系统/数据库管理系统** | **版本** | **数量（台**  **/套）** | **中间件/应用软件** | **IP 地址** | **重要程度** | **是否热备** |
| 1 | XXX 大学全流程数字化业务系  统 | 应用服务  器 | × | 服务器区 | CentOS | 7.4 | 1 | XXX | XXX | 非常重要 | 否 |
| 2 | XXX 大学全流程  数字化业务系统 | 数据  库服务器 | × | 服务器区 | CentOS | 7.4 | 1 | XXX | XXX | 非常重要 | 否 |
| 3 | XXX 大学全流程数字化业务系  统 | 反代服务  器 | × | DMZ 区 | Ubuntu | 9.3.0 | 1 | XXX | XXX | 非常重要 | 否 |

表 6-2 终端基本情况表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **物理/逻辑区域** | **操作系统** | **用途** | **数量（台/**  **套）** | **IP 地址** | **重要程度** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **物理/逻辑区域** | **操作系统** | **用途** | **数量（台/**  **套）** | **IP 地址** | **重要程度** |
| 1 | 运维终端 | 办公区 | Windows 10 专业版 | 系统运维 | XXX | XXX | 一般 |

# 承载的业务情况及业务应用软件

* 1. **应用软件基本情况**

**业务应用概述**[**3**](#_bookmark15)

表 7-1 业务应用基本情况表

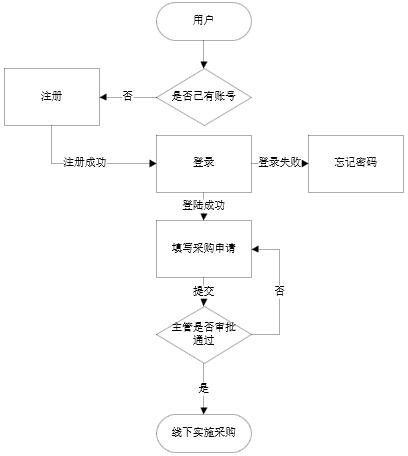
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **业务（服务）名称** | **所属定级系统** | **软件名称** | **主要功能** | **应用模**  **式（B/S 或 C/S）** | **硬件/**  **软件平台** | **自行开**  **发/外包开发**[**4**](#_bookmark16) | **开发商** | **业务数据类别**[**5**](#_bookmark17) | **业务数**  **据保护需求**[**6**](#_bookmark18) | **用户类**  **别及数量** | **重要程度**  [**7**](#_bookmark19) |

**填表说明**

1. 描述信息系统承载的业务应用（实现的主要业务功能或承载的业务使命）。
2. 如果是 外包开发请明确开发商。
3. 如鉴别数据、管理信息和业务数据等，而业务数据可从安全防护需求（保密、完整等）的角度进一步细分。
4. 保密性，完整性等。
5. 相对比较，分别赋值“关键、重要和一般”。

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | 主要面向学校 |  |  |  |  |  |  |  |  |
|  |  |  |  | 教职工，提供 |  |  |  |  |  |  |  |  |
|  |  |  |  | 采购计划申报 |  |  |  |  |  |  |  |  |
| 1 | XXX 大学全流程数字化业务系统 | XXX 大学全流程数字化业务系统 | XXX 大学全流程数字化业务系统 | 审批、采购立项、采购执行管理、合同管理、外贸进口  业务、采购监 | B/S | Linux | 外包开发 | XXX 有限公司 | 用户数据、业务数据 | 完整性、保密性 | 普通用户  /2000;管  理用户/1 | 非常重要 |
|  |  |  |  | 督管理、统计 |  |  |  |  |  |  |  |  |
|  |  |  |  | 归档管理等功 |  |  |  |  |  |  |  |  |
|  |  |  |  | 能。 |  |  |  |  |  |  |  |  |

* 1. **主要业务流程**[**8**](#_bookmark21)



1. 从不同类型业务用户的视角出发，给出关键业务处理流程图，并标注涉及应用组件/模块、主要处理动作，以及关键业务数据在主机设备（程序模块）之间的交换情况。可参考软件开发文档，如软件部署图，开发用例。

## 系统软件基本情况

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统软件名称** | **版本** | **软件厂商** | **硬件平台** | **涉及应用系统** |
| 1 | CentOS | XXX | XXX | Linux | XXX 大学全流程数字化业务系统 |
| 2 | Ubuntu | XXX | XXX | Linux | XXX 大学全流程数字化业务系统 |
| 3 | Oracle | XXX | XXX | Linux | XXX 大学全流程数字化业务系统 |
| 4 | Nginx | XXX | XXX | Linux | XXX 大学全流程数字化业务系统 |
| 5 | Tomcat | XXX | XXX | Linux | XXX 大学全流程数字化业务系统 |

1. **密码产品**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **产品/模块名称** | **生产厂商** | **商密型号** | **使用的密码算法** | **数量** | **用途** |
| 1 | SSL 数字证书 | DigiCert | - | XXX | 1 | 传输加密 |

1. **业务数据情况**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **数据名称** | **数据使用者或管理者及其访问权限** | **数据安全性要求** | | | **数据总量及日增量** | **涉及业务应用** | **涉及存储系统与处理设备** |
| **保密** | **完整** | **可用** |
| 1 | 用户数据 | 用户管理员/读写 | 中 | 中 | 中 | XXX | XXX 大学全流程数  字化业务系统 | Oracle 数据库 |
| 2 | 业务数据 | 普通用户/读写 | 高 | 高 | 中 | XXX | XXX 大学全流程数  字化业务系统 | Oracle 数据库 |
| 3 | 管理数据 | 应用管理员/读写 | 中 | 中 | 高 | XXX | XXX 大学全流程数  字化业务系统 | Oracle 数据库 |
| 4 | 审计数据 | 审计管理员/读 | 中 | 高 | 高 | XXX | XXX 大学全流程数  字化业务系统 | Oracle 数据库、日志  审计系统 |

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

1. **安全相关人员**[**9**](#_bookmark26)

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **人员姓名** | **部门/岗位/角色** | **联系电话** |
| 1 | XXX | XXX | XXX |
| 2 | XXX | XXX | XXX |
| 3 | XXX | XXX | XXX |
| 4 | XXX | XXX | XXX |

1. 人员角色主要包括：安全主管、系统建设负责人、系统运维负责人、物理安全负责人、人事负责人、系统管理员、网络管理员、安全管理员、系统开发人员、应用管理员、档案管理员、资产管理员、各管理员角色可以是多名。

# 安全管理文档

表 11-1 安全管理文档基本情况

|  |  |  |
| --- | --- | --- |
| **序号** | **文档名称** | **主要内容** |
| 1 | 《信息安全策略》 | 机构总体安全方针和政策方面的管理制度。 |
| 2 | 《教职工招聘和考核管理办法》 | 关于员工招聘和考核的管理制度。 |
| 3 | 《校园网核心机房管理办法》 | 关于校园网核心机房环境、消防、操作等方面的管理制度。 |
| 4 | 《恶意代码（病毒）防范管理制度》 | 外来人员病毒防范、内部人员病毒防范方面的管理制度。 |
| 5 | 《安全方案设计管理制度》 | 安全技术框架、总体建设规划和详细设计、方案工程实施过程管理方面的管  理制度。 |
| 6 | 《变更管理制度》 | 系统变更申报、审批、制度变更方案等方面的管理制度。 |
| 7 | 《数据备份与恢复管理规定》 | 关于数据备份和恢复工作流程的管理制度。 |
| 8 | 《网络安全监测预警通报工作制度》 | 关于安全事件监测、预警、应急演练等方面的管理制度。 |
| 9 | 《网络安全事件应急处理流程》 | 启动预案的条件、应急组织构成、应急资源保障、事后教育和 培训等方面的  文件。 |
| 10 | 《机房进入申请》 | 机房进入申请记录。 |
| 11 | 《XX 大学网站（信息服务申请备案表）》 | 外部人员接入受控网络申请记录。 |
| 12 | 《信息系统安全等级保护定级报告》 | 信息系统定级报告。 |
| 13 | 《专家评审意见》 | 信息系统定级专家评审意见。 |

|  |  |  |
| --- | --- | --- |
| 14 | 《上线实施计划》 | 被测评系统上线实施计划。 |
| 15 | 《全流程数字化业务系统操作手册》 | 被测评系统前端用户使用手册。 |
| 16 | 《巡检业务单》 | 机房巡检记录。 |
| 17 | 《安全域划分规范》 | 安全于划分操作手册。 |
| 18 | 《防火墙策略配置要求》 | 防火墙策略配置操作手册。 |
| 19 | 《终端安全管理规范》 | 终端操作手册。 |
| 20 | 《信息系统应急预案》 | 信息系统应急预案。 |
| 21 | 《网络和信息安全事件应急预案》 | 网络和信息安全事件应急预案 |
| 22 | 《校园网应急预案》 | 校园网应急预案。 |
| 23 | 《培训记录》 | 应急预案培训记录。 |

1. **安全服务**

|  |  |  |
| --- | --- | --- |
| **序号** | **安全服务名称 10** | **安全服务商** |
| 1 | 网络安全等级保护测评 | 北京 XXXX 信息技术有限公司 |
| 2 | 网络安全建设 | XXX |

1. **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  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 □邮件附件 □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 □其他其他说明： |
| 3 | 如何发现网络安全事件（多选） | □网络（系统）管理员工作监测发现 □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 □其他其他说明： |
| 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 □不清楚  攻击来源说明： |

|  |  |  |
| --- | --- | --- |
| **序号** | **安全事件调查** | **调查结果** |
| 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被修改  □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 □其他其他说明： |
| 7 | 是否发生过硬件故障 | □有 （注明时间、频率） 无  造成的影响是 |
| 8 | 是否发生过软件故障 | □有 （注明时间、频率） 无  造成的影响是 |
| 9 | 是否发生过维护失误 | □有 （注明时间、频率） 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、频率） 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、频率） 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、频率） 无 |

|  |  |  |
| --- | --- | --- |
| **序号** | **安全事件调查** | **调查结果** |
|  |  | 有请注明时间、事件后果 |
| 13 | 有无发生过莫名其妙的故障 | □有 （注明时间、频率） 无  有请注明时间、事件后果 |