信息系统资源申请登记表（试行）

1. 请申请人如实填写以下信息登记表，并将附件1交由本项目所有涉及的部署实施人员认真阅读。
2. 信息系统名称及入库编号：

|  |
| --- |
| 信息系统登记名称：  信息化项目库入库编号： |

1. 信息系统概述：

|  |
| --- |
|  |

1. 本系统安全责任人、运维责任人、承建单位及联系方式：

|  |
| --- |
| 本系统校内安全责任人及联系方式：  本系统校内运维人员及联系方式：  承建单位，实施工程师的联系电话、电子邮箱（多人可填写多行）： |

1. 本系统后续变更方式（请勾选并填写）：

|  |
| --- |
| 当部门/学院/团队/项目负责人发生变更时，本系统变更情况：  🞎跟随部门/学院，请注明  🞎跟随项目团队，请注明  🞎跟随项目负责人，请注明  🞎其他，请注明 |

1. 本系统功能描述：

|  |
| --- |
|  |

1. 业务信息描述（描述信息系统处理的主要业务信息及涉及的字段信息等）：

|  |
| --- |
|  |

1. 自评估当业务信息受到破坏时对所侵害客体造成具体侵害的确定（说明信息受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成哪些具体的侵害）：

|  |
| --- |
|  |

1. 业务信息受到破坏后对侵害客体的侵害程度的确定（请勾选）：

|  |
| --- |
| 🞎仅对公民、法人和其他组织的合法权益造成损害。  🞎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。  🞎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。  🞎对社会秩序和公共利益造成特别严重损害。  🞎国家安全造成严重损害。  🞎对国家安全造成特别严重损害。 |

1. 系统服务描述（描述信息系统提供哪些服务、服务对象等）：

|  |
| --- |
|  |

1. 自评估当系统服务受到破坏时对所侵害客体造成具体侵害的确定（说明系统服务受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成哪些具体的侵害）：

|  |
| --- |
|  |

1. 系统服务受到破坏后对侵害客体的侵害程度的确定（请勾选）：

|  |
| --- |
| 🞎仅对公民、法人和其他组织的合法权益造成损害。  🞎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。  🞎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。  🞎对社会秩序和公共利益造成特别严重损害。  🞎国家安全造成严重损害。  🞎对国家安全造成特别严重损害。 |

1. 信息系统服务情况（请勾选）：

|  |  |
| --- | --- |
| 服务范围 | 🞎全国 🞎仅本市 🞎区县  🞎跨省市 个 🞎跨市区 个  🞎其他 |
| 服务对象 | 🞎单位内部 🞎社会公众人员  🞎两者均包括 🞎其他 |

1. 本系统内敏感信息内容（请勾选）：

|  |  |  |  |
| --- | --- | --- | --- |
| 敏感信息存储数据类型 | 🞎有 🞎无 |  |  |
| 🞎用户信息  🞎地理信息  🞎交通信息  🞎网站信息  🞎征信信息  🞎邮政信息  🞎公民信息  🞎金融信息  🞎教育信息  🞎健康信息  🞎电子商务  🞎其他未列敏感信息 | 敏感信息拟存储容量（条） | 🞎0～1万  🞎1～10万  🞎10～100万  🞎100万以上 |

1. 填写本系统所用到的中间件、开发包、数据库、服务版本及（如：tomcat 版本8.0，apache 2.4.2 ，jquery 3.1.0，mysql 5.0等）：

|  |
| --- |
|  |

1. 资源需求：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 计算资源需求 | | | | | | | |
| 序号 | 业务官方名称 | 分类需求台数 | 处理器核数 | 内存容量 | 磁盘容量 | 网卡个数 | 操作系统 |
| 例1 | 某某网站 | 2台 | 2C | 8G | 300G | 1块 | Windows2012 |
| 例2 | 某业务系统 | 1台 | 4C | 16G | 500G | 1块 | CentOS7 |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 域名需求 | | | | | | | |
| 1 | .sus.edu.cn，多个域名可换行继续填写。 | | | | | | |

1. 信息系统开放的网络端口及用途信息：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 应用业务描述 | 业务应用范围 | 源IP/域名  第一次开具填写本系统 | 目标IP/域名  第一次开具填写本系统 | 访问协议 | 访问端口 | 有效期限 |
| 例1 | 信息办部门网站 | 所有人员访问 | 0.0.0.0 | 10.10.200.205  xxb.sus.edu.cn或本系统 | tcp | 80 | 开启后至该业务终结 |
| 例2 | 针对信息办网站的后台运维 | 信息办信息员某某某 | 10.10.130.? | http://wzgl.sus.edu.cn/ | tcp | 8080 | 开启后至岗位变更 |
| 例3 | 针对网站群服务器运维 | 网站群运维公司某工程师 | 10.10.20.199 | 本系统 | tcp | 22 | 开启后至运维合同服务期终止日2021-11-30 |
| 例4 | 互联网站点抽取校内站点的数据，满足该业务的数据同步 | 程序接口点对点对接 | 123.52.37.9 | 10.10.201.33 | tcp | 1521 | 开启后至该业务终结 |
| 例5 | 校内业务推送信息至市教委系统 | 程序接口点对点对接 | 本系统 | 219.200.211.86 | tcp | 8080 | 开启后至该业务终结 |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |

注：该表中所填写的内容可由部门填写，也可由承建单位的技术人员协助填写，信息办在接到登记表在研判后开具。

经办人：

日期：

附件1：

上海体育学院系统（网站）上线安全准入须知

为了确保学校上线系统（网站）的安全性，信息中心对上线的系统（网站）进行安全准入检测，满足要求后方可上线。在安全检测前，建设单位须按如下要求进行安全配置并提供相关信息。

一、系统要求：

1、基本要求

（1.1）、系统必须保证为正常上线系统，须已更新至最新。禁止采用失去技术升级的系统（如：windows 2003等）；禁止采用含有已知漏洞的组件、应用程序、框架（如：Struts 2.5 – Struts 2.5.10等）、应用程序服务器、web服务器、数据库服务器和平台定义，以上系统必须按需安装，且要执行安全配置，严禁默认安装。所有的软件应该保持及时更新。

（1.2）、从本机关闭不需要的端口（如：关闭windows netbios等服务），启用并设置本机防火墙如iptable对于访问的源地址进行限制，同时配置相关服务设置类似hosts.allow等策略。严禁关闭软件防火墙功能。

2、数据库要求

（2.1）、数据库和应用系统如在同一台服务器，须采用本机回路进行访问，且要限制好应用与数据库对本机资源占用，避免产生冲突。如前端及数据库分为不同服务器，须设置本机防火墙访问规则，禁止非前端服务器访问数据库网络端口。

（2.2）、使用最低权限的数据库用户作为前端应用所需，禁止具有不必要的额外权限。

3、业务系统要求

（3.1）、系统要求保证系统服务正常与上线系统一致，无各种调试、报错信息（如：断点，printf等调试信息）及注释信息，系统需删除安装文件及系统默认安装的各种例程、文档及管理程序。

（3.2）、对用户输入进行严格有效过滤，防止sql注入、xss跨站脚本、命令执行、crsf跨站请求伪造等，建议采用白名单过滤策略。

（3.3）、控制上传点，对于上传文件类型进行严格控制（禁止用js进行控制），同时上传目录不能有执行权限，原则上不允许有未经登陆验证的上传点。

（3.4）、禁止在HTTP请求中以明文或可逆编码（如base64、url编码等）的形式传递SQL语句到后端程序代入执行，禁止由Web前端直接生成和传递SQL语句到数据库进行执行，数据库查询必须采用预编译和参数结构化查询。如果程序确实需要将SQL语句作为内容（非可执行代码的形式，如学生毕业设计、代码样例等）到后台，请在项目上线交付前书面说明相应的功能代码及位置。

（3.5）、须按照标准端口配置http或https服务，严禁自行设置服务端口不报备。

4、数据要求

（4.1）、对于身份信息、单位职务、财务信息、健康信息、通讯信息等敏感信息禁止在数据库中明文存放。

（4.2）、系统中禁止暴露配置信息（如数据库连接信息），禁止在发布目录存放源码备份文件、当前应用的备份或打包文件以及.git,.svn仓库等。

5、身份认证要求

（5.1）、设置有效的身份认证、会话管理及访问控制机制，防止越权、平行权限及提权等（禁止利用js进行控制及验证）。

（5.2）、密码复杂度要求：系统必须有密码复杂度检查模块，设置有效的验证码或者滑动等手段防止暴力破解，密码长度须大于8位，含字母（大小写）、数字及符号组合，重要系统须采用二次认证。禁止在数据库中明文存放用户密码，需进行带salt的哈希之后入库。对于多次错误登陆进行封堵。如果长期不登陆默认账号应停用处理。

6、发布展示要求

（6.1）、任何展示信息发布须经审核后方可展示，展示信息中涉及个人敏感数据的须经本人同意方可展示，且展示时须做好必要的信息脱敏。

7、其他要求

（7.1）、系统的开发商和应用系统的个人开发者，对于因为程序代码、框架技术以及使用的中间件而产生的应用系统漏洞或bug等程序错误终身负责维护。对于应用系统等级保护检测出现的问题须无条件配合运维者整改，直至检测合格。同时有责任配合运维者进行各种维护。

（7.2）、接到系统安全评测或渗透报告发现的问题，系统使用方须须提供详实可行的整改报告，并积极整改反馈，经信息办验证合格后方可上线。