信息系统、服务器安全自查指引

一、检查更新登记信息

信息系统应在办事大厅上办理“信息系统校内登记”。

检查办事大厅上登记的信息系统详细信息，通过“信息系统校内登记（ 登记/变更/注销 ）”更新发生变更的信息。如系统已完成工作使命，应尽快关停下架，申请注销。

按“二、开展系统自查和整改”指引逐项自查，在网上办事大厅确认已完成“年度自查”。

1.1 办理信息系统校内登记/变更/注销和变更管理员

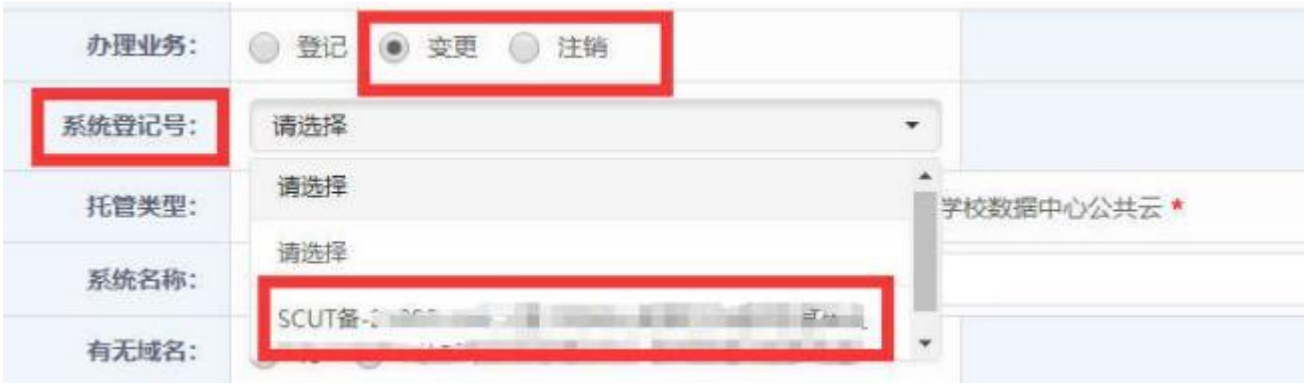
进入网上办事大厅 https://ehall.scut.edu.cn 搜索“信息系统校内登记”。或在网上办事大厅点击 “信息系统建设”

1.1.1 登记

点击“信息系统校内登记（登记/变更/注销）”。

在“办理业务”中选择：登记

1.1.2 变更/注销



在“办理业务”中选择：变更/注销

在“系统登记号”中选择要变更或注销的系统。

1.1.3 变更管理员

点击“信息系统校内登记变更管理员信息申请”。

1.2 查看已登记的信息系统详细信息

进入网上办事大厅 https://ehall.scut.edu.cn 的“服务管理与查询”模块，点击左侧栏“信息系统安全年度自查”， 可以查看到本人或者本单位登记的信息系统列表。点击列表中的“详细”或者导出列表，可以查看信息系 统的详细登记信息。

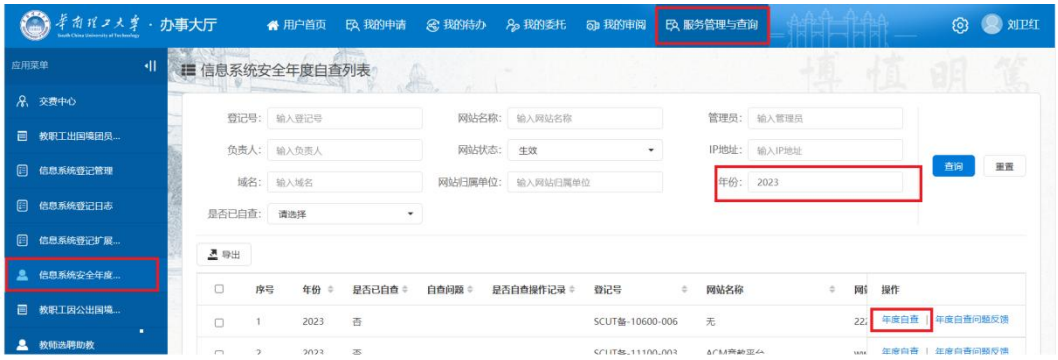
系统管理员可以查看本人登记的信息系统列表。

信息化联络员可以查看本单位登记的信息系统列表。

1.3 开展2023 年度自查

进入已登记的信息系统详细信息，点击“年度自查”。 按“二、开展系统自查和整改”指引逐项 自查，完成自查后，点击“已完成自查”。

如有问题反馈，请点击“年度自查问题反馈”。



二、开展系统自查和整改

2.1 服务器操作系统

（1）操作系统升级最新补丁

必须使用正版操作系统； 补丁包应及时手工更新或设置自动更新，需检查确认自动更新是有效的。

（2）清查操作系统和各类应用账号

应禁止匿名登录，去除guest 账号、已离职离岗管理员账号和其他不必要的管理账号； 不同账户权限分离，避免共享账号； 管理人员更换必须更换密码或取消账号； 强密码要求密码长度12 位以上，包含大小写字母+数字+特殊符号组合，不同帐号单独设密码； 定期更换密码，建议三个月更换一次。

多人共用的公共服务器，应采用 ssh 证书登陆或口令策略强制密码复杂度和强度（如 Ubuntu 配置/etc/pam.d/common-password ， CentOS 配置/etc/pam.d/system-auth 或/etc/security/pwquality.conf ）。

常见存在弱密码的应用有 smb、rdp、telnet、ftp、vnc、ssh、snmp、vmauthd、onvif 等。

常见存在匿名登录的应用有 Memcached、Redis、Elasticsearch、VNC、LDAP、Grafana、Spring Boot Actuator、

Apache Flink、ZooKeeper、 Hadoop yarn rpc、Alibaba Druid、Docker、Jenkins 等。

（3）启用安全软件

建议安装杀毒软件和网站安全狗，并开启防护功能； 应定期更新病毒库、特征库。

（4）定期进行全盘病毒、木马查杀

采用合法的杀毒软件并升级到最新病毒库后进行全盘查杀

（5）关闭不必要的服务端口

应遵循最小开放原则，配置防火墙开放策略。通过Windows 防火墙、Linux iptables/Firewall 配置，关闭不使用的服务端口；远程控制和仅供特定主机、或用户网段的应用服务，端口应配置为仅向该主机IP 或IP 段开放。

（6）删除盗版软件及其他不必要软件

卸载服务器上盗版或不正规渠道下载的软件； 不得在服务器上下载或安装与应用系统运行无关的软件、文件

（7）不得安装内网穿透软件

包括但不限于frp、ew、花生壳等穿透软件，如已使用应立即停止并卸载。如需校外远程管理，应向网络中心申请vpn 通道。

（8）开启服务器日志记录，留存不少于180天的日志； 指定人员定期进行日志审计，审计周期要求见3.1。

（9）做好“虚拟货币挖矿”防范措施，具体要求见：

https://open.work.weixin.qq.com/wwopen/mpnews?mixuin=MpfSCAAABwAJjnAgAAAUAA&mfid=WW0315-nQLXHQAABwCNST5RgoNmMwxjwcT64&idx=0&sn=0ac953673fba5bf56afc5cbbba004987

2.2 数据库

数据库，包括但不限于oracle、mysql、mssql、Redis、mongodb、postgres 等

（1）数据库应升级最新补丁

必须使用正版数据库；补丁包应及时手工更新或设置自动更新，需检查确认自动更新是有效的

（2）清查数据库账号

应去除不必要的账号； 不同账户权限分离，采取最小权限分配策略；管理人员更换必须更换密码； 强密码要求密码长度8 位以上，包含大小写字母+数字+特殊符号组合，不同帐号单独设密码。

（3）定期进行数据库备份

（4）开启数据库日志记录，留存不少于180天的日志； 指定人员定期进行日志审计，审计周期要求见3.1。

（5）配置数据库端口访问限制

仅允许对应应用服务器访问该数据库端口。

（6）重要数据应进行异机备份，并做数据恢复测试。

2.3 信息系统

（1）信息系统的应用软件、中间件应升级最新补丁

必须使用正版应用软件和中间件； 补丁包应及时手工更新或设置自动更新，需检查确认自动更新是有效的。升级 Web 应用到最新版本，如PHP、Apache、Ngnix、Tomcat、Struts2、Weblogic、Shiro，无法实施

的可配置版本漏洞的规避措施，升级和配置前建议先确认应用 Web 系统的兼容性。

（2）开启信息系统的应用软件、中间件日志记录，留存不少于 180天的日志； 指定人员定期进行日志审计，审计周期要求见3.1。

（3 ）清查存在本地认证账号

删除已过期用户、已离职离岗管理员账号；强制所有账号必须使用强密码。已集成学校统一认证的系统，本校学生、教职工用户必须使用学校统一认证，不得并行使用本地认证。

（4 ）关闭不必要的应用模块和页面

删除默认站点配置； 因开发模板或开源代码自带或版本变更遗留，使系统存在不必要的应用模块和页面（特别是登录页面），请务必要求开发人员排查并删除此类应用模块和页面。

（5 ）严格控制用户访问权限

请务必要求开发人员排查所有非公开页面是否都做了访问权限控制。

（6 ）检查信息系统内容

隐藏应用、中间件版本号；隐藏错误信息；检查系统跳转链接，删除已过期或作废的跳转链接； 公开发布内容，必须严格执行先审后发； 不得公开发布个人信息、单位内部信息。

（7 ）限制目录属性

（8 ）检查系统开发者或维护者是否使用代码管理平台，监督其修改默认配置、并严格访问控制策略。

（9 ）重要业务系统应进行异机备份，并做系统恢复测试。

2.4 信息系统第三方开发、运维服务管理

应对第三方开发、运维服务公司开展以下管理检查：

（1 ）第三方公司不得将系统数据传输至校外服务器，校内数据必须经过脱敏后方可用于开发测试；

（2 ）第三方公司不得将系统代码上传至境外代码管理平台，如使用国内或本地代码管理平台，必须修改默认配置、并严格配置访问控制策略；

（3）涉及招生、教学、宣传或全校学生或教职工信息的系统为重要系统，应与第三方开发和运维服务公司，及接触核心数据的服务人员签订安全保密协议。

三、其他

3.1 审计周期要求

校级重要系统，每周至少审计一次； 一般系统每月至少审计一次； 其他系统每三个月至少审计一次。重保期间，开放校外访问的系统，每日至少审计一次。