# 哈尔滨工程大学涉密信息设备和涉密存储设备

# 安全保密审计报告

编号：BMB/HEU-SJBG-01 版本：V1.05

# 1.总体情况

## 1.1设备基本信息

|  |  |  |  |
| --- | --- | --- | --- |
| 处级单位 |  | 基层单位 |  |
| 涉密计算机保密编号 |  | 密级 |  | 责任人 |  |
| 与计算机连接的外部设施设备保密编号 |  | 密级 |  |
| 与涉密计算机绑定涉密U盘保密编号 |  | 密级 |  |
| 审计时间范围 |  |

## 1.2审计情况概述

审计周期内涉密计算机运行正常。

物理安全审计概述：环境未发生变化，设备安全正常，介质使用正常。

运行安全审计概述：重要数据备份正常，计算机未感染病毒，打印输出登记完整，刻录输出登记完整，数据流入流出登记完整，便携式计算机使用正常，软件部署正常。

信息安全审计概述：身份鉴别正常，端口访问控制登记完整，电磁泄露发射防护正常，系统安全性能检测正常，三合一策略正常，主机审计策略正常，桌面防护策略正常，操作系统策略正常，防病毒软件策略正常，数据库备份正常，未出现违规情况。

# 2.审计方法

按照《哈尔滨工程大学涉密信息系统、涉密信息设备和涉密存储设备安全保密策略》要求，核对设备《涉密信息设备全生命周期使用登记簿（打印、刻录、复印）》、《涉密信息设备全生命周期使用登记簿（端口、管理员KEY、中间机）》、审计日志和其他相关登记记录。

# 3.物理设备安全审计

## 3.1物理和环境安全审计

### 3.1.1审计内容

核查涉密信息设备和涉密存储设备所在场所的物理环境、涉密设备与非涉密设备、偶然导体的距离，安防设施的运转。

### 3.1.2审计结果

涉密场所未发生变化，设备摆放距离符合要求，安防设施运转正常。

## 3.2通信和传输安全审计

### 3.2.1审计内容

核查密码保护措施的使用情况，红黑电源隔离插座、视频干扰仪使用情况。

### 3.2.2审计结果

涉密场所未发生变化，设备摆放距离符合要求，安防设施运转正常。

## 3.3信息设备安全审计

### 3.3.1审计内容

核查设备涉密设备台账、《哈尔滨工程大学涉密信息设备确定审批表》、《哈尔滨工程大学涉密信息设备变更审批表》、《哈尔滨工程大学涉密信息设备维修保密审批表》、《哈尔滨工程大学涉密信息设备维修保密协议》、《哈尔滨工程大学涉密信息设备维修过程记录单》、《哈尔滨工程大学涉密信息设备报废审批表》、《哈尔滨工程大学涉密载体销毁审批表》和《哈尔滨工程大学涉密载体销毁清单》。

### 3.3.2审计结果

设备台账信息准确、完整、账物相符，各类审批表齐全，均已存储全生命周期档案。

## 3.4存储设备安全审计

### 3.4.1审计内容

核查《哈尔滨工程大学涉密存储介质（U盘）汇总表》、《哈尔滨工程大学涉密存储介质（移动硬盘）汇总表》、《哈尔滨工程大学涉密计算机KEY汇总表》，核查介质存放、存储信息、存储介质使用是否满足要求。

### 3.4.2审计结果

介质台账信息准确、完整、账物相符，介质存放符合要求，存储信息正常，不存在超越密级存储涉密信息情况。

# 4操作安全审计

## 4.1身份鉴别审计

### 4.1.1审计内容

核查《哈尔滨工程大学涉密信息设备确定审批表》、《哈尔滨工程大学涉密信息设备变更审批表》，该计算机是否为多人共用，是否划分用户权限、用户数量设置是否符合要求、是否定期修改密码

### 4.1.2审计结果

用户设置符合要求，多人共用的用户均按照user权限划分，并定期修改密码。

## 4.2访问控制审计

### 4.2.1审计内容

核查三合一系统端口管理记录，与《涉密信息设备全生命周期使用登记簿（端口、管理员KEY、中间机）》端口登记。核查多人共用计算机的用户分区访问权限。

### 4.2.2审计结果

端口管理登记记录完整，内容与三合一日志记录相符，多人共用分区权限正确设置。

## 4.3信息导入安全审计

### 4.3.1审计内容

核查三合一系统文件导入记录、主机审计文件流入流出记录，与《涉密信息设备全生命周期使用登记簿（端口、管理员KEY、中间机）》、《涉密信息设备全生命周期使用登记簿（信息导入审批单）》登记。

### 4.3.2审计结果

信息导入登记记录完整，内容与三合一日志和主机审计日志记录相符。

## 4.4打印审计

### 4.4.1审计内容

核查主机审计系统打印数据与登记记录数据，主机审计系统打印输出记录 次，《涉密信息设备全生命周期使用登记簿（打印、刻录、复印）》打印输出 次。

### 4.4.2审计结果

打印输出登记记录、审批完整，记录内容与审计内容相符，共计打印输出 次。

## 4.5刻录审计

### 4.5.1审计内容

核查主机审计系统刻录数据与登记记录数据，主机审计系统刻录输出记录 次，《涉密信息设备全生命周期使用登记簿（打印、刻录、复印）》刻录输出 次。

### 4.5.2审计结果

刻录输出登记记录、审批完整，记录内容与审计内容相符，共计刻录输出 次。

# 5应用系统及数据安全审计

## 5.1应用系统安全审计

### 5.1.1审计内容

核查应用系统运行日志、网络安全、数据通讯安全、操作系统安全、数据库安全、应用程序安全、终端安全等是否满足要求。

### 5.1.2审计结果

应用系统运行正常，用户登录记录完整，信息传输完整，操作系统安全、数据完整满足保密要求。

## 5.2信息交换安全策略

### 5.2.1审计内容

核查《涉密信息设备全生命周期使用登记簿（端口、管理员KEY、中间机）》、《哈尔滨工程大学保密技术相关事件报告表》是否发生违规外联事件。

### 5.2.2审计结果

登记记录完整，无违规外联事件发生。

## 5.3数据和数据库安全审计（备份）

### 5.3.1审计内容

核查三合一服务器数据库备份情况，主机审计服务器数据库备份情况，三合一客户端日志备份情况，主机审计客户端日志备份情况。

### 5.3.2审计结果

数据已正常备份，无异常事件发生。

## 5.4开发和维护安全审计

### 5.4.1审计内容

核查开发和维护是否满足数据安全、运行安全、系统安全、物理安全、人员安全等策略。

### 5.4.2审计结果

开发和维护满足数据安全、运行安全、系统安全、物理安全、人员安全等策略，无异常事件发生。

# 6运维安全审计

## 6.1全生命周期档案审计

### 6.1.1审计内容

核查全生命周期档案存档内容与实际是否相符，档案是否体现设备完整生命周期，内容是否符合要求。

### 6.1.2审计结果

全生命周期档案存档内容与实际相符，档案能够体现设备完整生命周期，内容符合要求。

## 6.2计算机病毒与恶意代码防护审计

### 6.2.1审计内容

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 杀毒软件名称 | 软件版本 | 病毒库版本 | 升级时间 | 是否感染病毒 | 病毒类型 | 全盘查杀 |
|  |  |  |  |  |  |  |

### 6.2.2审计结果

瑞星防病毒软件运行正常，进行了2次更新，2次全盘查杀，未发现病毒。

## 6.3外出携带便携式计算机运行审计

### 6.3.1审计内容

核查计算机系统日志与《哈尔滨工程大学携带涉密信息设备和涉密存储设备外出保密审批表》、《哈尔滨工程大学涉密涉密信息设备和涉密存储设备外出操作记录及归还检查登记表》、《涉密信息设备全生命周期使用登记簿（端口、管理员KEY、中间机）》、《涉密信息设备全生命周期使用登记簿（打印、刻录、复印）》。

### 6.3.2审计结果

外出携带审批登记与实际相符，带出前、带回后检查记录完整、详实，各类登记簿登记、审批完整。

## 6.4软件部署审计

### 6.4.1审计内容

核查学校《涉密计算机软件白名单》、学院《涉密计算机软件白名单》、《哈尔滨工程大学涉密信息设备变更审批表》，与系统安装软件。

### 6.4.2审计结果

涉密计算机安装软件均在白名单内，未发现违规操作。

## 6.5三合一策略审计（三合一、主机审计、桌面防护）

### 6.5.1审计内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全产品策略 | 涉密中间机 | 涉密台式机 | 涉密输出机 | 涉密便携机 |
| PCMCIA接口卡 | 禁用使用 | 禁用使用 | 允许使用 | 禁用使用 |
| SCSI及RAID控制器 | 允许使用 | 允许使用 | 允许使用 | 允许使用 |
| CDROM驱动器 | 允许使用 | 禁用使用 | 允许使用 | 禁用使用 |
| 智能卡 | 允许使用 | 允许使用 | 允许使用 | 允许使用 |
| COM/LPT口 | 禁用使用 | 禁用使用 | 允许使用 | 禁用使用 |
| 图像设备 | 允许使用 | 禁用使用 | 允许使用 | 禁用使用 |
| 打印机 | 禁用使用 | 禁用使用 | 允许使用 | 禁用使用 |
| 单导设备 | 允许使用 | 允许使用 | 允许使用 | 允许使用 |
| 未知设备 | 允许使用 | 允许使用 | 允许使用 | 允许使用 |
| USB-打印机 | 禁用使用 | 禁用使用 | 允许使用 | 禁用使用 |

核实以上策略是否按要求配置。

### 6.5.2审计结果

三合一策略均按要求进行配置，未进行调整，系统运行正常。

## 6.6主机审计策略审计

### 6.6.1审计内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全产品策略 | 涉密中间机 | 涉密台式机 | 涉密输出机 | 涉密便携机 |
| 主机状态监控 | 策略状态 | 启用 | 启用 | 启用 | 启用 |
| 策略名称 | 主机状态策略 | 主机状态策略 | 主机状态策略 | 主机状态策略 |
| 监控项 | 硬件变化、软件变化、自启动变化 | 硬件变化、软件变化、自启动变化 | 硬件变化、软件变化、自启动变化 | 硬件变化、软件变化、自启动变化 |
| 违规开机报警 | 无 | 无 | 无 | 无 |
| 系统日志审计 | 策略状态 | 禁用 | 禁用 | 禁用 | 禁用 |
| 策略名称 | 系统日志监控 | 系统日志监控 | 系统日志监控 | 系统日志监控 |
| 日志库名 | 系统、应用程序 | 系统、应用程序 | 系统、应用程序 | 系统、应用程序 |
| 日志类型 | 错误、警告、审核失败、审核成功 | 错误、警告、审核失败、审核成功 | 错误、警告、审核失败、审核成功 | 错误、警告、审核失败、审核成功 |
| 日志来源 | 所有来源 | 所有来源 | 所有来源 | 所有来源 |
| 运行规则 | 无 | 无 | 无 | 无 |
| 处理措施 | 无 | 无 | 无 | 无 |
| 文件操作监控 | 策略状态 | 禁用 | 禁用 | 禁用 | 禁用 |
| 策略名称 | 文件操作 | 文件操作 | 文件操作 | 文件操作 |
| 对象类型 | 文件、文件夹 | 文件、文件夹 | 文件、文件夹 | 文件、文件夹 |
| 磁盘范围 | 所有 | 所有 | 所有 | 所有 |
| 监控路径 | 所有 | 是 | 是 | 是 | 是 |
| 子目录 | 否 | 否 | 否 | 否 |
| 操作类型 | 创建、修改、重命名、删除 | 创建、修改、重命名、删除 | 创建、修改、重命名、删除 | 创建、修改、重命名、删除 |
| 文件类型 | 所有 | 所有 | 所有 | 所有 |
| 操作进程 | 无 | 无 | 无 | 无 |
| 监控方式 | 允许 | 是 | 是 | 是 | 是 |
| 记录日志 | 是 | 是 | 是 | 是 |
| 文件流入流出 | 策略名称 | 文件流入流出策略 | 文件流入流出策略 | 文件流入流出策略 | 文件流入流出策略 |
| 策略状态 | 启用 | 启用 | 启用 | 启用 |
| 监控排除列表 | 无 | 无 | 无 | 无 |
| 文件打印监控 | 策略名称 | 文件打印策略 | 文件打印策略 | 文件打印策略 | 文件打印策略 |
| 策略状态 | 启用 | 启用 | 启用 | 启用 |
| 审计模块 | 记录日志 | 记录日志 | 记录日志 | 记录日志 |
| 账户变更审计 | 策略状态 | 禁用 | 禁用 | 禁用 | 禁用 |
| 策略名称 | 账户变更审计 | 账户变更审计 | 账户变更审计 | 账户变更审计 |
| 模块状态 | 启用 | 启用 | 启用 | 启用 |
| 补丁安装审计 | 策略名称 | 补丁监控策略 | 补丁监控策略 | 补丁监控策略 | 补丁监控策略 |
| 策略状态 | 启用 | 启用 | 启用 | 启用 |
| 补丁检测 | 启用 | 启用 | 启用 | 启用 |
| 补丁类型 | 系统、office、ie | 系统、office、ie | 系统、office、ie | 系统、office、ie |
| 刻录审计 | 策略名称 | 光盘刻录策略 | 光盘刻录策略 | 光盘刻录策略 | 光盘刻录策略 |
| 策略状态 | 启用 | 启用 | 启用 | 启用 |
| 非法外接检测 | 策略名称 | 非法外接策略 | 非法外接策略 | 非法外接策略 | 非法外接策略 |
| 策略状态 | 禁用 | 禁用 | 禁用 | 禁用 |
| TCP地址 | 202.118.177.201 | 202.118.177.201 | 202.118.177.201 | 202.118.177.201 |

核实以上策略是否按要求配置。

### 6.6.2审计结果

主机审计策略均按要求进行配置，未进行调整，系统运行正常。

## 6.7桌面防护策略审计

### 6.7.1审计内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全产品策略 | 涉密计算机 | 涉密输出机 | 涉密中间机 | 涉密便携式计算机 |
| 采用USB KEY与口令相结合的方式进行身份鉴别 | 🗸 | 🗸 | 🗸 | 🗸 |
| 空闲操作时间超过10分钟，进行重鉴别 | 🗸 | 🗸 | 🗸 | 🗸 |
| 鉴别尝试次数达到5次，对用户账户进行锁定，只能由计算机安全保密管理员恢复 | 🗸 | 🗸 | 🗸 | 🗸 |
| 所有登录情况均记录日志 | 🗸 | 🗸 | 🗸 | 🗸 |
| 当用户连续输入5次错误PIN码后，用户密钥锁定 | 🗸 | 🗸 | 🗸 | 🗸 |
| 用户拔掉Key时计算机进入锁屏状态 | 🗸 | 🗸 | 🗸 | 🗸 |
| 禁止强行结束客户端 | 🗸 | 🗸 | 🗸 | 🗸 |
| 禁止卸载客户端 | 🗸 | 🗸 | 🗸 | 🗸 |
| 禁止客户端调试日志 | 🗸 | 🗸 | 🗸 | 🗸 |
| 客户端随操作系统自动启动 | 🗸 | 🗸 | 🗸 | 🗸 |
| PIN码长度最少10位字符，并且至少包含一个数字，一个英文字母 | 🗸 | 🗸 | 🗸 | 🗸 |

核实以上策略是否按要求配置。

### 6.7.2审计结果

 桌面防护策略均按要求进行配置，未进行调整，系统运行正常。

## 6.8操作系统策略审计（密码、账户、审核、日志存储、服务）

### 6.8.1审计内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 终端系统安全配置策略 | 涉密计算机 | 涉密输出机 | 涉密中间机 | 涉密便携式计算机 |
| 查看系统安装时间是否与setupapi.log创建时间一致。 | 🗸 | 🗸 | 🗸 | 🗸 |
| 以NTFS格式分区，多人共用设定访问权限。 | 🗸 | 🗸 | 🗸 | 🗸 |
| 关闭系统自动还原。 | 🗸 | 🗸 | 🗸 | 🗸 |
| 安装屏保软件，屏保时间为10分钟，屏保解除需要密码。 | 🗸 | 🗸 | 🗸 | 🗸 |
| 删除多余系统账号仅保留使用administrator和用户账号，禁用guest账号，删除其他账号。 | 🗸 | 🗸 | 🗸 | 🗸 |
| 事件日志配置。安全日志最大值 100096KB系统日志大小最大值 1000096KB应用程序日志大小最大值 100096KB | 🗸 | 🗸 | 🗸 | 🗸 |
| 本地安全策略-密码策略：设置密码长度最小值10位；密码最长使用期限7天；密码最短使用期限1天；强制密码历史1个记住的密码。 | 🗸 | 🗸 | 🗸 | 🗸 |
| 本地安全策略-账户锁定策略：账户锁定阈值5次无效登陆；账户锁定时间30分钟；重置账户锁定计数器30分钟之后。 | 🗸 | 🗸 | 🗸 | 🗸 |
| 本地安全策略-审核策略：审核策略更改 成功，失败审核登陆时间 成功，失败审核对象访问 无审核过程追踪 无审核目录服务访问 无审核特权使用 成功，失败审核系统事件 成功，失败审核账户登录事件 成功，失败审核账户管理 成功，失败 | 🗸 | 🗸 | 🗸 | 🗸 |
| 禁用Server（共享服务） | 🗸 | 🗸 | 🗸 | 🗸 |

核实以上策略是否按要求配置。

### 6.8.2审计结果

操作系统策略均按要求进行配置，未进行调整，系统运行正常。

## 6.9防病毒软件策略审计（配置）

### 6.9.1审计内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全产品策略 | 涉密台式机 | 涉密便携机 | 涉密中间机 | 非涉密中间机 |
| 基本设置 | 基本选项 | 开机自动运行 | 是 | 是 | 是 | 是 |
| 启用安全消息中心 | 是 | 是 | 是 | 是 |
| 安全保护 | 病毒查杀 | 文件类型 | 所有文件 | 所有文件 | 所有文件 | 所有文件 |
| 扫描时进入压缩包 | 所有 | 所有 | 所有 | 所有 |
| 病毒处理方式 | 自动隔离 | 自动隔离 | 自动隔离 | 自动隔离 |
| 监控模式 | 全盘 | 全盘 | 全盘 | 全盘 |
| 垃圾清理 | 消息提醒 | 关 | 关 | 关 | 关 |
| 其它设置 | 关 | 关 | 关 | 关 |
| 杀毒扫描 | 全盘扫描 | 整个系统 | 整个系统 | 整个系统 | 整个系统 |
| 闪电查杀 | 核心区域 | 核心区域 | 核心区域 | 核心区域 |

金山毒霸策略

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全产品策略 | 涉密台式机 | 涉密便携机 | 涉密中间机 | 非涉密中间机 |
| 快速查杀 | 引擎级别 | 中 | 中 | 中 | 中 |
| 病毒处理方式 | 自动 | 自动 | 自动 | 自动 |
| 扫描范围 | 默认 | 默认 | 默认 | 默认 |
| 记录日志 | 是 | 是 | 是 | 是 |
| 声音报警 | 是 | 是 | 是 | 是 |
| 全盘查杀（含文件监控） | 引擎级别 | 中 | 中 | 中 | 中 |
| 病毒处理方式 | 自动 | 自动 | 自动 | 自动 |
| 扫描范围 | 无排除 | 无排除 | 无排除 | 无排除 |
| 记录日志 | 是 | 是 | 是 | 是 |
| 声音报警 | 是 | 是 | 是 | 是 |

瑞星2011策略

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全产品策略 | 涉密台式机 | 涉密便携机 | 涉密中间机 | 非涉密中间机 |
| 常规设置 | 开机自运行 | 是 | 是 | 是 | 是 |
| 加入云安全 | 否 | 否 | 否 | 否 |
| 扫描设置 | 流行病毒 | 启用 | 启用 | 启用 | 启用 |
| 启发式扫描 | 启用 | 启用 | 启用 | 启用 |
| 变频杀毒 | 启用 | 启用 | 启用 | 启用 |
| 压缩包扫描 | 不大于100M | 不大于100M | 不大于100M | 不大于100M |
| 病毒处理方式 | 自动 | 自动 | 自动 | 自动 |
| 发现病毒告警 | 启用 | 启用 | 启用 | 启用 |
| 病毒防御 | 监控等级 | 高级 | 高级 | 高级 | 高级 |
| 流行病毒扫描 | 启用 | 启用 | 启用 | 启用 |
| 启发式扫描 | 启用 | 启用 | 启用 | 启用 |
| 病毒处理方式 | 自动 | 自动 | 自动 | 自动 |
| 发现病毒告警 | 启用 | 启用 | 启用 | 启用 |
| 定时任务 | 快速扫描 | 核心区域 | 核心区域 | 核心区域 | 核心区域 |
| 全盘扫描 | 整个系统 | 整个系统 | 整个系统 | 整个系统 |

瑞星V16/V17策略

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全产品策略 | 涉密台式机 | 涉密便携机 | 涉密中间机 | 非涉密中间机 |
| 常规设置 | 开机自动启动 | 是 | 是 | 是 | 是 |
| 病毒扫描设置 | 仅程序及文档 | 是 | 是 | 是 | 是 |
| 处理方式 | 自动 | 自动 | 自动 | 自动 |
| 实时防护 | 防护级别 | 中 | 中 | 中 | 中 |
| 监控文件类型 | 所有 | 所有 | 所有 | 所有 |
| 处理方式 | 自动 | 自动 | 自动 | 自动 |
| 监控间谍文件 | 是 | 是 | 是 | 是 |
| 优化设置 | 关 | 关 | 关 | 关 |

360杀毒策略

核实以上策略是否按要求配置。

### 6.9.2审计结果

杀毒软件策略均按要求进行配置，未进行调整，系统运行正常。

## 6.10系统安全性能检测审计

### 6.11.1审计内容

核查自检自查记录，是否按时间要求进行自查、自查内容是否如实填写，自查，自查问题是否及时整改。

### 6.11.2审计结果

自检自查内容属实、记录完整、能够体现发现问题和进行整改。

# 7.主要存在问题及整改措施

责任人签字：

计算机安全保密管理员签字：

 审计时间：