厦门华锐莱普顿学校
CHIWAY REPTON SCHOOL XIAMEN

信息安全管理制度

Information Security Management Institution

2022-12-10

厦门华锐莱普顿学校

信息安全管理制度

（有效期：自发布之日起有效）

编制 _____ 日期 _____

审核 _____ 日期 _____

批准 _____ 日期 _____

修订记录

日　期	修订状态	修改内容	修改人	审核人	批准人

目录

一、 目的

为加强厦门华锐莱普顿学校信息安全管理工作，维护学校信息安全，保证网络环境的稳定，根据《网络安全法》、《网络安全等级保护 2.0》制度及相关法律法规及学校相关规章制度，特制定本管理制度。

二、 适用范围

本管理制度适用于厦门华锐莱普顿学校的内部管理。

三、 信息安全总体方针和安全策略

(一) 学校网络安全以满足信息系统运行要求，遵守相关规程，实施等级保护及风险管理，确保网络安全，实现持续改进。以信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断为总体安全方针。

(二) 本制度适用于厦门华锐莱普顿学校网络安全工作。由后勤部 IT 对该项工作的落实和执行进行监督，学校所属部门配合后勤部 IT 对本制度的有效性进行持续改进。

(三) 以谁主管谁负责为原则，加强对网络安全的管理。

(四) 建立一套关于物理、主机、网络、应用、数据、建设和管理等六个方面的安全需求、控制措施及执行程序，并定义相关的安全角色，并对其赋予管理职责。加强对网络安全工作人员的安全意识培训，不断优化系统分布的合理性和有效性。

(五) 安全层面

1. 物理方面：依据实际情况建立机房管理制度，明确机房的出入管理要求，机房介质存放方式，机房设备维护周期及维护方式，机房设备信息保密要求，机房温湿度控制方式等环境要求。明确机房责任人、建立机房管理相关制度、对维护和出入等过程建立记录等方式对机房安全进行保护。
2. 网络方面：从技术角度实现网络的合理分布、网络设备的实施监控、网络访问策略的统一规划、网络安全扫描以及对网络配置文件等必要信息进行定期备份。从管理角度明确网络各个区域的安全责任人，建立网络维护方面相关操作办法，并由相关人员或部门监督执行，确保各信息系统网络运行情况稳定、可靠、正

常的运行。

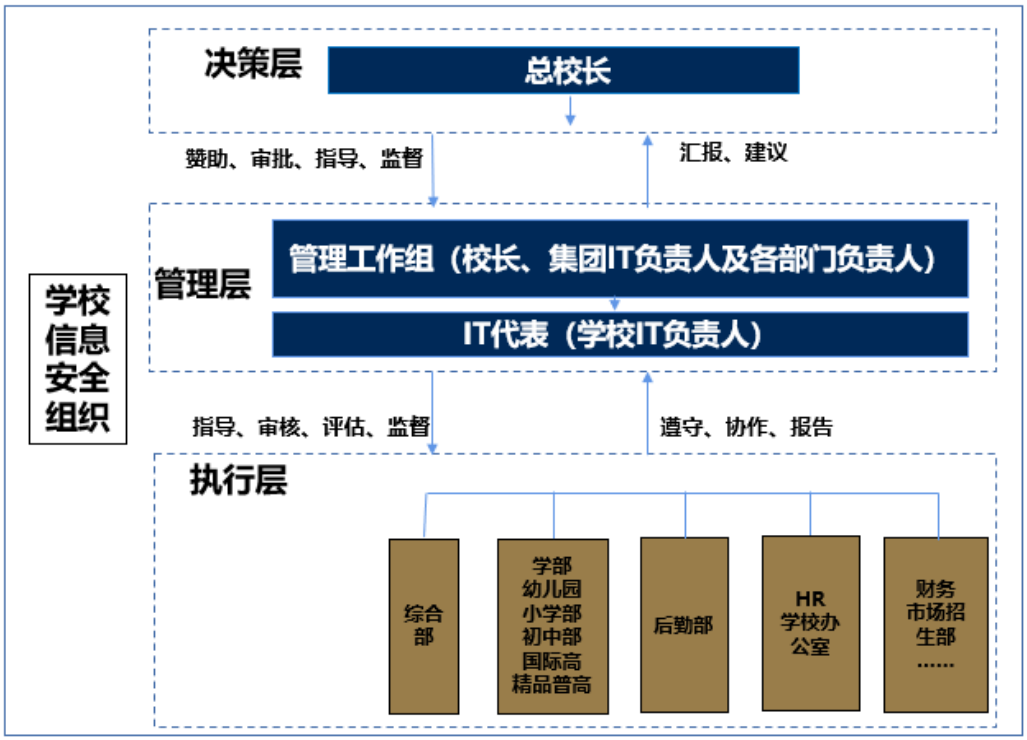
3. 主机方面：各类主机操作系统和数据库系统在满足各类业务系统的正常运行条件下，建立系统访问控制办法、划分系统使用权限、安装恶意代码防范软件并对恶意代码的检查过程进行记录。明确各类主机的责任人，对主机关键信息进行定期备份。
4. 应用方面：从技术角度实现应用系统的操作可控、访问可控、通信可控。从管理角度实现各类相应控制办法的有效执行，建立完善的维护操作规程，明确定期备份内容。
5. 数据方面：对学校的各类业务数据、设备配置信息、总体规划信息等关键数据建立维护办法，并由相关部门或人监督、执行。通过汇报或存储方式实现关键数据的安全传输、存储和使用。
6. 网络安全管理机制：成立网络安全管理主要部门，设立安全主管等主要安全角色，依据网络安全等级保护二级标准（要求），建立信息系统管理办法。
7. 网络安全管理组织：建立安全管理岗位和部门的职责文件，对相关人员的职责进行明确。建立信息发布、变更、审批等流程和制度类文件，增强制度的有效性。建立安全审核和检查的相关制度及报告方式。
8. 人员安全管理要求：对人员的录用、离岗、考核、培训、安全意识教育等方面应通过制度和操作程序进行明确，并形成记录文件。
9. 网络安全等级保护工作及风险评估要求：定期对已备案的信息系统进行等级保护测评，以保证信息系统运行风险维持在较低水平，不断增强系统的稳定性和安全性。
10. 报告安全事件要求：对突发安全事件建立应急预案管理制度和相关操作办法，并定期组织人员进行演练，以保证信息系统在面临突发事件时能够在较短时间内恢复正常的使用。
11. 业务持续性要求：根据对系统的等级测评、风险评估等间接问题挖掘，及时改进信息系统的各类弊端，包括业务弊端，应建立相关改进措施或改进办法，以保证对信息系统的业务持续性要求。

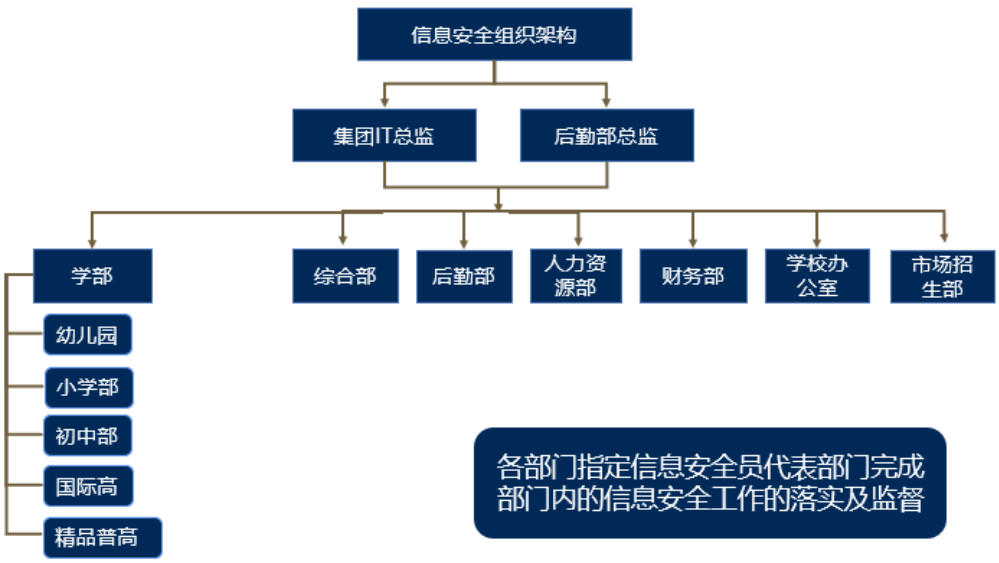
12. 违反网络安全要求的惩罚：建立惩处办法，对违反网络安全总体方针、安全策略的、程序流程和管理措施的人员，依据问题的严重性进行惩罚。

四、 信息安全组织机构和人员管理

(一) 组织机构和人员

学校信息安全组织架构：





成立学校信息安全领导小组，决策层为学校总校长。领导小组是网络安全的最高决策机构，下设办公室挂靠在后勤部 IT 工作组，负责领导小组的日常事务。

领导小组的职责主要包括：根据国家和行业有关网络安全的政策、法律和法规，制定学校网络安全总体策略规划、管理规范和技术标准；确定学校网络安全各有关部门工作职责，指导、监督、落实网络安全工作。

网络安全执行工作由后勤部 IT 人员担任，其主要职责：

1. 贯彻执行信息安全领导小组的决议，协调和规范学校网络安全工作。

2. 根据信息安全领导小组的工作部署，对网络安全工作进行具体安排、落实。

3. 定期组织对网络安全工作制度和技术操作策略进行审查，根据审查结果对网络安全工作制度进行修订，并拟订网络安全总体策略规划，并监督执行。

4. 负责协调、督促各职能部门的网络安全工作，参与信息系统工程建设中的安全规划，监督安全措施的执行。

5. 组织网络安全工作检查，分析网络安全总体状况，提出分析报告和安全风险的防范对策。

6. 负责接受各部门的紧急网络安全事件报告，组织进行事件调查，分析原因、涉及范围，并评估安全事件的严重程度，提出网络安全事件防范措施。

7. 及时向领导小组和上级有关部门报告网络安全事件。

8. 跟踪先进的网络安全技术，组织网络安全知识的培训和宣传工作。

(二)　关键岗位人员管理

1. 信息系统关键岗位人员是指与重要信息系统直接相关的管理人员、网络管理人员、系统管理人员等岗位人员。
2. 重要信息系统，是指涉及学校建设与经营管理、教学管理、学生管理等核心业务且有保密要求的信息系统。
3. 关键岗位人员上岗前必须经学校人事部门进行政治素质审查，工作经历和工作经验考查等，合格者方可上岗。
4. 关键岗位人员有责任保护信息系统的秘密，并以签署保密协议的方式做出安全承诺。
5. 关键岗位人员上岗必须实行“权限分散、不得交叉覆盖”的原则。系统管理人员、网

络管理人员、系统开发人员不得兼任业务操作员；系统开发人员原则上不应兼任系统管理员。

6. 对关键岗位人员应实行定期考查制度，关键岗位人员应定接受安全培训，加强自身安全意识和风险防范意识。
7. 关键岗位人员调离岗位，必须严格办理调离手续，承诺其调离后的保密义务。
8. 关键岗位人员离岗后，必须即刻更换操作密码或注销用户。

五、 网络安全检查

1. 安全检查包括信息系统运维部门自查和负责网络安全的人员定期执行的安全检查。
2. 信息系统运维部门的自查内容应包括业务系统日常运行、系统漏洞和数据备份等情况，自查工作应保留自查结果。自查应至少半年组织一次。
3. 负责网络安全的人员执行的安全检查内容应包括现有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和业务人员自查结果抽查等。安全检查应至少半年组织一次。
4. 自查和安全检查均应在检查之前形成检查表，应严格按照检查表实施检查，检查完毕，记录下所有检查结果。应对检查记录进行归档，只有授权人员可以访问阅读。应对检查结果进行汇总分析，形成安全检查报告，检查报告应对问题进行分析，提出解决建议。
5. 应制定措施防止安全检查结果的非授权散布，只对经过授权的人员通报安全检查结果。
6. 信息系统运维部门应阅读并理解安全检查报告，在网络安全人员的指导下对出现的问题进行整改。负责网络安全的人员应对整改过程进行监督，并将整改结果报送网络安全领导小组。

六、 人员安全管理：

（一） 角色：

人力资源部：负责学校教职工入职、转岗、离职等变动的管理；负责对信息安全违规人员进行沟通处理。

各职能部门：负责本部门员工的信息安全管理；负责本部门第三方人员的信息安全管理；负责本部门员工信息安全教育；负责协助学校关于人员安全管理的相关工作。

（二） 人力资源部职责：

录用前：对任用的教职工、第三方的候选人员进行充分的审查，对关键岗位还应进行背景调查。教职工入职必须签订劳动合同，劳动合同中必须包含对员工应履行的信息安全职责，信息保密要求和违背应承担的责任，必须签署附加保密协议。

录用后：按照组织的信息安全策略定义岗位安全职责，通过书面的岗位职责描述和说明

清晰地传达给教职员工和第三方人员。确保教职员工知悉并遵守《CRS 信息安全管理制度》等安全管理制度的规定。将信息安全知识培训纳入学校统一的培训体系内，定期组织各部门开展信息安全宣传和培训，宣传和培训内容应根据信息安全管理策略与规程、学校的发展与变化，以及信息安全趋势变化进行及时更新，由后勤部 IT 负责具体实施及考核。违反信息安全要求的教职员工和第三方人员将根据学校的员工手册等相关规定进行处分。当教职员工和第三方人员接受可能涉及解除劳动合同和法律诉讼的违规调查时，人力资源部必须暂停其日常工作，及时通知相关的 IT 管理人员停止其在学校内对系统拥有的所有访问权限。

离职后：劳动合同中必须清晰定义雇佣合同终止或变更时间，雇佣双方应承担的责任。根据集团相关政策，重要岗位员工离职时，需签订离职竞业禁止协议。如员工正常离职，按流程办理离职流程，由 IT 管理人员关闭邮箱、禁用或调整人员帐户访问权限。如员工非正常离职，人力资源部将立即通过邮件、电话等方式通知相关的 IT 管理人员，关闭邮箱、禁用或调整人员帐户访问权限。在终止雇佣、合同或协议时，所有教职员工及第三方人员必须按照离职流程至后勤部 IT 归还所领用的学校资产。

七、 第三方人员管理

1. 本办法所述的“第三方”人员包括软件开发商、产品供应商、系统集成商、设备维护商和服务提供商等外来人员。
2. “第三方”人员的访问方式包括现场访问和远程网络访问。
3. “第三方”人员访问重要区域（如机房、重要服务器或设备等），需学校领导审核同意，并在专人的陪同下方可进入。
4. 接待人必须全程陪同 “第三方”人员，告知有关安全管理规定，不应透露与“第三方”工作无关的信息，不得任其自行走动和未经允许使用网站系统的服务器设备。
5. 原则上禁止“第三方”人员携带的电脑接入学校网络系统。
6. 不允许“第三方”人员进行远程网络访问。如确因维护需要远程访问，必须由运维单位批准后方可进行。
7. “第三方”人员维护网络、主机等设备的安全配置时必须符合相应的安全配置标准

中相应规定。

8. 必须防范“第三方”人员带来的以下安全风险：“第三方”人员的物理访问带来的设备、资料盗窃；“第三方”人员的误操作导致各种软硬件故障；“第三方”人员的资料、信息外传导致泄密；“第三方”人员对计算机系统的滥用和越权访问；“第三方”人员给计算机系统、软件留下后门；“第三方”人员对计算机系统的恶意攻击。
9. 未经批准，禁止“第三方”人员私自将移动存储介质接入网站系统，移动存储介质必须在接待人的监控下使用。
10. 未经相关负责人特别许可，“第三方”人员不得在办公区域和机房内摄影、拍照。

八、 安全教育培训管理

(一) 培训分类

1. 结合学校目前的实际情况，网络安全培训分为：入职培训、年度培训、关键岗位（含安全管理员、系统管理员、机房网络管理员等）培训（包含关键岗位的入岗培训、关键岗位的年度培训）。
2. 入职培训专门针对新进教职工和新调入关键岗位的员工举办，旨在帮助教职工了解学校网络安全的各项要求、尽快适应工作需要的培训。
3. 年度培训指不脱离工作岗位，在工作中接受的网络安全类培训。旨在提高教职工网络安全综合素质，更新教职工网络安全技能，持续培养教职工网络安全意识，满足网络安全不断发展的需求。
4. 关键岗位培训，属于部门内部特定具体工作技能和网络安全要求的培训，其主要针对具体岗位的具体网络安全要求而进行。

(二) 培训计划

1. 关键岗位入职培训和年度培训的计划由安全管理员负责协调实施。入职培训以熟悉关键岗位所负责的信息系统具体安全要求及网络安全法律法规、国家标准、学校网络安全制度为主，年度培训以宣贯网络安全最新形势；国家法律法规、国家标准、学校网络安全制度的变化；以及网络安全新技术介绍为主。培训形式可采用学校内部培训、邀请网络安全专家讲座、讨论会等形式。

2. 入职培训和年度培训的计划由学校安全管理员制定，并报学校备案后，与人力资源部门协调实施。入职培训以熟悉网络安全法律法规、学校网络安全制度为主，继续教育培训以宣贯网络安全最新形势；国家法律法规、学校网络安全制度的变化。培训形式可采用内部培训、邀请网络安全专家讲座、讨论会等形式。
3. 后勤部 IT 根据各职位具体情况，汇总、平衡、协调各部门的需求，制订学校的年度网络安全培训计划及各阶段的具体实施方案。
4. 培训计划根据实际情况的变化而加以适当的修正与调整。培训计划的修正与调整须经领导审批。

(三) 培训实施

1. 各部门负责人和安全管理员每半年至少参加一次网络安全培训。
2. 关键岗位人员每半年至少参加一次网络安全专题培训，各部门负责人和安全管理员负责监督。
3. 部门员工每年至少参加一次网络安全专题培训，各部门负责人和安全管理员负责监督。
4. 每年根据实际情况提出培训具体要求和内容指导，协调组织各部门安全培训实施，所涉及部门必须予以配合并执行。
5. 公布培训课程，培训地点、培训讲师及参训人员。有关参训人员必须及时到达培训地点参加培训，不得无故缺席，并填写《员工培训签到表》。
6. 网络安全相关培训纳入学校统一培训考核计划，各部门在进行年度考核时，无故不参加组织安排的培训，或者参加培训考核不合格的员工，将进行通报批评。
7. 每次网络安全类培训结束后，培训组织者应将《员工培训签到表》交由实施培训部门归档留存。

九、 网络安全管理

(一) 管理策略及内容

1. 网络接入策略：教职工必须正确地管理 IT 终端设备及管理信息系统的接入信息，如分配的 IP 地址、用户 ID 和口令，对它们进行保密等，禁止与他人共享这些接入信息。

2. 禁止进行非法路由设定、个人热点共享网络连接、非法拨号连接设定、以及提供非法 http/ftp 访问服务或邮件服务等的设定；
3. 在发生计算机病毒或恶意代码感染的安全事件后，发生场合必须立即切断与学校内部网络的连接，上报学校后勤部 IT，在安全事件处理完成，确保清除病毒或恶意代码后，才可恢复与学校内部网的连接，该安全事件的处理过程应形成事件处置报告，报后勤部 IT 备存；
4. 对于不满足网络安全要求的计算机（如外借后归还部门的计算机，新购入的计算机，个人计算机用于日常办公等），必须进行相应安全设置，符合安全要求后，才能与学校内部网连接。
5. 微软操作系统的计算机安全管理措施：服务器、测试机、ICT 教室、个人计算机、笔记本电脑等安装微软 Windows 系列操作系统的计算机。所有安装微软操作系统的计算机，必须安装正版防毒软件。如有特殊原因或需要，不能安装防毒软件，需要取得领导许可，并确保安全。安装的杀毒软件应实时更新病毒库文件；防护功能缺省为有效状态；定期（每周 1 次）扫描所有文件；开启 Windows update 功能确保定期从微软官方网站下载安全补丁。用户管理、口令管理、文件系统的权限设定须符合《访问控制管理》。
6. UNIX/Linux 类操作系统的计算机安全管理措施：服务器、测试机等安装 UNIX/Linux 类操作系统（包括 Solaris、HPux、Aix、Linux、SuSe 等）的计算机。必须关闭不必要的服务。如因工作需要，必须开启服务的计算机，必须安装服务相关的全部安全补丁；所有安装 UNIX/Linux 类操作系统的计算机，必须安装对应的正版防毒软件。如有特殊原因或需要，不能安装防毒软件，需要取得领导许可，并确保安全；用户管理、口令管理、文件系统的权限设定须符合《访问控制管理》。
7. 桌清和屏清策略。员工必须遵守针对文件和可移动计算机介质的桌清策略，以及针对个人计算机的屏清策略，以减少非授权访问、丢失和损坏部门资产的风险；桌清和屏清策略适用于任何时间任何地点。

1) 桌清说明

   a. 含受限信息的文件或计算机介质在不用时必须存放在合适的带锁文件柜或

其他形式的防护装置中，特别是在下班后和当办公室无人时；

b. 确保打印机/传真机上的信息及时被取走；

c. 受限信息一旦打印出来，必须从打印机处迅速取走；

d. 各部门应督促部门员工切实遵守上述规定，后勤部 IT 应安排专人巡查。

2) 屏清说明

a. 计算机在无人照管或者不再使用时应立即锁定、注销或关机；

b. 计算机应设定带口令保护的自动定时屏保功能，建议定时利用系统缺省值（Windows 系统自动定时屏保缺省值不能超过 15min）；

c. 各部门应督促部门员工切实遵守上述规定，后勤部 IT 应安排专人巡查。

8. 会话超时。对于不活动的网络连接或会话，应设定在连接或会话不活动超过一定期间后自动中断连接的功能。重要服务器必须设定连接或会话不活动的超时设定。

9. 无人值守的设备。服务器等无人值守计算机和设备应采取如下保护措施：远程计算机登录窗口如临时终止使用，需对远程计算机采取屏清操作，如长期（超过半小时）不使用应终止会话（Logoff）；若本地计算机登录了远程计算机，本地窗口临时终止时，应先对远程计算机采取屏清操作，再对本地计算机进行屏清操作；对于无人值守且长期不使用的计算机等设备，应关机。

十、 访问控制

（一） 访问控制原则

1. 最小授权：用户只应具有完成某项工作所需的最小访问权限；
2. 按需审批：权限审批时应根据用户实际需要授权；
3. 职责分离：一个用户不能同时承担多个存在权利冲突的角色，访问的请求方、授权方、管理方也应实现职责分离；
4. 默认拒绝：未经明确授权，一律视为禁止。

（二） 网络和网络服务访问控制管理

1. 应对网络和网络服务进行管控，确保用户只能访问已获授权的网络和网络服务。
2. 采用防火墙技术和虚拟局域网（VLAN）技术实现网络区域的逻辑分离，并保证各个网络区域之间只有授权的信息流交换；

3. 保持严格的分离控制措施，保证跨边界的网络访问安全。防火墙策略设计应遵守“默认拒绝”原则，只允许必须的信息流通过网络，阻止未授权 IP 地址访问；
4. 逻辑上对网络上的设备进行认证和标识，物理上使用资产标签的方式进行设备标识；
5. 外部连接用户访问内部网络或系统应使用 VPN 加密等安全方式进行连接；
6. 对日常工作不需要使用的信息处理设施的远程诊断和配置端口进行严格控制，默认设置成禁用，需要时再进行开启；
7. 网络访问控制策略至少每一年进行复审一次，防止访问控制策略不适宜或不严谨，并将复查结果记录在《访问权限评审记录》表中，提交给后勤部 IT 归档。

（三） 信息系统访问控制管理

1. 信息系统管理员应根据业务要求和工作需要，进行数据和应用系统功能的访问控制；
2. 对所有信息系统的登录应进行必要的管控，以防止非授权访问，并且记录登录成功与失败的日志；
3. 信息系统管理员应对用户注册、授权授予过程进行必要的管理，遵循以下要求：所有用户账号的开通应遵守正式的账号申请审批流程；申请过程中应核实用户申请和用户资料；使用唯一的用户账号，保证可由此账号追溯用户；保存所有用户注册的审批记录；定期进行用户帐号复查，识别及无用或非法用户及权限并进行清理或注销。
4. 信息系统管理员应对用户账号、权限的变更或注销过程进行管理，遵循以下要求：所有用户账号、权限的变更或注销应通过正式的变更或注销审批过程；核实用户账号、权限变更或注消的申请；在教职工工作职责发生变化后，应及时变更用户账号或权限； 在教职工离职后，应及时注销或禁用用户账号，取消该用户访问权； 用户权限变更时，应及时审核账号权限，取消非必要权限；保存所有用户账号、权限变更或注消的审批记录；
5. 记录特殊访问权限的审批过程，定义其使用期限，并定期评审特殊权限所有人的职能和能力是否与其使用的特殊权限一致；
6. 定期至少每一年进行一次权限复查，识别并清理未授权的访问权限，并将复查结果记录在《访问权限评审记录》表中，提交给信息安全部归档确认。

（四） 用户账号和密码管理

1. 所有信息系统用户应妥善保管自己的账号与身份认证信息，对自己使用的账号与身份认证信息所产生的任何活动负责。除特别工作需要，不得将自己负责的账号与身份认证信息提供给他人使用；
2. 用户应对密码进行保密，且密码应符合学校规定的复杂性要求。密码应满足国家密码管理规定的安全要求，同时应定期进行更新；
3. 应严格控制远程用户的操作，如果必须进行远程连接或者控制，应选择使用符合国家密码管理规定的密码技术和产品进行线路加密；
4. 应对可能超越信息系统控制的特权使用工具加以管控。特权使用工具包括但不限于网络及主机系统管理与监控、漏洞扫描、渗透测试、网络嗅探、口令破解等工具；
5. 应严格保护一切合法用户的账号资料和信息，并且要专人专用，防止泄漏。

十一、 机房管理

（一） 机房的日常运行及相关设备的日常管理由机房网络管理员负责操作实施。

（二） 环境控制

1. 严禁在机房内吸烟、大声喧哗、聚众聊天或玩游戏；
2. 机房内物品必须摆放整齐，严禁在机房内堆放杂物；
3. 设备安装过程中产生的各类包装物应在当日及时清理干净；
4. 必须建有机房清洁卫生保洁机制，定期做好机房及设备的清洁保养；
5. 机房的温度、湿度必须满足计算机设备、网络设备、计算机辅助设备、信息存储媒介的要求。

级别 / 项目	机房
温度(℃)	23±1
相对湿度(%)	40～55
温度变化率(℃/h)	＜ 5，不得凝露

表 1 开机时机房的温、湿度

级别 / 项目	机房
温度(℃)	5～35
相对湿度(%)	40～70
温度变化率(℃/h)	＜ 5，不得凝露

表 2　停机时机房的温、湿度

品种	纸介质	光盘	磁带		磁盘	
			长期保存已记录的	未记录的	已记录的	未记录的
温度	5~50℃	20~50℃	18-28℃	0-40℃	18-28℃	0-40℃
相对湿度	40%-70%	10%-95%	20%-80%		20%-80%	
磁场强度			<3,200A/m	<4,000A/m	<3,200A/m <4,000A/m	

表 3　媒体介质库的温、湿度

6. 机房环境监控系统和远程报警系统，必须每天检查系统的运行状况，确保报警系统正常运行。
7. 机房内 UPS 和电池按照以下要求进行管理：
    1) 使用年限超过 10 年的 UPS 应予更换；
    2) 机房内 UPS 电池品牌应选用国际或国内优质品牌中的一种；
    3) 使用 5 年以上的 UPS 电池应视情况进行更换。

（三） 设备与系统日常运行管理

1. 机房网络管理员必须做好机房设备的登记工作，建立详细的设备台账（包括编号、设备名称、型号与主要配置、主要用途、帐号口令、维修情况等，服务器主机还需记录所安装的操作系统、数据库等系统软件和应用软件等），以便于管理和维护；
2. 设备进出机房须进行登记，新设备进入机房须填写《设备进出机房登记表》，并由机房网络管理员统一分配 IP 地址、网络与信息安全管理区域后，方能安装使用；

3. 设备带出机房，由机房管理员登记确认，填写《设备进出机房登记表》；
4. 机房内的设备须由负责管理和维护该设备的人员进行安装、拆卸和配置等操作，操作时应严格按照该设备的操作规程进行；
5. 机房设备的开关操作严格按照设备说明书规定的使用说明进行；
6. 建立机房内设备的硬件检修记录档案，填写系统运行日志，机房内的网络设备、计算机设备采用实时监控，遇有机房设备报警，故障等，处理完毕后，必须填写《机房设备故障表》，每年定期对机房内设备进行检修维护，确保其始终处于良好的运行状态；
7. 为保证系统安全，除网络管理员外，任何人未经批准，不得对机房内网络或计算机设备进行操作；
8. 严格按照数据备份的操作流程，完成业务系统的操作系统和数据的备份工作，严禁完成备份工作前擅自实施新项目或关机；
9. 机房内严禁使用来历不明的软盘、光盘、U 盘等移动存贮介质。严禁携带病毒盘和游戏进入机房，严禁在互联网上下载与工作无关的内容，以防系统被破坏；
10. 严禁各岗位工作人员越权操作，对重要的计算机信息处理系统应分级加设系统口令，以防机密信息的泄露；
11. 机房内计算机、服务器、数据库及各应用系统的管理员口令必须密码复杂化工作，并且包含有字母、数字和特殊字符，口令定期进行更换；
12. 机房网络管理员必须按规定做好机房内主机及网络安全等设备的日志日常备份与管理工作，尤其是主机数据库的审计日志、网络安全设备的参数配置有变动时，要及时记录并备份加密。
13. 定期对机房环境及设施进行检查和维护，数据中心机房设备应每周检查 1 次，并进行巡检记录。
14. 定期对机房的空调设备及附属配件系统，UPS 主机及电池附属配件系统进行维保检查，并将维保报告进行存档。
15. 数据中心机房进出管理：经常在机房内工作的人员，由申请人提交 OA->校园卡权限申请表审批后开通门禁权限，平时进入机房工作时，凭门禁卡进入，同时必须佩戴

工作牌。第三人员如需进入机房，必须由校内接口人提交 OA->学校 IT 需求申请，写明人员姓名、事由等，由部门负责人审批后，须填写《机房出入登记表》，由 IT 授予临时出入权限方可进入，须由 IT 人员全程陪同。

十二、 介质安全管理

可移动存储介质（包括移动硬盘、U 盘、各类存储卡等同类介质）在连接计算机的接口或外接接口时，必须先进行病毒扫描，确认介质的安全性。使用该类介质需注意以下事项：

1. 因工作需要使用可移动存储介质时，须填写《易耗品领用单》向后勤部 IT 提出领用/借用申请；
2. 领用/借用的可移动存储介质只能由借用者本人使用，不得私自将设备再转借他人；
3. 使用可移动存储介质存储受限信息前须得到部门负责人批准；
4. 介质使用完毕后，应及时将借出可移动存储介质归还；
5. 后勤部 IT 在回收借用完毕的可移动存储介质后应将其中数据进行逻辑清除以便下次使用；
6. 对因工作需要须长期使用可移动存储介质的人员，需经相关部门负责人批准，并报送后勤部 IT 备案；
7. 对承载过重要敏感信息或涉密信息的介质的使用、销毁、存放、运输和销毁，应按照《厦门华锐莱普顿学校保密工作制度》《厦门华锐莱普顿学校档案管理制度》进行管理。

十三、 恶意代码防范管理

1. 禁止以任何名义制造、传播、复制、收集恶意代码。
2. 未经许可，不得随意下载使用标准规定之外的防病毒软件或病毒监控程序。
3. 发布最新版本杀毒软件后，必须在一周内对杀毒软件进行升级。
4. 防病毒网关以及杀毒软件需启用实时更新功能，保证恶意代码库实时更新。
5. 新购置的、借入的或维修返回的服务器，在使用前应当对硬盘认真进行恶意代码检查，确保无恶意代码之后才能投入正式使用。

6. 软盘、光盘以及其它移动存储介质在使用前应进行病毒检测，严禁使用任何未经防病毒软件检测过的存储介质。计算机软件以及从其它渠道获得的电脑文件，在安装或使用前应进行病毒检测，禁止安装或使用未经检测过的软件或带毒软件。
7. 管理人员职责

（1）定期每月查看一次防病毒网关日志文件，跟踪解决发现的病毒问题；

（2）及时跟踪恶意代码库的升级情况；

（3）对于不能立即解决的病毒问题，应及时组织协同相关的技术和业务人员进行跟踪解决，在问题解决前尽快采取相应措施阻止事件进一步扩大；

（4）对病毒的发作时间、发作现象、清除等信息的进行维护、备案、并制作案例；

（5）日常病毒信息的公告和发布。

十四、 数据备份与恢复管理

（一） 数据备份的对象

1. 数据备份的对象为与学校正常运作相关的所有关键数据。具体含各类重要业务数据；重要服务器和网络设备的日志信息、配置信息；重要安全设备的日志信息、配置信息；重要信息系统的数据库信息、日志信息等等；
2. 用户终端上的办公数据属于组织数据资源的一部分，要统一纳入数据备份与管理范畴。人员调离工作岗位前要进行完整移交；
3. 数据备份要求有明确的备份策略，由专人负责。备份策略每年由备份管理负责人和部门负责人重新审定，视情况修改和补充。

（二） 数据备份的方式，根据信息系统的情况和备份的内容，有多种数据备份方式：

1. 完全备份：对备份的内容进行整体备份；
2. 增量备份：仅备份相对于上一次备份后新增加和修改过的数据；
3. 差异备份：仅备份相对于上一次完全备份之后新增加和修改过的数据；
4. 按需备份：仅备份应用系统需要的部分数据。

（三） 数据备份操作

1. 已规定对重要信息进行本地备份和恢复，完全数据备份至少每周一次，增量备份或差异备份至少每天一次，备份介质应在数据执行所在场地外存放，并对重要信息进

行异地备份，利用通信网络将关键数据定时批量传送至备用场地，传输过程实行加密，保证信息的、真实性、完整性。

2. 备份操作由数据备份管理员执行。
3. 对于自动完成的备份操作，备份结束后数据备份管理员检查备份日志。
4. 重要备份数据备份至少应保留两份拷贝，一份在本地保存，以保证数据的正常快速恢复和数据查询，另一份在异地保存，避免发生灾难数据无法恢复。

（四） 数据备份策略

1. 为保证系统安全运行，对重要信息系统的关键数据应定期进行备份和恢复演练，重要数据应异地存放，以备数据破坏后恢复。依据谁建设谁运维的原则，各重要信息系统的运维部门根据系统各种数据的重要性及容量，确定备份方式、备份周期和存留周期，制定确保数据安全、有效的备份策略以及恢复预案，并报学报备案。
2. 新建系统的规划与设计，后勤部 IT 在规划设计新建系统时应充分考虑系统备份需求，在系统投运前完成备份策略和恢复预案的制定并在系统投运后同时开始执行，且在运行系统备份需求发生变化时，及时更新数据备份策略和恢复策略。
3. 系统升级与更新：后勤部 IT 对计算机和设备进行软件安装、系统升级改造或更改配置时，应进行系统数据、设备参数的完全备份。应用系统更新后，应实现数据迁移或转换，确保历史数据完整性，并对原系统及其数据进行完全备份，备份数据至少保存 1 年以上，如应用系统有明确要求，按各应用系统要求执行。
4. 介质选择。备份系统的建设要统一纳入信息规划，备份系统及介质的选型要满足各系统的备份策略和数据备份及保存的要求，包括安全可靠性、性能和服务质量、冗余等。
5. 介质管理。数据备份与管理的责任部门要加强对备份介质的管理，关于介质的管理和报废程序，具体信息参见《介质安全管理》，备份介质存放在适于保存的安全环境（如防盗，防潮，防鼠害，磁性介质远离磁性、辐射性等），并有严格的访问控制，对有备份数据的介质要进行定期检查，确认所备份数据的完整性、正确性和有效性。
6. 备份介质存放管理：做好数据备份的文卷管理，所有备份有明确标识，包括卷名、

运行环境、备份人。卷名按统一的规则来命名，由“系统名称-（数据类型+备份方式+存储介质）-备份时间-序号”组成。运行环境：操作系统名称、版本号、数据库名称、版本号等。备份人及其所在部门：某某（部门名称和备份人姓名）。

7. 备份恢复管理

1) 当由于出现故障而导致系统或数据确实损坏并无法抢救时，需要恢复备份数据时，需求部门提交 OA 申请->学校 IT 需求申请表，内容包括数据内容、恢复原因、恢复数据来源、计划恢复时间等，由需求部门以及系统管理员相关负责人审批。

2) 恢复操作前所有相关信息系统的系统管理员同时到场，先备份现场系统、数据和环境，再按照要求进行恢复。

3) 系统恢复后，由相关信息系统的系统管理员进行测试，同时再进行一次备份，恢复的情况应报告运行维护部门。

4) 备份管理员每半年对备份数据进行恢复测试工作，确保备份恢复工作能够按照备份恢复操作手册顺利进行，备份恢复测试应作明细的纪录，填写《备份恢复测试表》，根据测试结果更新备份恢复操作步骤。

5) 对于关键信息系统，每年至少进行一次备份数据的恢复演练，并做出可靠性评估。

8. 数据备份评估

后勤部 IT 应加强对数据备份和管理工作的考核力度。若因未严格遵守规定造成备份系统等发生故障，或数据丢失、泄漏，或导致信息系统无法正常运行的，由发生网络安全事件所在部门安全管理员评估造成的损失，仔细填写《网络安全事态报告单》，并提交后勤部 IT 和上级管理部门。

十五、 系统建设安全管理

（一） 系统定级及系统安全方案设计

1. 信息系统设计前应由中锐教育集团信息管理部进行风险评估，根据风险评估的结果进行系统的设计。
2. 信息系统的安全防护设计应随系统设计、建设和开发一起同步进行。

3. 信息系统的边界将根据系统的实际连接情况进行，包括网络互联、信息系统的互联等，严格按照等级防护的要求进行设计和风险评估。
4. 系统建设方案应当由中锐教育集团信息管理部或者组织专家进行论证和评审，并上报信息安全管理组进行审批，信息安全管理组审批完成后上报学校决策层由总校长最终审批，系统建设中形成相关的技术文件应当保存，以备核查。

（二） 安全产品采购和使用

1. 安全产品在系统方案设计中要经过详细的安全和技术论证，确保满足系统的安全要求。
2. 安全产品应满足国家有关的规定。
3. 安全产品必须有公安部的许可。

（三） 自行软件开发

1. 原则上不自行软件开发，以免与现有软件存在不兼容等问题。
2. 因工作需要，必须自行开发软件时，开发环境要同实际运行的环境物理隔离。
3. 自行软件开发时，应当进行详细的系统设计，针对开发的过程要制定合理的控制方法，并且明确开发人员的职责，严格进行编码、系统测试、功能测试的过程，可参照 CMMI 二级以上的要求进行。
4. 自行软件开发时，软件的开发文档、过程文档、原代码、测试代码等要由专人保管，方便以后的软件维护、升级等工作。

（四） 外包软件开发

1. 以委托外包的形式进行软件开发时，注意软件开发过程的连续性，一般情况下，原来系统在进行功能性增加的情况下应由原来的软件学校进行。
2. 外包的软件，在开发后需要严格按照 CMMI 三级以上的要求进行代码的质量测试，同时提供相关软件设计的各种设计文件和使用指南。
3. 外包的软件，应在开发设计完成后选择第三方软件测试方进行软件包中的原代码检测，主要检测包括恶意代码、缺陷代码、功能逻辑错误、后门等方面，只有在检测验收合格后方可并网上线试运行。
4. 软件外包方应具备 CMMI 三级以上的认证资质。

5. 软件外包方应具备相关行业的软件开发经验。
6. 软件外包方应具备安全系统设计的能力和经验。

（五） 工程实施

1. 信息系统建设实施中，建议邀请具有相关监理资质的单位负责工程监理工作，协助全面的施工管理。
2. 工程施工要由监理单位（若有）、施工需求方、施工组织方和施工方制定详细的工程施工方案，在完全可控、可监督的环境下进行。
3. 工程实施质量控制按一下步骤进行：
   1) 审查进入施工现场的分包单位的资质证明文件，控制分包单位的质量。
   2) 审批施工承包方的开工申请书，检查、核实与控制其施工准备工作质量。
   3) 审批施工方提交的方式方案、施工组织设计或施工计划。
   4) 审批施工承包方提交的有关材料、半成品和构配件质量证明文件（出厂合格证、质量检验或试验报告等）。
   5) 审核施工方提交的反映工序施工质量的动态统计资料或管理图表。
   6) 审核施工方提交的有关工序产品质量的证明文件（检验记录及试验报告）、工序交接检查（自检）、隐蔽工程检查、分部分项工程检查报告等文件、资料。
   7) 审批有关设计变更、修改设计图纸等。
   8) 审核有关应用新技术、新工艺、新材料、新结构等的技术鉴定书，审批其应用申请报告。
   9) 审批有关工程质量缺陷或质量事故的处理报告。

（六） 测试验收

1. 指定专门的部门或人员负责项目的测试、验收工作。
2. 测试验收前应制订测试验收方案，并组织相关人员对其进行评审和论证，确保测试验收方案的可实行性和规范性。
3. 测试验收前应制定错误恢复方案及应急方案，包括自动化程序失效时的手工替代方法。
4. 测试验收负责部门应要求厂商提供相应培训及过程文档，并妥善保存。

5. 验收标准应科学准确，应严格按照测试验收方案进行，以保证测试验收的效果。
6. 测试验收中产生的信息和结果应采取保密措施加以管理，防止信息泄露。

（七） 系统交付

1. 工程监理（若有）、工程施工方要制定系统的交付清单，后勤部 IT 要根据交付清单对所交接的设备、软件和文档等进行详细的清点，包括设备的详细配置。
2. 系统验收后，割接上线前要由系统开发方、施工方等对系统运行维护人员进行技能培训和产品使用维护培训，并提供相应的过程文档和系统维护文档。

（八） 安全服务商选择

1. 信息系统建设时，系统设备、软件开发服务商应符合国家的有关规定，具有满足要求的相应资质。
2. 选定的安全服务商，应具备系统连续升级（包括漏洞扫描系统库的升级、防病毒库的升级和更新等）的能力。
3. 信息系统建设时，应与安全服务商签订服务合同，约定相关的技术支持等详细条款，明确相关的责任和义务，确保系统安全可控可靠运行。

十六、 变更管理

(一) 信息系统变更工作可分为一般变更工作和重大变更工作，重大变更工作特指：系统拓扑结构改变、系统网络或安全设备变更、系统关键主机变更、系统数据库变更、系统应用软件变更、系统网络、主机、数据库、应用系统等安全策略或安全配置发生重大变更、系统数据备份设备变更。

(二) 需进行系统重大变更的部门根据实际应用情况提出变更需求和变更方案（变更方案中必须包含变更前数据备份方案，以及变更成功和失败时系统恢复的方案），填写《系统变更申请表》，并向上级领导提交变更申请，若未申请通过，而擅自进行重大变更，按学校相关的规定进行处罚。

(三) 参照国家信息系统等级保护的相关标准，由后勤部 IT 组织相关部门和网络安全专家讨论方案的安全性，根据讨论结果修改和审批方案。

(四) 系统取得变更申请审批后，后勤部 IT 根据《系统变更申请表》中描述和变更方案，进行系统变更。

（五）系统重大变更前必须按照变更前数据备份方案进行关键数据的全面备份，系统变更成功或失败时，应立即根据系统恢复方案进行系统恢复。

（六）系统重大变更后必须进行信息系统基线检测并合格后方可上线运行。

（七）系统重大变更成功后，后勤部 IT 应根据系统变更情况对系统各项网络安全管理进行监控检查确认，并报领导知悉。

（八）紧急重大变更细则

1. 若因工作需要，对信息系统进行紧急重大变更，需求和运维管理部门可通过电子邮件等书面形式向后勤部 IT 提出简易快速申请。
2. 后勤部 IT 根据重要性和紧迫性做判断，确定其优先级和影响程度，并进行相应快速审批处置。
3. 紧急变更过程由系统维护人员进行变更操作和过程记录，并在事后一周内报后勤部 IT 进行评估和备存。
4. 在紧急事件处理完成后，必须在一周内补办正式、完整的文档，并根据重大变更的一般规则进行相应变更后的安全管理。
5. 若系统由第三方进行维护管理，需进行系统变更操作时，由维护方填写变更申请表，并交由系统运营单位进行保存。

十七、 信息安全事件管理

（一） 网络安全事件分类

1. 有害程序事件：包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件等。
2. 网络攻击事件：包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件等。
3. 信息破坏事件：包括信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件等。
4. 信息内容安全事件：违法法律和行政法规的网络安全事件；发布反动、色情等有害信息；组织串连、煽动集会游行的网络安全事件。

（二） 网络安全事件分级

1. 特别重大安全事件，指能够导致特别严重影响或破坏的网络安全事件，包括以下情

况：会使特别重要信息系统遭受特别严重的系统损失；产生特别重大的社会影响。重大安全事件，指能够导致严重影响或破坏的网络安全事件，包括以下情况：会使特别重要信息系统遭受较大的系统损失，或使重要信息系统遭受严重的系统损失、一般信息系统遭受特别严重的系统损失；产生较大的社会影响。

2. 一般安全事件，指不满足以上条件的网络安全事件，包括以下情况：会使特别重要信息系统遭受较小的系统损失，或使重要信息系统遭受较大的系统损失、一般信息系统遭受特别严重或严重以下级别的系统损失；产生一般的社会影响。

3. 安全事件处置流程

(三) 事件处置

1. 由学校进行事件首次确认，确定这起安全事件侵害是否为网络安全事件或仅为误警；若没有明确证据确认是误警时，应作为可疑的网络安全事件，上报上级领导进行第二次评审。
2. 确认是否为网络安全事件，如果是网络安全事件则立即触发响应机制，同时采取必要的取证分析和通报行动。
3. 如果网络安全事件已被控制，触发随后必须的进一步响应，并记录所有信息用于事件评审。
4. 如果事件失去控制，触发危机救援并召集相关人员，例如部门负责业务连续性的管理人员和工作组。
5. 记录所有活动，以备后续分析。

(四) 网络安全事件的改进

网络安全事件解决完毕并经各方(可能包括外部相关方)同意结束处理过程后，进行下面的活动:

1. 进一步收集相关证据；
2. 迅速从网络安全事件中总结教训，分析事件发展的趋势和模式；

3. 确定新的或经过变化的防护措施并立即付诸实施；

4. 确定对本文件的改进。

十八、 信息安全应急预案

（一） 应急保障措施

1. 重要信息系统应建立数据备份，做好数据备份的维护及保护工作。

2. 各部门应加强日常技术储备与保障管理工作，适时组织相关专家和机构分析当前网络安全角势，对网络应急预案及实施进行评估，开展现场研究。

3. 宣传、培训和演习。各部门应加强对普通人员安全使用计算机的宣传教育工作，全面提高网络使用人员的安全意识。定期对重要系统相关人员进行技术培训和应急演练，保证应急预案的有效实施，提高通信保障应急的能力。

（二） 预案的启动

1. 确定事件类型

1） 应急工作小组应及时判断事件的类型和紧急程度；

2） 确定事件范围，检查敏感信息失密情况及程度，分析攻击来源及侵入点；

3） 判断事件危害性及损失程度，分析人为原因、事件潜在危害性；

4） 确定事件发生时间及延续时间；

5） 判断需采用的手段及准备处理事件需要的必备资源；

6） 根据损失程度及延续时间等情况确定等级，特别重大、重大信息险情需立即报信息部门，同时启动相关应急处置预案。

2. 事件报告

1） 报告方式：根据事件的类型及紧急程度及时向信息部门报告，同时进行事件确认，制定具体措施。后勤部 IT 对事件进行确认，并根据事件级别要求系统运行维护管理部门牵头迅速成立相应级别的领导小组并上报上级领导。

2） 报告内容：事件的基本信息（故障发生的时间、故障点、故障情况）、事件的类型、表现出来的现象、涉及的网络，事件当前的状态及可能造成的后果，以及事件解决的建议和措施。

3） 现场处理：抑制事件的影响进一步扩大，限制潜在的损失与破坏，对事件分类进行

处理。

(三) 应急处置预案

1. 黑客攻击或软件系统遭破坏性攻击时的应急预案

1) 信息系统使用部门，应预先拟定各重要信息系统针对此类事故的详细流程、应急预案并上报信息部门审查备案，并定期开展应急预案演练。

2) 重要信息系统必须每日进行配置文件和重要数据备份，备份数据应存放于安全处。

3) 当发现信道传输内容被篡改，或通过入侵监测系统发现有黑客正在进行攻击时，应立即向信息部门报告。

4) 系统管理人员应在 10 分钟内赶到现场，首先将被攻击（或病毒感染）的服务器等设备从网络中隔离出来，保护现场，并同时向后勤部 IT 通报情况。

5) 后勤部 IT 负责组织人员恢复与重建被攻击或被破坏的系统，恢复系统数据，并及时追查非法信息来源。

6) 事态严重的，立即向领导报告，并根据指示向上级或公安部门报警。

2. 网络线路中断或硬件设备故障时的应急预案

1) 后勤部 IT 应预先拟定各重要信息系统针对此类事故的详细流程、应急预案并上报审查备案，并定期开展应急预案演练。

2) 网络主、备用线路有一条中断或硬件设备发生故障，应立即启动备用线路或备用设备接续工作，同时向后勤部 IT 上报。

3) 系统维护人员接到报告后，应协助系统信息部门迅速判断故障节点，查明故障原因，并及时予以恢复。如网线路中断属外联学校原因的，应立即与外联学校联系，要求恢复。

3. 如果主、备份线路同时中断，或者发生故障的硬件设备一时无法修复的，应在判断故障节点，查明故障原因后，尽快研究恢复措施，并立即向后勤部 IT 汇报。

(四) 应急预案现场处理流程

1. 计算机病毒

1) 断网、升级系统补丁及防病毒软件，查找病毒源，进行杀毒；

2) 一时不能查，应向有关部门进行报告，提供病毒样本；

3) 查找计算机病毒感染的存储介质；

4) 对病毒利用的系统漏洞要通过补丁和升级的方式进行填补；

5) 记录全部处理过程。

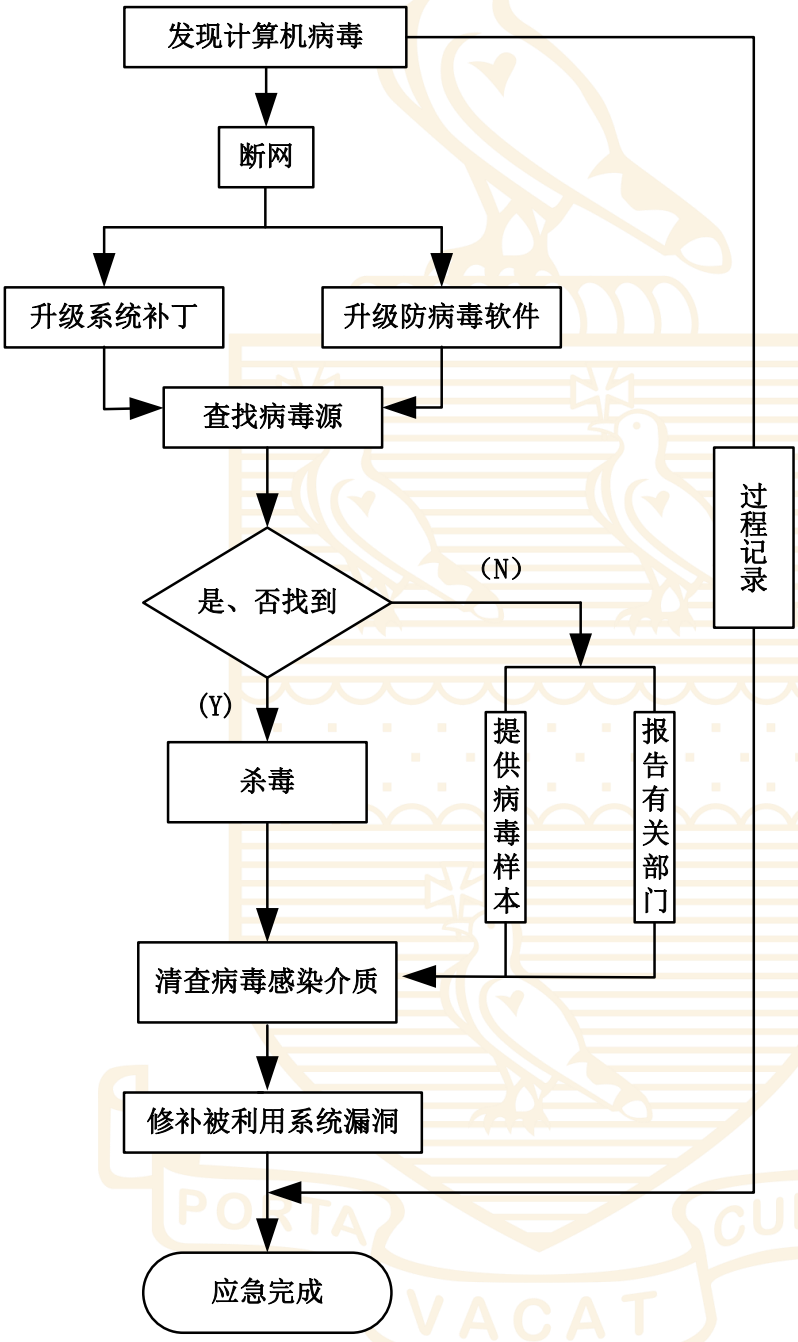


图 1 计算机病毒现场处理流程图

2. 黑客入侵。采取必要措施抵御入侵行为，保护系统和数据安全，利用完整性检查工具进行检查，必要时向公安机关报告并申请技术协助。

1) 记录系统状况；
2) 立即复制系统登录文件、历史文件、日志文件等重要文件；
3) 修改防火墙、路由器等网络安全设备的过滤规则；
4) 断开被攻主机、关闭不需要的服务；
5) 处理可疑的文件和程序；
6) 修改不安全的帐号和口令；
7) 恢复被修改的软件和数据；
8) 安装相应的补丁程序，填补安全漏洞；
9) 编写报告，详述事件过程及处理步骤。

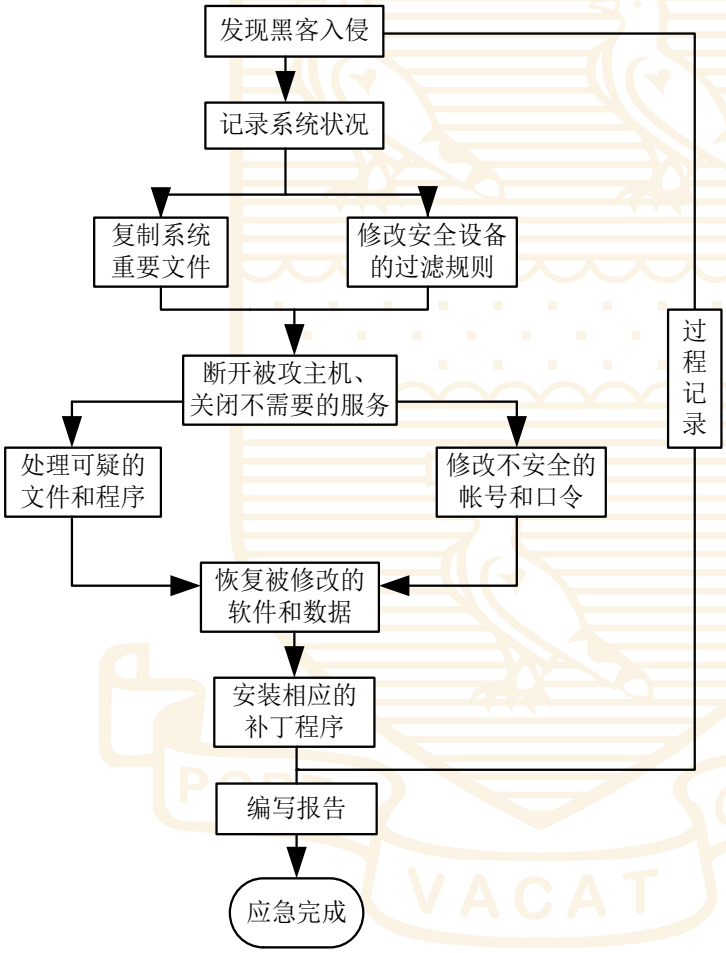


图 2 黑客入侵处理流程图

（五） 定期每年对应急预案进行一次审查，根据实际情况，如演练过程中出现的问题等对内容进行更新，以便更贴合信息系统实际情况。

（六） 为提高网络安全突发事件应急响应水平，信息部门应每年至少组织一次预案演练；检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求。通过演练，进一步明确应急响应各岗位责任，对预案中存在的问题和不足及时补充、完善。

十九、 附则

本文件由后勤部负责解释。本办法自印发之日起执行。

二十、 附录表单

1. 附件一：《员工培训签到表》
2. 附件二：《访问权限评审记录》
3. 附件三：《机房巡检记录表》
4. 附件四：《设备进出机房登记表》
5. 附件五：《机房出入登记表》
6. 附件六：《机房设备故障表》
7. 附件七：《信息系统资产分类表》
8. 附件八：《易耗品领用单》
9. 附件九：《介质作废登记表》
10. 附件十：《备份恢复测试表》
11. 附件十一：《网络安全事态报告》
12. 附件十二：《系统变更申请表》

厦门华锐莱普顿学校
CHIWAY REPTON SCHOOL XIAMEN

培训签到表 Training Record

培训内容 Content			
培训对象 participants		组织部门/讲师 Organizer/Trainer	
培训地点 Venue		培训时间 Duration	

本人确认已学习并理解本次培训内容。
I confirm that I have learned and understood the content of this training.

No.	部门Department	姓名 Name	签名Signature
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

备注Remarks：
员工参加培训必须准点到达现场，先签到后培训。
Participants must join the training on time and sign this form firstly.

<table>
<tr><td rowspan="3">评审内容</td><td colspan="3">部　　门: 评审部门名称</td><td colspan="4">项　　目: 评审的内容，例如：文件服务器、邮件组、上网权限、门禁权限、USB权限等</td></tr>
<tr><td colspan="3">服务器名: file、sever（如若不知，请询问IT）</td><td colspan="4">评审对象:① 如：管理权限、用户权限、应用策略等</td></tr>
<tr><td colspan="3">清单版本:②
_____年____月 ____日
IT给导出清单的最新日期，如：12月7日导出一份，12月10日又导出一份，这填写12月10日</td><td colspan="4">评审日期:　_____年____月_____日
填写评审当日的日期</td></tr>
<tr><td rowspan="6">权限评审</td><td colspan="3">正确性验证
评审人员将自己手中的清单与IT导出的清单进行评审，若账号、权限均正确，则勾选即可；只要有一项不正确，则需说明
（核对清单与服务器中实际开设情况是否一致）</td><td colspan="4">合理性验证
评审人员将清单评审后，交由 部门领导 评审最终账号和权限是否合理
（根据业务实际情况判断是否需要调整）</td></tr>
<tr><td colspan="2">账号清单</td><td colspan="2">权限设定</td><td colspan="2">账号清单</td><td colspan="2">权限设定</td></tr>
<tr><td>□ 正确</td><td>□ 不正确</td><td>□ 正确</td><td>□ 不正确</td><td>□ 合理</td><td>□ 需调整</td><td>□ 合理</td><td>□ 需调整</td></tr>
<tr><td colspan="4">不正确说明:③</td><td colspan="4">调整说明:③</td></tr>
<tr><td colspan="4">若不正确，需说明不正确的内容是什么；
若正确，此处无需填写；</td><td colspan="4">若需调整，需说明调整的内容是什么；
若合理，此处无需填写；</td></tr>
<tr><td colspan="2">评 审 人:</td><td colspan="2">信息安全员签字（需手签）</td><td>负 责 人:</td><td colspan="3">部门负责人签字（需手签后）</td></tr>
<tr><td rowspan="3">跟踪处理</td><td colspan="4">处理结果:③</td><td colspan="4">处理结果:③</td></tr>
<tr><td colspan="4">若以上有不正确，信息安全员需找IT沟通进行处理，此处需填写最后调整后的结果以及将最新的清单一并提交；
如正确，此处无需填写；</td><td colspan="4">若以上有需要调整，信息安全员需找IT沟通进行处理，此处需填写最后调整后的结果以及将最新的清单一并提交；
如合理，此处无需填写；</td></tr>
<tr><td colspan="2">管 理 员:</td><td colspan="2">若有处理，则对应处理的IT管理员姓名；
如无，则无需填写；</td><td>管 理 员:</td><td colspan="3">若有处理，则对应处理的IT管理员姓名；
如无，则无需填写；</td></tr>
<tr><td>验证</td><td colspan="2">评 审 人
签　　字:</td><td colspan="2">若有处理，信息安全员签字（需手签）；
如无，则无需填写；</td><td>负 责 人
签　　字:</td><td colspan="3">若有处理，部门负责人签字（需手签）
如无，则无需填写；</td></tr>
<tr><td>备注</td><td colspan="7">①“评审对象”可参照随后内容填写：文件共享权限、某系统账号权限等。
②“清单版本”应根据权限清单的最后一次变更日期填写。
③“权限评审”结果如果正确无需调整，则可以不用填写。</td></tr>
</table>

凝远网络机房巡检记录登记表

巡检年月：　　巡检人：

巡检记录					
序号	条目	内容（正常方框内打钩）	巡检日期：		
			正常	异常	异常说明
1	机房环境	1、门禁情况	□	□	
		2、卫生情况	□	□	
		3、温度	□	□	
		4、湿度	□	□	
		5、照明可靠	□	□	
		6、窗户密闭	□	□	
2	空调运行情况	1、空调可正常运行	□	□	
		2、空调功能状态	□	□	
3	配电系统情况	1、电压范围正常	□	□	
		2、配电柜状态正常	□	□	
		3、防雷、接地设施完好可靠	□	□	
4	消防系统情况	1、消防设备齐全完好	□	□	
		2、应急照明设施完好	□	□	
5	网络运行情况	1、光纤、防火墙、交换机连接正常	□	□	
		2、网络通讯正常	□	□	
		3、数据指示灯正常	□	□	
		4、交换机端口及网线连接状态正常	□	□	
		5、设备标示、标签是否清晰牢固	□	□	
6	服务器运行情况	1、服务器指示灯运行正常	□	□	
		2、电源运行状态	□	□	
		3、风扇运行状态	□	□	
		4、硬盘运行状态	□	□	
7	UPS运行情况	1、UPS指示灯状态	□	□	
		2，UPS运行情况	□	□	
		3、UPS负载情况	□	□	
存在问题					

巡检人：					
序号	条目	内容（正常方框内打钩）	巡检情况		异常说明
			正常	异常	
1	机房环境	1、门禁情况	□	□	
		2、卫生情况	□	□	
		3、温度	□	□	
		4、湿度	□	□	
		5、照明可靠	□	□	
		6、窗户密闭	□	□	
2	空调运行情况	1、空调可正常运行	□	□	
		2、空调功能状态	□	□	
3	配电系统情况	1、电压范围正常	□	□	
		2、配电柜状态正常	□	□	
		3、防雷、接地设施完好可靠	□	□	
4	消防系统情况	1、消防设备齐全完好	□	□	
		2、应急照明设施完好	□	□	
5	网络运行情况	1、光纤、防火墙、交换机连接正常	□	□	
		2、网络通讯正常	□	□	
		3、数据指示灯正常	□	□	
		4、交换机端口及网线连接状态正常	□	□	
		5、设备标示、标签是否清晰牢固	□	□	
6	服务器运行情况	1、服务器指示灯运行正常	□	□	
		2、电源运行状态	□	□	
		3、风扇运行状态	□	□	
		4、硬盘运行状态	□	□	
7	UPS运行情况	1、UPS指示灯状态	□	□	
		2，UPS运行情况	□	□	
		3、UPS负载情况	□	□	
存在问题		（时间）月份： 周别：			

设备出入机房登记表

日 期	设备类型	设备配置明细	设备序列号	来访人员（单位）	单位/部门	进入时间	离开时间	设备位置	设备出入事由

机房出入登记表

日 期	姓名	单位/部门	事　由	陪同人	进入时间	离开时间	IT人员

IT故障记录表

序号	IT类别	故障设备	故障现象	故障原因	发生时间	解决时间	故障性质

填表须知

内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

关注方面		注意事项
关于资产列举的颗粒度		越重要的资产，列举时颗粒度越细；越不重要的资产，列举颗粒度越粗。此原则适用于实物资产或数据资产，如服务器须一一列举，而办公电脑可考虑按其用户岗位或其用途分组列举。
关于资产用途的描述		资产表中的“用途”，指的是实物、软件、数据资产的功能或价值体现。例如，对于实物资产而言，可以列出其承载的业务和应用，以及可能影响到的工作。
关于资产的归属部门		基于“谁主管，谁负责”的原则进行划分；具有资产管理权限、对资产的安全管理负最终责任的部门即为资产的归属部门。某些资产管理可能涉及多个管理部门。
		部门内部生成的文档和数据，归该部门自身所属。
关于资产的保存位置		电子类数据文件的保存位置即其存放的介质。如果电子文件有多份拷贝和多个保存位置，也应说明（包括逻辑存放位置如硬盘、介质的物理存放位置文件柜等）。
		软件保存位置即其安装在哪里。
		实物资产的保存位置即实物资产安置的物理位置。大物件精确到楼层、房间，小物件精确到保险柜、文件架等。
		数据资产的保存位置可能不止一处，需要全部列举，例如个人电脑、笔记本电脑、服务器、打印纸质件等。
关于责任人的确定		无论资产是本部门产生还是源自其他部门，本部门都应该指定责任人，对该资产在本部门的安全负责，资产责任人一般为保管人。对于公共资产其责任人为部门负责人。
关于保管者/维护者的确定		如果信息资产在个人电脑上，保管者是个人电脑/笔记本电脑的使用者。
		对于存放在公共平台（公共服务器、数据库、公共PC）中的信息资产，保管者为指定的运维人员（管理员）。
关于使用者的确定		信息资产的最终用户，如应用系统的终端用户。
关于CIA取值的说明	数据资产的CIA	不同的数据类型CIA取值倾向有所不同，如对于业务数据等，数据资产主要以完整性（I）为主，完整性的高低将直接影响到业务的运行状态正常与否； 同样的数据资产，在不同部门作识别时，其机密性要求应一样（根据现有密级划分标准确定），而I和A可能会不同。
	软件资产的CIA	软件资产C值的确定，应该考虑到该软件与哪一级别数据资产直接关联。关键应用则对可用性A的关注程度相对较高。
	实物资产的CIA	实物资产C值的确定也是根据直接关联的数据资产的C值而确定，比如磁带或光盘存放C值为2的数据，那么该实物资产的C值也为2。但是对于数据库服务器、文件服务器等保存大量数据的实物资产来说，可以考虑将其保密等级比所存放数据资产的最高密级增加一级。比如一台大量存储了C值为3的文件的文件服务器的C值可以认定为4。
	人员资产的CIA	人员资产的CIA确定也和实物资产有类似考虑，人员的CIA取值与他能访问的其他资产的取值直接关联。
	服务资产的CIA	与服务提供商所服务的信息资产的CIA取值相关。对于服务来说，优先考虑可用性，CI取值适当考虑服务提供商服务过程可能给其他资产带来的风险。

资产分类

内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

资产类别		示例
数据资产	包括各种业务系统数据、业务数据、纸质文档，可按照部门现有文件明细列举，或者根据部门业务流程从头至尾列举。对于非重要数据，要求识别的是分组或类别，不必具体到特定的单个文件；对于重要数据则要求尽可能详尽。 数据资料的列举和分组应该以业务功能和保密性要求为主要考虑。本部门产生的数据以及其他部门按正常流程交付到本部门的数据和文件，都在列举范畴内。对于本部门生成的数据资产的列举应尽量详尽。	电子数据类： 客户资料、卡片信息、户口信息、交易信息、业务统计数据、财务数据、交易数据、制度文件、管理办法、技术方案及报告、工作记录、表单、配置文件、拓扑图、系统信息表、用户手册、数据库数据、操作和统计数据、软件源代码、用户手册、系统日志等**（以上均应填写具体名称，以独立的文件或文件组为单位）**
		纸质文件类： 公文、合同、操作单、项目文档、记录、传真、财务报告、发展计划、应急预案、或各类经领导审批过的文档等
实物资产	各类硬件设备或设施，这些硬件设施或者安装有已识别的软件（服务器），或者其上存放各种数据资产（存储介质），或者是各类网络设备、机房设备等。	主机设备、存储设备、网络设备、安全设备、打印机、复印机、刻录机、碎纸机、文件柜、移动硬盘、光盘、移动存储介质、布线系统、UPS等**（关注承载重要系统或重要信息的设备和介质）**
人员资产	本部门的工作人员，包含正式员工及临时员工、外聘员工等；列举时按其岗位或角色进行分类，不必精确到个人。	包括（可能不限于）本部门现有的岗位列表；关注掌握重要信息和核心业务的人员
服务资产	本部门通过购买方式获取的，或者需要支持部门特别提供的，能够对其他已识别资产的运行起支持作用（也就是对业务有支持作用）的服务。	产品技术支持、运行维护服务、桌面帮助服务、网络接入服务、安全保障服务、呼叫中心、保洁、安保、咨询审计、基础设施服务等
软件资产	本部门通过自主开发、第三方开发、直接购买方式获取的各类系统软件。	包括：操作系统、数据库软件、应用程序软件、网络软件、安全管理软件、办公应用系统、业务系统软件、软件开发工具等，这些软件资产负责处理、存储或传输各类信息。

资产分类

内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

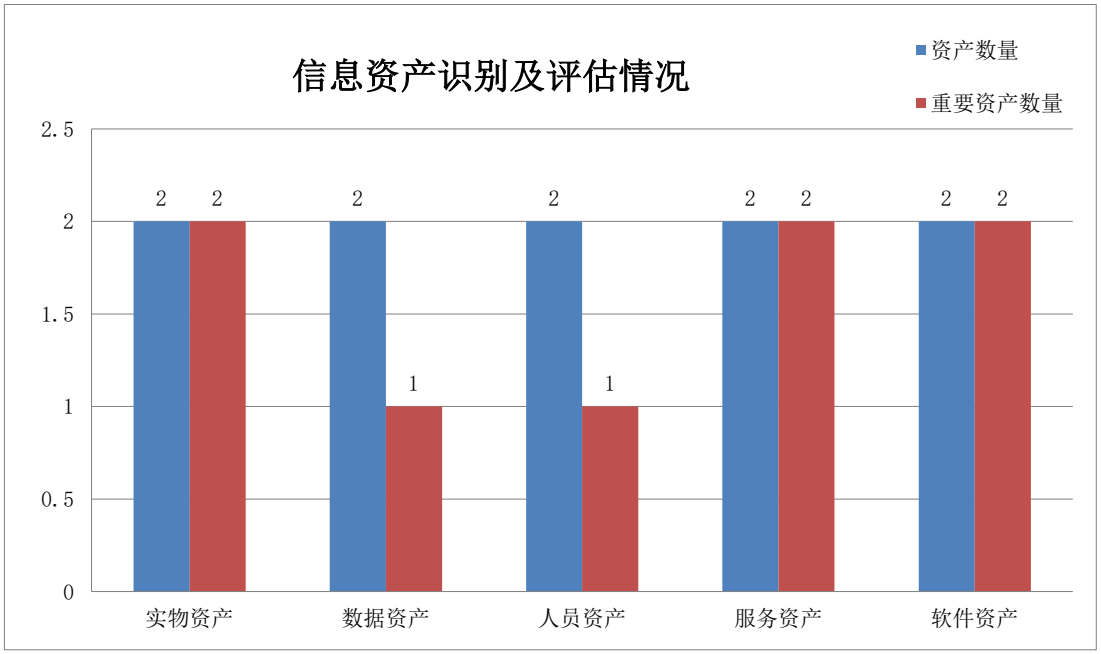
取值	资产等级（重要性）	机密性Confidentiality			完整性Integrity			可用性Availability		
		一般资产	人员	示例	一般资产	人员	示例	一般资产	人员	示例（仅供参考）
5	很高	内容涉及组织最重要的秘密，关系未来发展的前途命运，对组织利益有着决定性的影响，如果泄露会造成灾难性的损害	可以访问组织最高秘级信息的人员	**人员类：**核心系统管理人员； **实物类：**主机设备、核心网络设备； **软件类：**关键业务系统； **数据类：**核心系统配置参数 **服务类：**主机服务	完整性的破坏会对组织造成重大影响，对业务冲击重大，并可能造成严重的业务中断和无法弥补的损失	人员如未正确履行其职责，将对核心资产的完整性带来非常严重的影响	**人员类：**核心系统管理人员、数据库管理人员、备份系统管理人员； **实物类：**主机设备、核心网络设备； **软件类：**关键业务系统； **数据类：**核心系统配置参数	可用性要求非常高，合法使用者对信息及信息系统的可用度达到年度99.9%或以上	如果要维持业务正常运作，可以容忍该人员所承担职务突然缺席不得超过1个工作日，否则会对业务造成影响	**人员类：**核心系统管理人员； **实物类：**主机设备、核心网络设备； **软件类：**关键业务系统； **数据类：**核心系统配置参数 **服务类：**核心系统维保商
4	高	内容涉及组织的重要秘密，其泄露会使组织的安全和利益受到严重损害	最高可以访问到机密级信息的人员	**人员类：**部门管理人员； **实物类：**文件柜、物理监控设备； **软件类：**系统软件、IT服务台 **数据类：**系统监控配置参数； **服务类：**关键系统维保商、网络维保商	完整性的破坏会对组织造成重大影响，对业务冲击严重，较难弥补	人员如未正确履行其职责，将对重要资产的完整性带来严重的影响	**人员类：**部门管理人员； **实物类：**文件柜、物理监控设备； **软件类：**主机系统软件、IT服务台 **数据类：**系统监控配置参数； **服务类：**关键系统维保商、网络维保商	可用性要求较高，合法使用者对信息及信息系统的可用度达到每天90%以上，或系统允许中断时间小于10分钟	如果要维持业务正常运作，可以容忍该人员所承担职务突然缺席不得超过3个工作日	**人员类：**关键系统管理人员； **实物类：**开放设备、物理监控设备； **软件类：**主机系统软件、IT服务台 **数据类：**系统监控配置参数； **服务类：**网络专线
3	中等	组织的一般性秘密，其泄露会使组织的安全和利益受到损害	最高可以访问一般性的秘密信息和内部使用信息的人员	**人员类：**业务操作人员； **实物类：**办公台式机； **软件类：**OA系统、防病毒软件； **数据类：**内部管理文件； **服务类：**安保	完整性的破坏会对组织造成影响，对业务冲击明显，但可以弥补	人员如未正确履行其职责，将对其他资产的完整性带来较严重的影响	**人员类：**业务操作人员； **实物类：**办公台式机； **软件类：**OA系统、防病毒软件； **数据类：**制度文档、应急演练报告； **服务类：**安保	可用性要求中等，合法使用者对信息及信息系统的可用度在正常工作时间达到70%以上，或系统允许中断时间小于30分钟	如果要维持业务正常运作，可以容忍该人员所承担职务突然缺席超过3个工作日，但不能超过5个工作日	**人员类：**业务操作人员； **实物类：**办公台式机； **软件类：**OA系统、防病毒软件； **数据类：**制度文档、应急演练报告； **服务类：**外联专线
2	低	仅能在组织内部或在组织内某一部门内公开的信息，向外扩散有可能对组织的利益造成轻微损害	只可以接触/存取内部使用的信息	**实物类：**UPS、空调； **软件类：**OFFICE办公套件； **数据类：**制度文档； 服务类：供电	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，对业务冲击轻微，容易弥补	如果该人员未正确执行其职务内容，只会对业务运作带来轻微影响	**实物类：**UPS、空调； **软件类：**OFFICE办公套件； **服务类：**供电	可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到25%以上，或系统允许中断时间小于60分钟	如果要维持业务正常运作，可以容忍该人员所承担职务突然缺席超过5个工作日	**实物类：**光盘刻录设备
1	很低	可对社会公开的信息，公用的信息处理设备和系统资源等	只可以接触/存取对外公开的信息		完整性价值非常低，未经授权的修改或破坏会对组织造成的影响可以忽略，对业务冲击可以忽略	如果该人员未正确执行其职务内容，不会对业务运作造成影响		可用性价值可以忽略，合法使用者对资产的可用度在正常工作时间低于25%	如果该人员缺席，不会对业务正常运作造成影响	

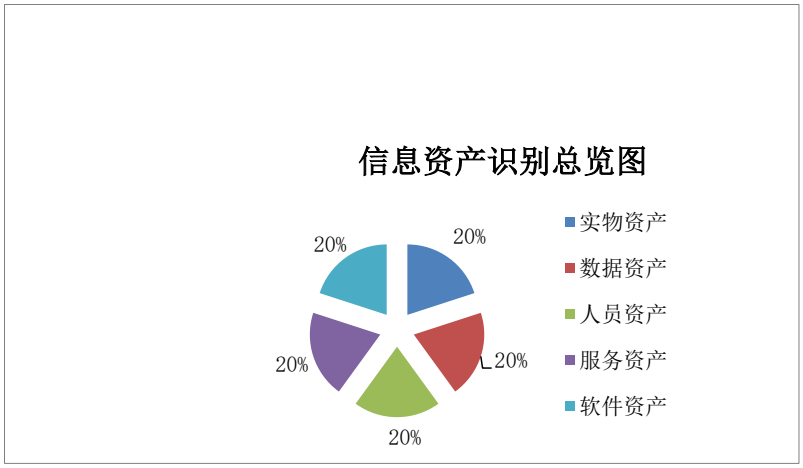
资产分类

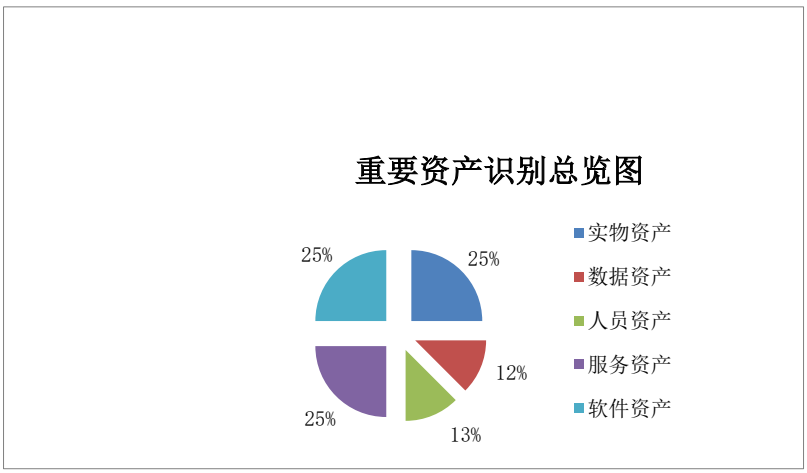
内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

	实物资产	数据资产	人员资产	服务资产	软件资产	总数
资产数量	2	2	2	2	2	10
重要资产数量	2	1	1	2	2	8







实物资产

内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

此处填写产生业务数据或影响业务数据的关键实物

序号	所属系统	资产类别	设备名称	设备型号	序列号	固资编号	IP地址	设备用途	存放位置	使用人	责任人	机密性	完整性	可用性	资产价值	是否为重要资产
1	OA系统	网络设备	OA系统核心交换机	HWXXXXXX	000XXXX	1234	192.168.X.X	用于OA系统网络核心传输	机房/机柜/U位	XX	XX	5	5	5	5	是
2	OA系统	主机设备	OA系统管理员PC	DellXXX	000XXXX	2345	192.168.X.X	用于OA系统管理	A栋XXX室工位号	XX	XX	5	3	3	5	是
3															0	否
4															0	否
5															0	否
6															0	否
7															0	否
8															0	否
9															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否
															0	否

数据资产

内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

此处填写涉及公司业务数据的关键文件

编号	业务系统	资产类别	数据名称	存储形式	内容描述	归属部门	责任人	保存位置	机密性	完整性	可用性	资产价值	是否为重要资产
XXXXX	ERP系统	软件源代码	ERP系统软件源代码	文本存储	用于ERP系统相关接口二次开发	IT部门	XXX	XX服务器	5	5	5	5	是
XXXXX	ERP系统	用户手册	ERP系统客户端用户手册	文本存储	用户操作ERP的步骤参考手册	ERP部门	XXX	XXPC	3	2	2	3	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否
												0	否

人员资产

内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

此处填写接触业务数据的关键人员

资产类别	部门	岗位（职责描述）	姓名	登录账号	机密性	完整性	可用性	资产价值	是否为重要岗位	是否有后备人员
技术经理	IT部门	管理技术部门日常运营	XXX	员工系统唯一识别号	4	4	4	4	是	是
实习人员	ERP部门	协助ERP部门技术人员测试	XXX	员工系统唯一识别号	2	1	2	2	否	是
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	
								0	否	

服务资产

内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

此处填写产生业务数据或影响业务数据的关键服务

编号	资产类别	服务分类	服务供应商	服务内容描述	服务范围（涉及的系统、部门）	服务开始/终止时间	接口部门	机密性	完整性	可用性	资产价值	是否为重要服务资产	是否产生业务数据
XXXX	网络接入服务	IT资源服务	电信	提供公司Internet网络接入	XXX部门XXX系统	2010-2020	IT部门	5	5	5	5	是	是
XXXX	系统维护服务	ERP软件维护服务	XX公司	保障公司环境卫生	XX部门XXX系统	2010-2021	ERP部门	5	5	5	5	是	是
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	
											0	否	

软件资产

内部使用
Internal Used

保存部门	信息管理部
保存期限	产生日期+3年
保存方式	电子档

此处填写产生业务数据或影响业务数据的关键软件

编号	业务系统	资产类别	资产名称	生产商	归属处室	资产负责人	业务分类	描述	备份位置	机密性	完整性	可用性	资产价值	是否为重要资产
1	OA系统	数据库软件系统	OA系统主库数据库软件	Oralce	IT部门	XXX	OA系统业务	OA系统数据库系统	数据中心磁带机	5	5	5	5	是
2	ERP系统	数据库软件系统	ERP系统数据库	Oracle	ERP部门	XXX	ERP系统业务	ERP部门数据库系统	数据中心磁带机	5	5	5	5	是
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否
													0	否

易耗品领用单 Supplies Acquisition Form

存放位置 Location: 责任负责人 Responsible Person: 耗材类型 Tpye of Supplies:

序号 SN	物品名称 Item Title	品牌型号 Brand & Model	数量 QTY	领用人签字 Signature	领用日期 Date

固定资产领用单 Supplies Acquisition Form

存放位置 Location: 责任负责人 Responsible Person: 耗材类型 Tpye of Supplies:

序号 SN	物品名称 Item Title	品牌型号 Brand & Model	数量 QTY	领用人签字 Signature	领用日期 Date

存储介质报废申请表

<table>
<tr><td>申请部门</td><td colspan="2"></td><td>申请时间</td><td></td></tr>
<tr><td>报废原因</td><td colspan="4"></td></tr>
<tr><td>介质类型</td><td>密级</td><td colspan="2">责任人</td><td>序列号</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="5">部门领导意见：

签字：　　年 月 日</td></tr>
<tr><td>信息是否消除</td><td colspan="4">☐是
☐否
签字：　　年 月 日</td></tr>
<tr><td colspan="5">信息管理部意见：

签字：　　年 月 日</td></tr>
<tr><td>备注</td><td colspan="4">1、
本表适用于所有介质（光盘、硬盘、移动硬盘、U盘等）报废申请；
2、 除光盘外介质报废必须填写序列号，消除信息。
3、此表由信息技术部机房管理员留存归档。</td></tr>
</table>

备份恢复测试记录表

测试人		时间	
测试硬件环境			
测试软件应用系统			
记录测试过程			
恢复测试失败原因			
措施			
负责人签字			

厦门华锐莱普顿学校

CHIWAY REPTON SCHOOL XIAMEN

目录content

厦门华锐莱普顿学校
CHIWAY REPTON SCHOOL XIAMEN

PART 1

厦门华锐莱普顿学校
CHIWAY REPTON SCHOOL XIAMEN

PART 2

厦门华锐莱普顿学校
CHIWAY REPTON SCHOOL XIAMEN

感谢收看 Thank You

厦门华锐莱普顿学校
CHIWAY REPTON SCHOOL XIAMEN

联系我们

咨询电话

0592-2100886

24小时邮件咨询

admissions@chiway-repton.com

学校地址

厦门市集美区西滨路388号

附件十二　　系统变更申请表

申请部门：	
申请变更类型：	□功能完善　□系统缺陷修改　□统计报表生成 □OA 账户申请　□其他业务申请（请写明具体需求）
申请变更项目：	

原始内容：	
需求描述：	

审批部门意见	（签字）	信息管理部意见	（签字）

年　　月　　日

验收签字：