安 全 日 常 运 维 管 理

目录

[第一章 安全运维管理体系分析 4](#_Toc459882551)

[1.1 安全日常运维管理的必要性 4](#_Toc459882552)

[1.2 安全运维管理的技术支撑体系 5](#_Toc459882553)

[1.3 安全运维管理遵循的PDCA周期 6](#_Toc459882554)

[1.4 安全日常运维管理的目标 6](#_Toc459882555)

[第二章 帐户口令管理 8](#_Toc459882556)

[2.1 职责定义 9](#_Toc459882557)

[2.2 口令账号五个保密等级 9](#_Toc459882558)

[2.2.1 【最低等级】等级一 9](#_Toc459882559)

[2.2.2 【低等级】 等级二 10](#_Toc459882560)

[2.2.3 【中等级】 等级三 10](#_Toc459882561)

[2.2.4 【坚固级】 等级四 11](#_Toc459882562)

[2.2.5 【最高级】 等级五 12](#_Toc459882563)

[2.3 账号管理 13](#_Toc459882564)

[2.3.1 账号角色分配目的 13](#_Toc459882565)

[2.3.2 建立的原则 13](#_Toc459882566)

[2.3.3 账号建立的过程 14](#_Toc459882567)

[2.4 口令管理 16](#_Toc459882568)

[2.4.1 口令管理原则 16](#_Toc459882569)

[2.4.2 口令设置原则 17](#_Toc459882570)

[2.4.3 口令设置最低标准 18](#_Toc459882571)

[2.5 权限管理 19](#_Toc459882572)

[2.5.1 概述 19](#_Toc459882573)

[2.5.2 确定最小权限 19](#_Toc459882574)

[2.5.3 建立权限体系 20](#_Toc459882575)

[2.6 账号口令审计管理 21](#_Toc459882576)

[2.6.1 概述 21](#_Toc459882577)

[2.6.2 账号审查通用要求 22](#_Toc459882578)

[2.6.3 账号口令审计流程设计建议 23](#_Toc459882579)

[第三章 服务与端口 24](#_Toc459882580)

[3.1 什么是端口 24](#_Toc459882581)

[3.2 什么是服务 24](#_Toc459882582)

[3.3 端口安全配置 25](#_Toc459882583)

[3.4 常用端口列表 25](#_Toc459882584)

[第四章 操作系统安全 26](#_Toc459882585)

[4.1 用户密码策略 26](#_Toc459882586)

[4.2 系统防火墙策略 26](#_Toc459882587)

[4.3 用户组策略 26](#_Toc459882588)

[第五章 数据库安全 27](#_Toc459882589)

[5.1 数据库安全访问 27](#_Toc459882590)

[5.2 数据库用户和密码控制 27](#_Toc459882591)

[5.3 数据库权限控制 28](#_Toc459882592)

[5.4 数据库审计 28](#_Toc459882593)

[5.5 数据库备份 29](#_Toc459882594)

[第六章 应用程序安全 30](#_Toc459882595)

[6.1 文件审计 30](#_Toc459882596)

[6.2 程序操作审计 30](#_Toc459882597)

[6.3 程序登录帐号密码安全 30](#_Toc459882598)

[6.3 程序和数据备份 31](#_Toc459882599)

[第七章 安全补丁 32](#_Toc459882600)

[7.1 概述 32](#_Toc459882601)

[7.2 补丁安装与操作 32](#_Toc459882602)

[第八章 终端管理 33](#_Toc459882603)

[第九章 数据备份 35](#_Toc459882604)

[9.1 备份管理 35](#_Toc459882605)

[9.1.1 信息识别 35](#_Toc459882606)

[9.1.2 制定备份计划 35](#_Toc459882607)

[9.1.3 实施备份计划 36](#_Toc459882608)

[9.1.4 备份存放 37](#_Toc459882609)

[9.1.5 备份测试 37](#_Toc459882610)

[9.1.6 备份恢复 38](#_Toc459882611)

[9.2 数据恢复 38](#_Toc459882612)

# 第一章 安全运维管理体系分析

## 1.1 安全日常运维管理的必要性

IT系统是否能够正常运行直接关系到业务或生产是否能够正常运行。但IT管理人员经常面临的问题是：网络变慢了、设备发生故障、应用系统运行效率很低。IT系统的任何故障如果没有及时得到妥善处理都将会导致很大的影响，甚至会造成可怕的经济损失。但是什么原因导致IT系统屡出问题？是产品、技术、还是缺乏有效的、系统化的安全运维管理？

随着电信IT系统的发展，业务应用的持续增加，其IT基础设施的架构越来越复杂，单纯凭某个工具或某个人不可能有效地保护自己的整体网络安全;信息安全作为一个整体，需要把安全过程中的有关各层次的安全产品、分支机构、运营网络、管理维护制度等纳入一个紧密的统一安全管理平台（系统)中，才能有效地保障企业的网络和信息安全。

IT环境的复杂性，使更多的安全威胁被揭示出来。很多企业尝试通过部署“最佳”安全产品来保护自己，比如防病毒网关、防火墙、入侵防护系统、VPN、访问控制、身份认证等。在这种极度复杂的情况下，需要的是一个集成的解决方案，使得企业能够收集、关联和管理来自异类源的大量安全事件，实时监控和做出响应，需要的是能够轻松适应环境增长和变化的管理体系，需要的就是企业完整的安全管理平台解决方案。

总而言之，对于企业安全运维管理来说，三分技术，七分管理，在企业内部建立一套完善的安全管理规章制度，使管理机构依据相应的管理制度和管理流程对日常操作、运行维护、审计监督、文档管理等进行统一管理，同时加强对工作人员的安全知识和安全操作培训，建立统一的安全管理体系，帮助企业识别、管理和减少信息通常所面临的各种威胁，架构企业的安全保障体系。

## 安全运维管理的技术支撑体系

PPDRR模型包括策略（Policy）、防护（Protection）、检测（Detection）、响应（Response）和恢复（Recovery）5个主要部分，其中，防护、检测、响应和恢复构成一个完整的、动态的安全循环，在安全策略的指导下共同实现安全保障信息安全的重要理论模型包括信息安全的概念范畴、信息安全保障体系的结构框架、信息安全的三维结构和PPDRR模型

**安全监控和基础维护**

**安**

**全**

**技术**

**支撑**

**运维**

**策略**

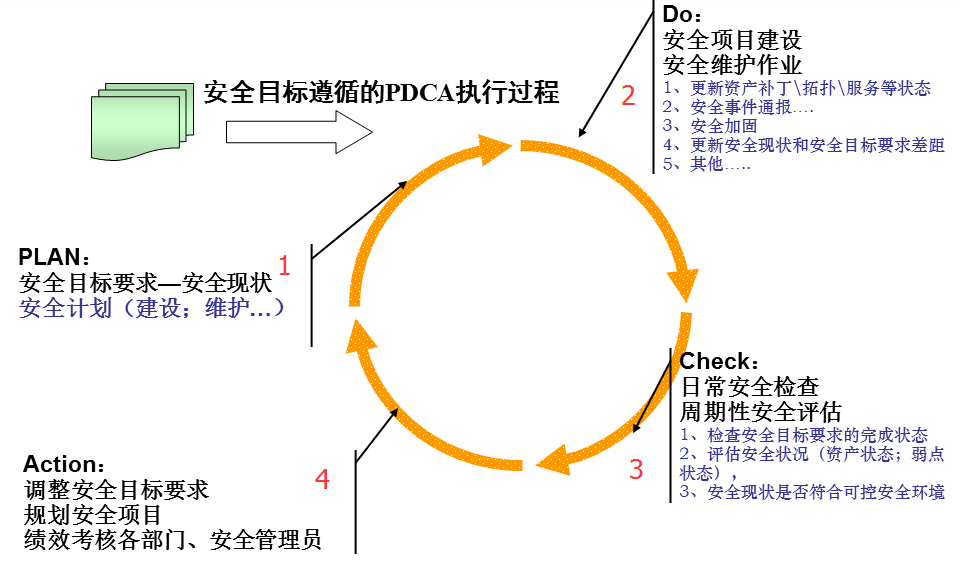
**安全监控和基础维护**

**安全技术**

**支撑**

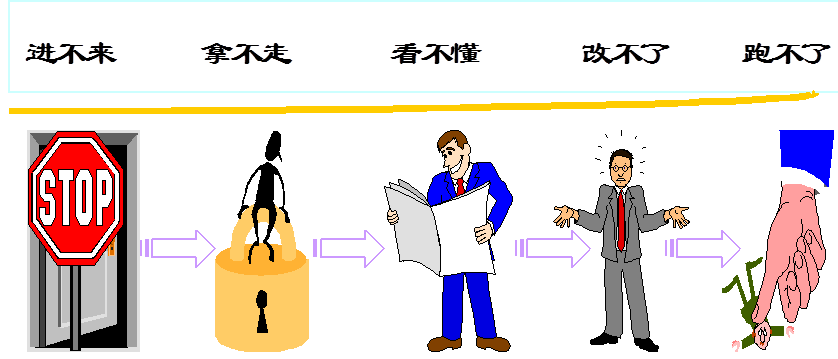
1. 制定网络和系统层面的整体安全技术保护方案和技术规范；
2. 逐步实现安全自评估，全面掌握安全风险；
3. 提供重大安全预警信息发布和解决方案；
4. 协调响应网络层面的各类重大安全事件；
5. 对各类安全事件有关数据进行综合分析，形成安全运行分析报告；
6. 对生产层面的安全策略进行集中控制；
7. 跟踪研究各种安全问题和技术，收集各种基础信息资源。
8. 进行7×24小时的日常安全安全事件监测，负责受理安全投诉。
9. 对安全事件进行收集汇总，进行事件预处理。
10. 系统日常口令维护，加载安全补丁和梳理服务端口等
11. 实施各类安全设备和配套管理设备的日常维护。
12. 实施一般安全预警和安全应急事件的处理。
13. 落实系统自身安全应急预案，并参加安全应急演练

## 1.3 安全运维管理遵循的PDCA周期



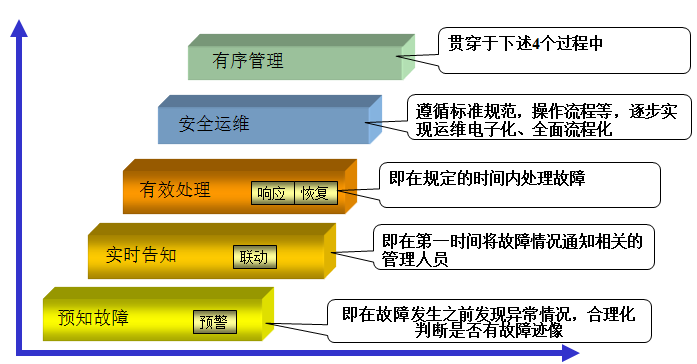
## 1.4 安全日常运维管理的目标

安全工作的目的就是为了在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，完成下述网络与信息安全的保障任务。



* 进不来：使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性
* 拿不走：使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实现对网络资 源及信息的可控性。
* 看不懂：使用加密机制，确保信息不泄漏给未授权的实体或进程，即“看不懂”，从而实现信息的保密性
* 改不了：使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其它人“改不了”，从而确保信息的完整性。
* 跑不了：使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者、抵赖者“走不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

为保障IT系统的正常运行，应能做到如下所示

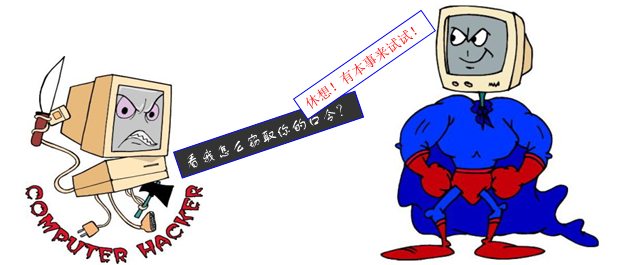


总结：安全日常运维管理可总结为**高效管理能力、全面运维能力、安全保护能力、隐患发现能力、应急响应能力、快速恢复能力**

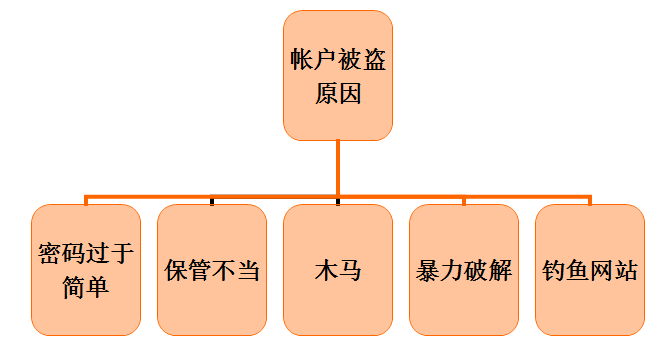
# 第二章 帐户口令管理

**为什么有这么多人钟情于窃取帐号口令？**

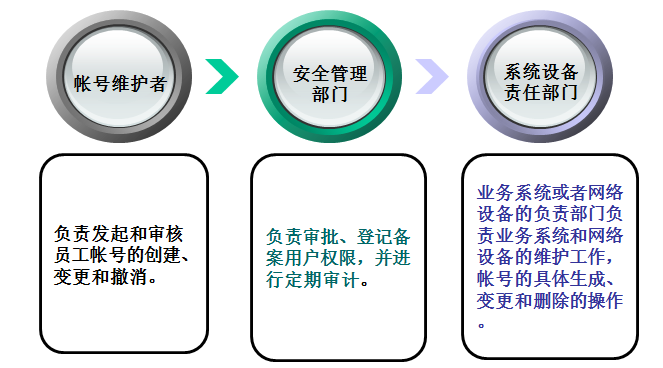
攻击者窃取帐号有着非法的目的、意图，恶意毁坏操作等行为，他们或以出名，或以炫耀技术为目的。而目前，窃取帐号的行为都与窃取商业机密和机密信息、数据、经济利益相关，大都有着利益化的倾向犯罪行为。



**帐号衩窃取的常见原因**



## 2.1 职责定义



## 2.2 口令账号五个保密等级

### 2.2.1 【最低等级】等级一

**只有基本的甚至没有保障措施，用于电子系统的帐号。**

在第一等级的保障的情况下，只有基本的甚至没有保障措施用于电子系统的帐号，等级一的情况下，错误的口令、帐号和权限管理可能导致给公司、客户或者第三方带来最小的不便。

不会给公司、客户或者第三方带来直接的经济损失

不会给公司、客户或者第三方带来不快

不会给公司、客户或者第三方带来名誉或者地位的损失

不会破坏公司、客户或者第三方需要执行的商业措施或者交易

不会导致民事或者刑事犯罪

不会向未经授权的组织或个人暴露个人、公司、政府、商业的敏感信息

未验收和未投入使用的系统，工程过程中的系统（假设没有涉及知识产权，例如软件代码泄密的问题的情况下）

### 2.2.2 【低等级】 等级二

**通过常用的措施即可保护系统的可信认证，必须充分考虑代价和认证安全性的平衡**

这种等级的认证被误用或者破坏可能导致：

给公司、客户或者第三方带来较小的不便

给公司、客户或者第三方带来较小直接的经济损失或者没有直接经济损失

会给公司、客户或者第三方带来较小的不快

会给公司、客户或者第三方带来较小名誉或者地位的损失

存在一定的风险，可能破坏公司、客户或者第三方需要执行的商业措施或者交易不会导致民事或者刑事犯罪。

存在一定风险，可能少量向未经授权的组织或个人暴露个人、公司、政府、商业的敏感信息

举例：

一台常用办公电脑，该电脑上没有存储任何机密文件，他的帐号被窃取可能导致公司常用信息例如通讯录被泄漏。一个有查询系统的帐号，用户可以通过Internet注册来查询自己的帐单。该帐号失窃可能导致用户信息的泄漏。

### 2.2.3 【中等级】 等级三

如果该级别的帐号被破坏，攻击者往往可以通过这种系统作为中转，进而对部分关键的系统主机进行破坏。这种级别的帐号口令虽然不是直接的业务系统或者数据库的帐号，但是，如果该级别的帐号被破坏，攻击者往往可以通过这种系统作为中转，进而对部分关键的系统主机进行破坏，该等级被误用的主要风险有：

通过中转可能给公司、客户或者第三方带来较大的不便

通过中转有可能给公司、客户或者第三方带来较大直接的经济损失或没有直接经济损失

通过中转会给公司、客户或者第三方带来较大的不快

通过中转会给公司、客户或者第三方带来较大名誉或者地位的损失

存在一定的风险，会破坏公司、客户或者第三方需要执行的商业措施或者交易

可能会导致民事或者刑事犯罪

存在一定风险，可能大量向未经授权的组织或个人暴露个人、公司、政府、商业的敏感信息

举例：

维护终端的用户帐号，由于一些业务系统会对终端做特定限制，维护终端被破坏后，导致攻击者可以进一步破坏业务系统，重要的可信网络设备的帐号等。

### 2.2.4 【坚固级】 等级四

通常等级四意味着正式的业务流程使用的帐号，通常需要较高信心来保证身份的认证和正确的授权。

通常等级四意味着正式的业务流程使用的帐号，通常需要较高信心来保证身份的认证和正确的授权，这种等级的认证被误用或者破坏可能导致：

给公司、客户或者第三方带来较大的不便

给公司、客户或者第三方带来较大直接的经济损失或者没有直接经济损失

会给公司、客户或者第三方带来较大的不快

会给公司、客户或者第三方带来较大名誉或者地位的损失

存在较大的风险，会破坏公司、客户或者第三方需要执行的商业措施或者交易

会导致民事或者刑事犯罪

存在较大风险，可能大量向未经授权的组织或个人暴露个人、公司、政府、商业的敏感信息

举例：一般的主机操作系统、数据库、和路由器的高权限帐号，例如root、administrator、dba等。业务系统的关键管理帐号，可以读写重要的用户信息、业务信息和帐单信息。

### 2.2.5 【最高级】 等级五

等级五的保障通常对应需要非常大的信心保障的系统。

等级五的保障通常对应需要非常大的信心保障的系统这种等级的认证被误用或者破坏可能导致：

给所有公司、客户或者第三方带来巨大的不便

给公司、客户或者第三方带来极大直接的经济损失或者没有直接经济损失

会给公司、客户或者第三方带来极大的不快

会给公司、客户或者第三方带来巨大名誉或者地位的损失

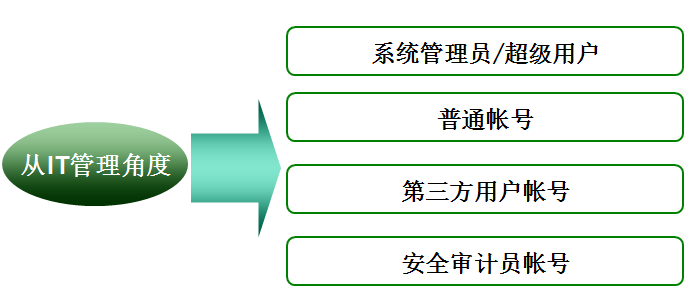
破坏公司、客户或者第三方需要执行的商业措施或者交易

会导致民事或者刑事犯罪

大量向未经授权的组织或个人暴露个人、公司、政府、商业的敏感信息

举例：关键系统，例如计费系统数据库主机的操作系统和数据库。用于存储公司最高商业机密或密级为绝密的系统的认证。

## 2.3 账号管理



### 2.3.1 账号角色分配目的

（一）加强网络与信息安全管理，明确各级系统用户权的职责。

（二）根据业务系统的要求及网络信息管理规范，进一步完善各级用户在系统中的职能划分与角色定位。

（三）强化系统帐户和密码的管理，降低帐户和密码泄漏对系统和数据安全产生的影响，确保各相关信息报告系统安全、有效运行。

系统管理员和超级用户是有权限对系统的配置、系统最核心信息进行更改的帐号和角色，

普通帐号是用户用于访问业务系统，实现日常业务操作的用户，是最为常见的用户类型，

第三方帐号通常指由于某种特殊情况，系统允许移动以外的人员和组织访问的帐号。

在核心系统中，应该设置安全审计员帐号，该帐号可以对系统安全设置和日志信息进行专门的审计。

### 2.3.2 建立的原则

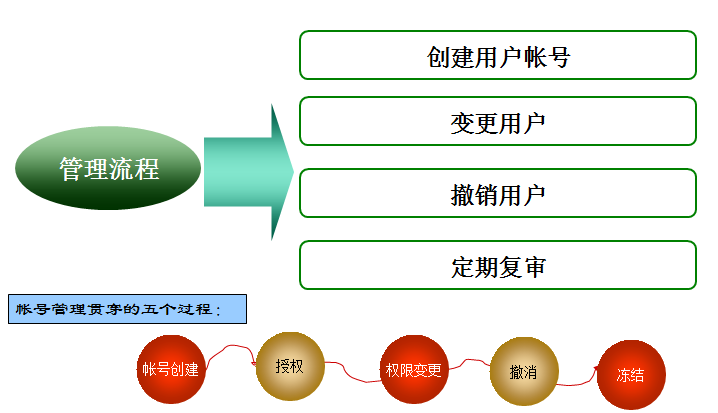
（1）不同类型用户的建立应遵循满足其工作需要的原则，而用户的权限分配则应以保障网络与信息的高效、准确、安全为原则。

（2）用户的权限分配应尽量使用系统提供的角色划分。如需特殊的操作权限，应在准确理解其各项操作内容的基础上，尽量避免和减少权限相互抵触、交叉及嵌套情况的发生，经测试成功后，再创建相应的角色赋予本级用户或直报用户。

（3）通过对用户进行角色划分，分配审计账号、用户权限，合理限制对其他角色用户、数据的修改权限，将审查数据与配置数据相对剥离，即原始配置数据与统计查看查看信息分开。

（4）系统内所有涉及查看数据的帐户信息均必须采用真实信息，即有查询机制确认审计人员信息准确。

### 2.3.3 账号建立的过程



**帐号管理贯穿帐号创建、授权、权限变更及帐号撤销或者冻结全过程**

* 帐号设置应与岗位职责相容；
* 坚持最小授权原则，避免超出工作职责的过度授权；
* 应制定严格的审批和授权流程，规范帐号申请、修改、删除等工作，授权审批记录应编号、留档（表格命名规则及格式参见附件，各省公司可重新制定相关表格）；
* 帐号创建、调整和删除申请审批通过后，应及时更新系统中的帐号状态，确保与审批结论保持一致；
* 原则上，除低权限的查询帐号外，各系统不允许存在其它共享帐号，必须明确每个帐号责任人，不得以部门或用户组作为最终责任人。
* 在完成特定任务后，系统管理员应立即收回临时帐号。

**帐号创建、变更、删除审批流程**

超级帐号由主管领导以授权的方式授予具体的系统管理员，授权书至少应包括系统名称、超级帐号名、授予人姓名、职责描述、有效期等；

所有帐号，包括系统管理员帐号、普通帐号、程序帐号的责任人，应按规定的申请表格式要求提出申请，申请表至少包含申请人姓名、联系方式、申请人职责描述、申请时间、申请目的、申请帐号所属系统名称、帐号类型、创建或者变更或者删除操作类型、帐号权限描述、主管领导审批意见、系统管理员变更操作记录及签字确认、权责描述备注栏目等；

主管领导进行审批，重点检查所申请权限与申请人职责的一致性；

系统管理员负责创建、变更或者删除帐号，保留审批表格、并备案。

**如因系统能力或者管理原因无法按用户创建帐号时，应采取如下管理措施：**

* 明确共享帐号责任人，责任人负责按照上述流程要求提出共享帐号审批表，并在审批表中注明该共享帐号的所有用户名单；
* 限制共享帐号的使用人数，建立相关管理制度保证系统的每项操作均可以对应到执行操作的具体人员；
* 限定使用范围和使用环境；
* 建立完善的操作记录制度，对交接班记录、重要操作记录表等等；
* 定期更新共享帐号密码。
* 对于程序运行或者程序自身由于管理需要访问其它系统所使用的专用帐号，应符合如下要求：
* 只允许系统和设备之间通信使用，不得作为用户登录帐号使用；
* 将此类帐号的维护管理权限统一授权给该系统的系统管理员，由后者归口管理；

## 2.4 口令管理

### 2.4.1 口令管理原则

* 口令至少由6位及以上大小写字母、数字及特殊符号等混合、随机组成，尽量不要以姓名、电话号码以及出生日期等作为口令或者口令的组成部分。
* 应以HASH或者加密技术保存口令，不得以明文方式保存或者传输；
* 口令至少每90天更换一次。修改口令时，须保留口令修改记录，包含帐号、修改时间、修改原因等，以备审计；
* 5次以内不得设置相同的口令；
* 由于员工离职等原因，原帐号不能删除或者需要重新赋予另一个人时，应修改相应帐号的口令。
* 如系统能力支持，应开启并设置自动拒绝不符合上述口令管理规则帐号和口令的参数；
* 对于无法建立口令规则强制检查的系统，帐号用户应在每次口令修改后留有记录。
* 对于无法进行定期修改口令的帐号，如内置帐号、专用帐号等，由系统管理员负责在系统升级或重启时督促落实口令修改工作，负责督促落实调用该帐号的程序与所访问系统两侧的口令同步工作。

当发生下述情况时，应立即撤销帐号或更改帐号口令，并做好记录：

* 帐号使用者由于岗位职责变动、离职等原因，不再需要原有访问权限时；
* 临时性或阶段性使用的帐号，在工作结束后；
* 帐号使用者违反了有关口令管理规定；

有迹象，表明口令可能已经泄露等。

### 2.4.2 口令设置原则

* 口令必须具有足够的长度和复杂度，使口令难于被猜测
* 口令在一定时间或次数内不能循环使用
* 不同帐号的口令应当不同，并且没有直接联系，以保证不可由一个帐号的口令推知其它帐号的口令
* 同一帐号前后两个口令之间的相同部分应当尽量减少，减低由前一个口令分析出后一个口令的机会
* 口令不应当取过于简单的字符串，如电话号码、使用者的姓名、宠物、生日或其倒序，6位字符都相同、6位连续字符等易于猜测的信息
* 开户时设定的初始口令必须是随机产生的口令，而不能是相同或者有规律的口令
* 所有系统管理员级别的口令（例如root、enable、NT administrator、DBA等）在没有使用增强口令的情况下，必需按照较短周期进行更改，例如每三个月更换一次。应该注意关键性帐号信息的定期行备份。
* 用户所使用的任何具备系统超级用户权限（包括并不限于系统管理员帐号和有sodu权限帐号）帐号口令必需和这个用户其他帐号的口令均不相同。
* 如果有双要素认证机制，则以上的要求和下面关于强口令选择的要求可以不考虑。
* 口令不能在电子邮件或者其他电子方式下以明文方式传输。
* 当使用SNMP时，communication string不允许使用缺省的Public、Private和system等，并且该communication string不应该和系统的其他口令相同，应该尽量使用SNMPv2以上的版本。

### 2.4.3 口令设置最低标准

* 如果技术上支持，口令至少要有6位长
* 口令必须是字母和非字母的组合
* 口令第1位和最后1位至少应包含1个非数字字符
* 与前次口令比较，在任何位置不能有超过3个字符连续相同
* 口令不能包含超过2个连续相同的字符
* 用户名不能作为口令一部分
* 与前4次相同的口令不能重复使用
* 口令不能被共享除非每个口令的行为都能被区分
* 对于级别要求很高的系统，普通用户口令要求8位以上
* 管理员/超级用户帐号最近20个口令不可重复，口令的长度不可小于7位，口令中必须包含大写字母、小写字母和数字中的两类，口令中同一个符号不得多于2次，且不得有1个以上的字符出现两次，前后2个口令中相同位置的字符相同的不得多于2个；口令不得有明显的意义修改
* 帐号的使用人应当定期修改帐号口令，修改口令的间隔应小于本标准的相关规定，对于本标准没有规定的用户，其间隔应当小于6个月
* 不同用户的修改口令的最大间隔为：

1) 普通帐号应当小于6个月

2) 管理员帐号和超级管理员帐号应当小于3个月

* 匿名用户帐号可以不修改口令

## 2.5 权限管理

### 2.5.1 概述

按照“谁主管，谁负责”、“谁使用、谁负责”、所有帐号均应落实责任人的原则制定本办法。

帐号和口令管理包括基于帐号的操作或访问控制权限的管理。帐号是作为访问的主体。而基于帐号进行操作的目标就是访问的客体。通常这个客体被当成为资源。

对资源的访问控制权限的设定依不同的系统而不同。从移动帐号管理的角度，可以进行基于角色的访问控制权限的设定。即对资源的访问控制权限是以角色或组为单位进行授予。

### 2.5.2 确定最小权限

1、所谓最小特权（Least Privilege），指的是“在完成某种操作时所赋予网络中每个主体（用户或进程）必不可少的特权”。最小特权原则，则是指“应限定网络中每个主体所必须的最小特权，确保可能的事故、错误、网络部件的篡改等原因造成的损失最小”。   
2、最小特权原则一方面给予主体“必不可少”的特权，这就保证了所有的主体都能在所赋予的特权之下完成所需要完成的任务或操作；另一方面，它只给予主体“必不可少”的特权，这就限制了每个主体所能进行的操作。   
最小特权原则要求每个用户和程序在操作时应当使用尽可能少的特权，而角色允许主体以参与某特定工作所需要的最小特权去签入（Sign）系统。被授权拥有强力角色（Powerful Roles）的主体，不需要动辄运用到其所有的特权，只有在那些特权有实际需求时，主体才去运用它们。如此一来，将可减少由于不注意的错误或是侵入者假装合法主体所造成的损坏发生，限制了事故、错误或攻击带来的危害。它还减少了特权程序之间潜在的相互作用，从而使对特权无意的、没必要的或不适当的使用不太可能发生。这种想法还可以引申到程序内部：只有程序中需要那些特权的最小部分才拥有特权。

3、基于角色的访问控制是一种新型访问控制模型，它的基本思想是将权限与角色联系起来，在系统中根据应用的需要为不同的工作岗位创建相应的角色，同时根据用户职务和责任指派合适的角色，用户通过所指派的角色获得相应的权限，实现对文件的访问。它支持最小特权、责任分离以及数据抽象三个基本的安全原则。

4、最小权限原则规定：每个用户/任务/应用在必需知情的前提下被赋予明确的访问对象和模块的权限。遵循最小权限原则运行的系统要求授予用户访问对象的明确权限。准许或拒绝访问数据库或服务器对象的第一步是认证和授权

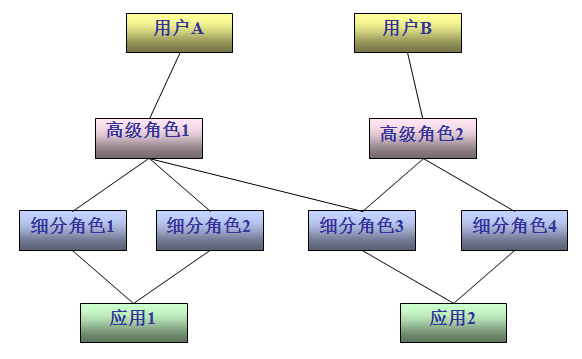
* 对帐号的授权，应以其能进行系统管理、操作的最小权限进行授权。比如这个帐号作为系统帐号只能进行数据备份的操作，那就只授权其可以进行数据备份操作的命令。别的诸如进行系统网络状态监控的命令则不授权其可以进行。
* 对于授权，应该支持一定的授权粒度控制，从而控制用户的访问对象和访问行为，保证用户的最小授权。

### 2.5.3 建立权限体系

基于角色访问控制（RBAC）模型是目前国际上流行的先进的安全访问控制方法。它通过分配和取消角色来完成用户权限的授予和取消，并且提供角色分配规则。安全管理人员根据需要定义各种角色，并设置合适的访问权限，而用户根据其责任和资历再被指派为不同的角色。这样，整个访问控制过程就分成两个部分，即访问权限与角色相关联，角色再与用户关联，从而实现了用户与访问权限的逻辑分离。

　　由于实现了用户与访问权限的逻辑分离，基于角色的策略极大的方便了权限管理。例如，如果一个用户的职位发生变化，只要将用户当前的角色去掉，加入代表新职务或新任务的角色即可。研究表明，角色/权限之间的变化比角色/用户关系之间的变化相对要慢得多，并且给用户分配角色不需要很多技术，可以由行政管理人员来执行，而给角色配置权限的工作比较复杂，需要一定的技术，可以由专门的技术人员来承担，但是不给他们给用户分配角色的权限，这与现实中的情况正好一致。

　　基于角色访问控制可以很好的描述角色层次关系，实现最小特权原则和职责分离原则



## 2.6 账号口令审计管理

### 2.6.1 概述

号口令管理的执行情况，在很大程度上取决于帐号口令审查的监督力度。在公司内部推行帐号口令管理制度的很大一部分工作需要通过不断的监督、审查再配合相关的奖惩规定来保证。因此完善的帐号口令审查制度对于整个帐号口令管理至关重要。

### 2.6.2 账号审查通用要求

* 对于保障等级一、二类帐号的普通用户，可以根据实际情况决定是否进行定期审查
* 对于保障等级一、二类帐号的超级用户，定期审查的时间间隔不超过六个月
* 对于保障等级三、四类帐号的普通用户，定期审查的时间间隔不超过三个月
* 对于保障等级四、四类帐号的超级用户，定期审查的时间间隔不超过一个月
* 对于保障等级五类帐号的所有用户，定期查的时间间隔不超过一个月
* 任何变化发生后应进行审查，如：发生非法入侵、人员变动等；
* 对于审查过程中出现的多余、闲置或非法的帐户，应及时予以冻结或删除
* 对核查中发现的问题，应督促相关人员采取必要措施予以纠正通用原则
* 对于已经实施集中认证系统，审计的主要工作是对于认证和授权的日志进行检查，审核是否有非法登陆事件，是否有越权使用的行为等
* 对于操作系统级的帐号口令审计分为两种：第一种可以设置帐号登陆和权限使用事件的追踪，这种帐号口令的审计也是对系统日志和防火墙等访问控制设备日志的审计；对于不能实现帐号登录和权限追踪的系统，需要人工进行审计，应该根据业务系统的属性制定详细的审计checklist，由专门的安全组织进行定期或者不定期的帐号随机抽查审计
* 对于应用系统的帐号审计工作也是参照操作系统的分类进行处理
* 对于网络设备的帐号审计工作，由于大部分的设备帐号都是没有日志记录的，所以主要审计方式是人工审计，由专门的信息安全组织根据设备的风险等级规定审计的频度和审计的checklist
* 审计checklist的内容主要依据审计对象的帐号口令管理规定制作，审计的关键点是帐号口令的复杂度，权限，更改的要求等等
* 在制作审计checklist设计的时候，需要区别不同业务系统不同级别帐号的差异，对于关键业务系统和关键帐号的审计频度和审计的内容要求更加严格
* 审计的结果应该和奖惩规定挂钩，对于多次审计不合格或者优秀的员工和分公司要按照奖惩规定进行相应的奖惩
* 专门的信息安全部门或者组织应该对审计的结果定期进行公布，力争将审计的威慑力逐步提高，让帐号使用者提高安全使用帐号口令的意识

### 2.6.3 账号口令审计流程设计建议

* 帐号口令的审计流程以业务系统的风险等级做为差异定制，针对不同的风险等级制定不同的审计checklist
* 帐号口令的审计可以结合现有的IT技术，尽可能通过日志文件等方式进行审计，但是有部分系统没法提供电子审计对象，对于高风险等级的系统，必须制定替代的审计方法，包括手工的方法
* 帐号口令审计工作应该以省为单位由省公司安全部门牵头，各业务系统维护单位负责的方式，涉及难以实现电子化审计的，省安全审计负责人应该制定一些不定期抽查制度，对于抽查中出现的与审计不符合的情况，应结合奖惩规从严处理
* 帐号口令管理流程中需要考虑相应的组织建立，可以明确责任的，确定责任人，不能落实到人的，落实到部门的安全相应领导
* 帐号口令审计后应该将审计结果及时公布，对于违规和表现良好的可以进行典型案例的宣传，起到增强员工帐号口令安全意识的作用

# 第三章 服务与端口

## 3.1 什么是端口

什么是端口号，一个端口就是一个潜在的通讯通道，也是一个入侵通道，开放一个端口就是一台计算机在网络上打开了一扇窗户，黑客入侵的方法就是用手工扫描或利用扫描软件找到服务器所开放的端口，去根据其相应的漏洞对服务器进行入侵或攻击，因此对端口的了解是非常重要的。

按对应的协议类型，端口有两种：TCP端口和UDP端口。由于TCP和UDP 两个协议是独立的，因此各自的端口号也相互独立，比如TCP有235端口，UDP也 可以有235端口，两者并不冲突。

端口号只有整数，范围是从0 到65535

## 3.2 什么是服务

一台拥有IP地址的主机可以提供许多服务，比如Web服务、ftp服务、SMTP服务等，这些服务完全可以通过1个IP地址来实现。那么，主机是怎样区分不同的网络服务呢？显然不能只靠IP地址，因为IP地址与网络服务的关系是一对多的关系。实际上是通过“IP地址+端口号”来区分不同的服务的。

需要注意的是，端口并不是一一对应的。比如你的电脑作为客户机访 问一台WWW服务器时，WWW服务器使用“80”端口与你的电脑通信，但你的电脑则可能使用“3457”这样的端口

* 端口都有确切的定义，对应着相应的服务，每一个打开的端口，都代表一个系统服务。
* 例如，80端口就代表Web服务。21对应着FTP，25对应着SMTP、110对应着POP3等。
* 动态端口(从1024到65535) 当你需要与别人通信时，Windows会从1024起，在本机上分配一个动态端口，如果1024端口未关闭，再需要端口时就会分配1025端口供你使用，依此类推。
* 但是有个别的系统服务会绑定在1024到49151的端口上，例如3389端口(远程终端服务)。从49152到65535这一段端口，通常没有捆绑系统服务，允许Windows动态分配给你使用。

## 3.3 端口安全配置

* Windows中开启系统防火墙，过滤掉非必要的端口，如非必要，不对外映射公网端口，一样要映射，需在防火墙上设置好安全策略（可以的话设置只对指定IP或IP段开放公网端口访问权限）
* Linux中开启iptables，过滤相关协议和端口，同样需要对公网开放权限时，遵循第一点的要求

## 3.4 常用端口列表



# 第四章 操作系统安全

## 4.1 用户密码策略

* 禁用GUEST用户
* 开启系统密码强度

## 4.2 系统防火墙策略

## 4.3 用户组策略

# 第五章 数据库安全

数据库安全主要包含数据库访问、数据库文件备份、数据库用户密码、数据库权限的控制和数据库审计这几大块

## 5.1 数据库安全访问

* 关闭互联网访问权限，修改默认端口
* 确保指定主机才有访问权限，并且控制访问用户的操作权限，赋予最小权限
* 不允许免密码登录(my.cnf中配置skip-grant-tables)和直接将密码明文配置到my.cnf配置文件中

## 5.2 数据库用户和密码控制

* 禁用超级管理员用户(mysql为root,sql server为sa)，另外新建其他用户替代超级管理员用户。例如新建DBA用户，赋予grant权限
* 删除空密码用户，删除默认用户，对于mysql使用host精确匹配，删除所有%匹配的用户
* 密码的设置请参照2.4.2口令设置原则，不允许设置空密码
* 对于新系统前期立项，需要告知需求，走流程申请新增数据库及用户，每个项目单独分配一个指定用户，并且评估需要的权限，密码按规定强度设置（一般为数字，大小写字母和特殊字符的组合，不能少于8个字符）
* 备份脚本及my.cnf文件中不能配置密码明文
* 对于过期的用户或者已经下线产品用户，要先revoke用户权限，再做drop user操作。

直接做drop user操作，权限不会回收，下次建相同用户名的user，这些权限还是存在，这个只适用Mysql

## 5.3 数据库权限控制

* 程序中涉及到数据库的研发（例如：触发器、存储过程、函数和视图），代码生成都必须基于分配的用户创建(这点主要针对mysql)
* 每个项目默认分配的用户根据需求评估赋予最小化权限，后期需要提升权限，要走流程申请
* 只有DBA用户具有all privileges和grant privileges，并且只支持localhost或指定内网IP登录，其他用户一律最小化权限。例如只给分配select,insert权限

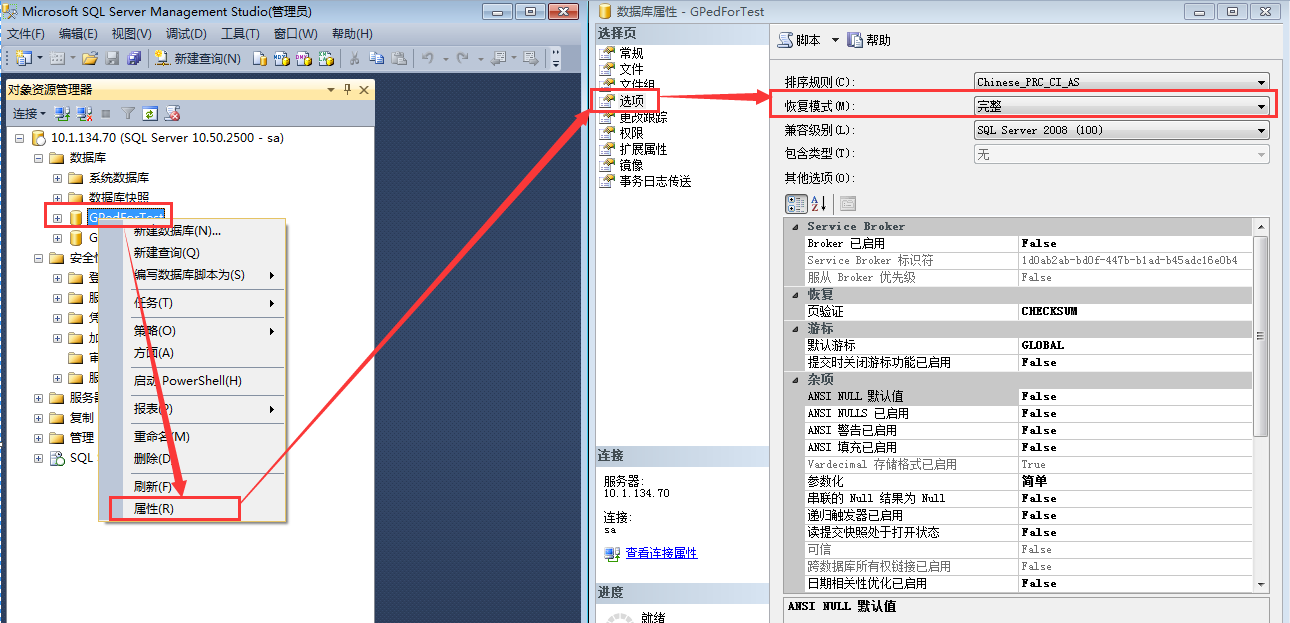
## 5.4 数据库审计

对于Mysql数据库：

* 开启binlog
* 开启数据库审计功能（mysql5.5以前的版本默认不支持审计，5.6版本才完善,不过貌似企业版才支持，有待验证）

对于sql server数据库：

* 数据库日志模式开启为完整模式



* 开启数据库审计功能，默认sql server 2008就自带，具体功能有待验证

## 5.5 数据库备份

关于备份请参考“第九章 数据备份”

# 第六章 应用程序安全

应用程序安全主要包含程序文件审计、程序操作审计、程序登录帐号密码安全和程序和数据备份

## 6.1 文件审计

文件审计主要记录应用所涉及的文件的操作，例如：新增，删除，更新等。需要记录谁，什么时间，做了什么操作，以log的形式存在。具体实现参照如下链接：

<https://help.aliyun.com/knowledge_detail/41069.html>

## 6.2 程序操作审计

程序的操作审计主要是指哪个IP，什么时候，用哪个用户登录了系统，在系统里面做了什么操作，这种Log建议存储到数据库的表中，方便select。

最好还能实现IP访问黑白名单配置

关于具体的实现，需要研发协助做功能开发。

## 6.3 程序登录帐号密码安全

* 帐号和密码必须满足一定的复杂度，并且不能有规律
* 新增密码强度判断功能，密码的设置和更新必须做复杂度判断，判断是否符合安全级别
* 新增用户必须包括密码设置界面，如果没有，登录前一定要提示修改密码，并且密码得满足要求的安全级别（这个主要是针对智慧校园，因为智慧校园新增的学生和老师信息都可以作为用户进行登录，并且默认密码都是000000，安全级别太低。但是若其他系统也是这样，也必须得做相应修改）
* 新增用户过期功能，新增用户时默认有个使用期限，到期前1周进行提醒，如要续期则走申请流程，不续期则禁用，禁用1个月还没进行申请从新开通的，直接删除该用户

## 6.3 程序和数据备份

关于备份请参考“第九章 数据备份”

# 第七章 安全补丁

## 7.1 概述

信息系统的基础构成是PC、网络、业务系统等，随着病毒和漏洞的结合，CodeRed、Nimda、SQLSlammer、Blaster蠕虫、僵尸、漏洞等对网络甚至经济都造成了严重的影响。这些漏洞造成的危害 ，是利用了操作系统或者应用程序、设备的漏洞，而消除漏洞的常规办法就是安装补丁。

## 7.2 补丁安装与操作

这块操作可向信息中心请教具体操作

# 第八章 终端管理

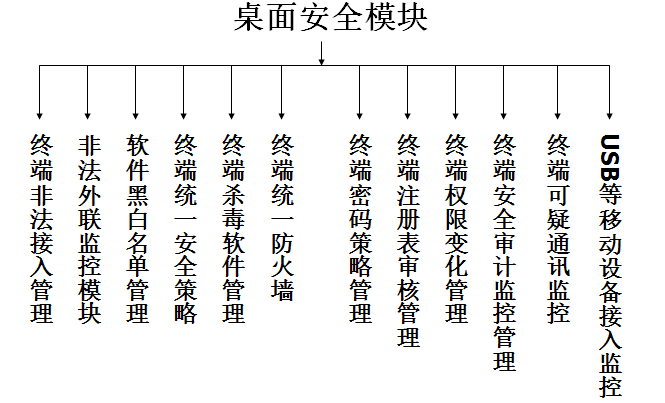
以往提起信息安全，人们更多地把注意力集中在防火墙、防病毒、IDS（入侵检测）、网络互联设备即对交换机、集线器和路由器等的管理，却忽略了对网络环境中的计算单元—服务器、台式机乃至便携机的管理。正确、全面的认识终端桌面管理的发展趋势和技术特点，是IT研发厂商面临的发展抉择，同时也是企、事业IT管理人员和高层决策人员在进行终端桌面安全防护部署时必须考虑的议题。

终端桌面安全管理技术的兴起是伴随着网络管理事务密集度的增加，作为网络管理技术的边缘产物而衍生的，它同传统安全防御体系的缺陷相关联，是传统网络安全防范体系的补充，也是未来网络安全防范体系重要的组成部分。因此，终端桌面安全管理技术无论在现在还是未来都应当归入基础网络安全产品体系之列。

近两年的安全防御调查也表明，政府、企业单位中超过80%的管理和安全问题来自终端，计算机终端广泛涉及每个用户，由于其分散性、不被重视、安全手段缺乏的特点，已成为信息安全体系的薄弱环节。因此，网络安全呈现出了新的发展趋势，安全战场已经逐步由核心与主干的防护，转向网络边缘的每一个终端。

建立桌面计算机安全管理系统的意义在于：解决大批量的计算机安全管理问题。具体来说，这些问题包括：加强桌面计算机的安全性，例如：通过批量设置计算机的安全保护措施提高桌面计算机的安全性，及时更新桌面计算机的安全补丁，减少被攻击的可能；实现动态安全评估，实时评估计算机的安全状态及其是否符合管理规定，例如：评估计算机的网络流量是否异常，评估计算机是否做了非法操作（拨号上网、安装游戏软件等），评估计算机的安全设置是否合理等；批量管理设置计算机，例如：进行批量的软件安装、批量的安全设置等；防止外来电脑非法接入，避免网络安全遭受破坏或者信息泄密；确保本单位的计算机使用制度得到落实，例如：禁止拨号上网，禁止使用外部邮箱，禁止访问非法网站，禁止将单位机密文件复制、发送到外部等；出现安全问题后，可以对有问题的IP/MAC/主机名等进行快速的定位；实现计算机的资产管理和控制。

管理措施如下图所示：



# 第九章 数据备份

## 9.1 备份管理

### 9.1.1 信息识别

* 内容：确定本部门/业务系统需要备份的电子数据。
* 标准：识别重要的信息资产，或信息资产的子系统相关的数据。
* 操作：收集需要备份的资产的相关信息，主要包括信息资产的名称、重要性、资产的保护级别等属性，填写《信息备份识别清单》。需要检查的信息资产可能包括：

1. 生产机上运行的应用系统软件源代码；
2. 数据库结构（表结构、存储过程、视图、索引、函数等）
3. 业务运作数据；
4. 系统配置参数；
5. 日志文件。

* 关键点：具体是否需要备份，还要看信息是否被损坏的威胁程度。
* 特情处理：无法备份的信息，尽量多使用其复制件，而保存原件。

### 9.1.2 制定备份计划

* 内容：填写《信息备份计划》。
* 标准：计划符合信息本身的特点，完整填写《信息备份计划》中的每一项。
* 关键点：选择合适的备份方式与周期。
* 特情处理：责任人没有足够的工具或条件可要求相关的工程师协助。
* 操作：根据资产识别的《信息备份识别清单》，制定《信息备份计划》，备份计划具体包括：

1. 确定备份周期：根据信息更新速度，易损坏程度，及备份媒体的有效期，确定备份周期。另外，在相关业务每次重大行动之前，以及每年年底的最后一天，也需要进行备份。
2. 备份介质类型：确定备份使用的媒体，一般是电子信息光碟，软盘、硬盘或磁带库，要同时考虑成本与可靠性。
3. 备份方式：一般要采用复制，双系统同步，转储，压缩复制等。
4. 备份工具：备份使用的工具，如光盘刻录机、复印机、软驱、压缩软件、磁带机，选择工具时，要确定在信息失效之前，对应的恢复工具可用。
5. 份数：确定备份的数量，一般信息备份一份即可，对于特别重要的信息需要备份多份。
6. 存放位置：备份信息一般应与原始信息尽量分开存放，要根据信息保密级别有相应的保密措施。
7. 责任人：确定备份的责任人。
8. 备份计划应提交给相关部门负责人，经部门负责人确认并批准后予以实施。

### 9.1.3 实施备份计划

* 内容：执行《信息备份计划》的计划。
* 标准：计划规定的周期与备份方式。
* 操作：对于分散的信息整理、归类；执行备份程序，检查备份数据的可用性；清理过程中的临时数据，填写完整的《信息备份记录》。
* 关键点：信息备份要保证完整性，同时保证信息在备份过程中的保密。
* 特情处理：如果是绝密信息，可通过特殊方式来进行处理。

### 9.1.4 备份存放

* 内容：将备份的媒体存放在安全位置。
* 标准：存放位置应符合软件管理程序的规定。
* 操作：备份完毕，备份操作员需向部门负责人或备份管理人员提交备份结果，包括：备份使用的媒体，备份过程中的相关文件，如：备份记录文件、备份恢复工具或软件、备份恢复指导书等；将备份媒体保存到《信息备份计划》中指定的位置，一般要按时间顺序存放。媒体的存储主要考虑以下几个方面：

1. 对业务影响重大的关键备份媒体要异地存储，以避免主要场地发生灾难时损坏备份媒体。比如可保存到银行保险柜中；一般的备份媒体或数据可保存在信息中心的防磁柜中；
2. 涉及公司秘密的备份信息或保密性十分重要的备份信息，备份应通过加密方法进行保护；
3. 分配专人（如设备管理员）对备份媒体进行管理，对备份媒体的访问进行控制。

* 关键点：存储场地的物理环境等因素要符合备份媒体的存储条件。

### 9.1.5 备份测试

* 内容：对备份的信息，定期抽样检查与测试。
* 标准：每种媒体类型，一次抽检二个以上。
* 操作：要定期测试备份媒体，以确保当需要应急使用时，可以依靠这些备份媒体来恢复数据；恢复程序应定期检查和测试，以确保有效，并能在合理的恢复时间内完成。
* 关键点：本次抽检时，要选择与上次抽检不同的媒体。

### 9.1.6 备份恢复

* 内容：在原始数据不可用时，用备份数据恢复原始数据。
* 标准：恢复后的数据能正常实现原有功能。
* 操作：当重要信息被篡改、破坏或丢失时，使用备份数据恢复信息；当存在多份备份时，应根据需要选择合适的备份；备份信息使用前，应检查备份信息的完整性和可用性。
* 关键点：备份媒体使用完毕，应按规定安全返还到备份地点。
* 特情处理：如果备份信息不可用，要有相应的处理计划。

## 9.2 数据恢复

* 目的：使用备份数据恢复被损坏或丢失的业务数据，保证业务系统数据的完整性和可用性。
* 适用范围：已进行备份的业务数据
* 职责：由系统部、业务部负责进行业务数据的恢复。
* 操作程序：数据恢复申请 -> 申请审批 -> 实施数据恢复 -> 结果检查