目　录

第一章

信息系统安全防护工作执行标准

文 件 名	信息安全系统管理标准要求		
电子文件编码	AQGL-A01-001	序　码	2 - 1

一、信息安全系统管理的重要性

信息安全管理是安全管理系统的一个重要内容。信息管理与危险分析、决策制订、工作反馈、系统运行等安全系统的主要功能关系极为密切。建立良好的信息管理系统，对于进行事故统计分析，找出事故的根本原因；对于进行系统安全分析，提供定量分析所需的信息、数据；对于提高产品安全水平，从而全面地提高企业安全生产水平，都有十分重大意义。

二、信息安全系统管理具体要求

1. 确定安全信息的需要，即确定需要多少信息，如何、什么时候及由谁来使用这些信息，信息传递方式等。

2. 就是确定安全信息来源的可靠性，数据的准确性和有效性等。

3. 把收集的信息和数据加以编选提练和编减并分类排除，向管理人员提供有关只与他们特定任务的信息。

4. 把正确的信息及时、适时地提供给有关管理部门或人员，实行信息资料共享。

5. 对各类具体保存价值的信息应利用计算机或资料存档进行存储，以备必要时可以再次使用这些信息。

6. 将处理后的信息根据其准确性、传递方式及时加以使用。

7. 信息安全管理应适应现行安全管理体制和决策的需要。

8. 信息安全管理应具有统一性、经济性，实行集中指挥、分

执行部门		责任人（签名）	

文 件 名	信息安全系统管理标准要求		
电子文件编码	AQGL-A01-001	序　码	2 - 2

层管理。

9.信息安全管理应实现标准化，各种报表、文字、符号等信息传递媒介均应标准化。

10.信息安全的传递和处理要努力做到环节少、流程短、速度快、效率高。还应实行循环，即信息源发出的信息流收并处理输出后必须再返回信息源。

执行部门		责任人（ 签名）	

文 件 名	信息管理系统构建执行标准		
电子文件编码	AQGL-A01-002	序　码	2 - 1

一、信息管理系统构建原则

1.信息系统的建立应以企业的安技部门为信息管理核心。并以上层领导部门，各职能科室、各生产单位为内部信息网点，以上级部门等为外部信息网点，在信息中心和网点之间应实行单向或双向传递。

2.安技部门应专(兼)职安全信息员，各网点由安技员兼任安全信息员。

3.中心与各网点应该通过人员、报表等进行定期的有组织的联系。

4.设计的系统尽可能简单，缩短处理过程，减少有关费用。

5.系统应保证外部环境、内部条件发生变化以后，仍能提供详尽、准确的信息。

6.系统输入、输出形式，传递语言要统一，以有利于各种系统间的协作。

7.设计系统时要计算对系统的投资和运行费用的支出，并比较所获效益。选择即经济又能达到目标的手段。

二、信息管理系统构成

1.信息源

可分为内部信息源和外部信息源两种。

(1)外部信息源主要有国内外有关部门、上级有关部门。

(2)内部信息源是安全信息源的主体，主要有领导部门、职能

执行部门		责任人(签名)	

文 件 名	信息管理系统构建执行标准		
电子文件编码	AQGL-A01-002	序　码	2 - 2

科室、生产现场等，其中应着重于生产、计划、机动、维修、设计、工艺、基建、技改、运输、供应等部门及车间、班级。

2. 信息处理系统

一般包括四部分：

(1)用于收集、选择和记录有关安全数据、资料的数据采集装置。

(2)用于整理、计算和处理数据、资料的数据变换装置。

(3)将数据从信息源输送到处理中心和将信息从处理中心输送给接收者的数据传输装置。

(4)存贮数据和信息以供随时提取的数据存贮和检索装置。

3. 信息管理者

即为负责管理安全信息系统的设计、运行，使其他单元协调配合的有关人员。

4. 信息接收器

主要包括存贮媒体和用户两个部分。

执行部门		责任人（ 签名）	

文 件 名	信息系统安全风险确认标准		
电子文件编码	AQGL-A01-003	序　码	5 - 1

一般认为，信息系统风险是系统脆弱性和/或漏洞，以及以系统为目标的威胁和/或威胁的总称。系统脆弱性和/或漏洞是风险产生的原因，威胁或攻击是风险的结果。从另一个角度看，风险的客体是系统脆弱性和/或漏洞，风险的主体是针对客体的威胁或攻击。可见，当风险的因果或主客体在时空上一致时，风险就危及或破坏了系统安全，或者说信息系统处于不稳定、不安全状态中。这种情况正是信息系统安全必须规避的。

一、信息系统组件固有的缺陷和脆弱性

1.硬件系统

信息系统硬件组件的安全隐患多来源于设计，这些问题主要表现为物理安全方面的问题。由于这种问题是固有的，一般除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此在自制硬件和选购硬件时应尽可能减少或消除这类安全隐患。

2.软件组件

软件组件的安全隐患来源于设计和软件工程中的问题。

(1)软件设计中的疏忽可能留下安全漏洞，如软件设计中不必要的功能冗余以及软件过长过大，不可避免地存在安全脆弱性；软件设计不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所要求的安全级别等。

(2)软件工程实现中造成的软件系统内部逻辑混乱，导致垃圾软件，这种软件从安全角度看是绝对不可用的。

执行部门		责任人(签名)	

文 件 名	信息系统安全风险确认标准		
电子文件编码	AQGL-A01-003	序　码	5 - 2

3.网络和通信协议

在当今的网络通信协议中，局域网和专用网络的通信协议具有相对封闭性，因为它直接与异构网络连接和通信。这样的 封闭'网络本身基于两个原因比开放式的因特网的安全特性好，一是网络体系的相对封闭性，降低了从外部网络或站点直接攻入系统的可能性，但信息的电磁泄露性和基于协议分折的搭线截获问题仍然存在；二是专用网络自身具有效为完善、成熟的身份鉴别、访问控制和权限分割等安全机制。

安全问题最多的，还是基于TCP/IP协议栈的因特网及其通信协议。因为因特网本身是一个没有明确物理界线的网际，其中的国与国之间、组织与组织之间和个人与个人之间的网络界限是依靠协议、约定和管理关系进行逻辑划分的，因而是一种虚拟的网络现实；而且支持因特网运行的TCP/IP协议栈原本只考虑互连互通和资源共享的问题，并未考虑也无法兼容解决。

对数据通信系统的威胁包括：信息的泄露；对信息的滥用、讹用或篡改信息或网络资源的被窃、删除或丢失；对信息或网络资源的破坏；服务的中断和禁止。

威胁主要分为以下几类：

(1)偶发性威胁

偶发性威胁是指那些不带预谋企图的威胁。偶发性威胁的实例包括系统故障，操作失误和软件出错。

(2)故意性威胁

执行部门		责任人(签名)	

文 件 名	信息系统安全风险确认标准		
电子文件编码	AQGL-A01-003	序　码	5 - 3

故意性威胁的范围，可从使用易行的监视工具进行随意的检验，到使用特别的系统知识进行精心策划的攻击。一种故意的威胁如果实现就可认为是一种 攻击 ”。

(3)主动性威胁

对系统的主动性威胁涉及到对系统中所含信息的篡改，或对系统的状态或操作的改变。一个非授权的用户不怀好意地改动路由选择表就是主动威胁的一个例子。

(4)被动性威胁

被动性威胁是指这样一些威胁，它的实现不会导致对系统中所含信息的任何篡改，而且系统的操作与状态也不受改变。使用消极的搭线窃听办法以观察在通信线路上传送的信息就是被动性威胁的一种实现。

二、攻击分类

1.服务拒绝

当一个实体不能执行它的正当功能，或它的动作妨碍了别的实体执行它们的正当功能的时候便发生服务拒绝。这种攻击可能是一般性的，比如一个实体抑制所有的消息，也可能是有具体目标的，例如一个实体抑制所有流向某一特定目的端的消息，如安全审计服务消息；这种攻击可以是对通信业务流的抑制，如本例中所述，或产生额外的通信业务流；也可能抑造出试图破坏网络操作的信息，特别是如果网络具有中继实体，这些中继实体根据

执行部门		责任人（ 签名）	

文 件 名	信息系统安全风险确认标准		
电子文件编码	AQGL-A01-003	序　码	5 - 4

从别的中继实体那里接收到的状态报告来作出路由选择的决定。

2. 外部攻击

外部攻击可以使用的方法包括：搭线(主动的与被动的)；截获辐射；冒充为系统的授权用户或冒充为系统的组成部分；为鉴别或访问控制机制设置旁路。

3. 内部攻击

当系统的合法用户以非故意或非授权方式进行动作时便出现内部攻击。多数已知的计算机犯罪都和使系统安全遭受泄露的内部攻击有密切的关系。

能用来防止内部攻击的保护方法包括：

(1)对工作人员进行仔细审查。

(2)仔细检查硬件、软件、安全策略和系统配置，以便在一定程度上保证它们运行的正确性(称为可信功能度)。

(3)审计跟踪以提高检测出这种攻击的可能性。

三、威胁和攻击的来源

1. 内部操作不当

信息系统内部工作人员操作不当，特别是系统管理员和现代安全管理员出现管理配置的操作失误，可能造成重大安全事故。

2. 内部管理不严

信息系统内部缺乏健全管理制度或制度执行不力，给内部工作人员违规和犯罪留下缝隙。其中以系统管理员和现代安全管理

执行部门		责任人(签名)	

文 件 名	信息系统安全风险确认标准		
电子文件编码	AQGL-A01-003	序　码	5 - 5

员的恶意违规和犯罪造成的危害重大；内部人员私自安装拨号上网设备，则绕过了系统现代安全管理控制点；内部人员利用隧道技术与外部人员实施内外勾结的犯罪，也是防火墙和监控系统难以防范的。此外，内部工作人员的恶意违规(例如，采用禁止服务攻击形式)可以造成网络和站点拥塞、无序运行甚至网络瘫痪。

3.黑客进攻

黑客译自英文hacker，取其谐音而得名。术语hacker原本是计算机 入侵者 ’用来称呼他们自己的；而hacking则被美国的法律机构用于描述那些专业的计算机欺骗和滥用行为，同时美国警方将其用于描述几乎任何涉及到 利用 ’、‘ 借助 ’、‘ 通过 ’计算机的犯罪或 阻挠 ’计算机的行为。英文hacker的行为就是hacking，由此推理，黑客的行为就是涉及阻绕计算机系统正常运行或者利用、借助和通过计算机系统进行犯罪的行为。

黑客正是通过信息系统各组件(硬件、操作系统、通信协议和应用程序等)所存在的缺陷和漏洞，才能潜(进)入他人的信息系统中。黑客对信息系统的最大威胁不只在于直接的攻击或成功的攻击，更重要的则在于通过攻击，获得信息系统的技术经验和技术方法，特别是绕过或逃脱信息系统管理的网上跟踪和反跟踪的方式和方法。

执行部门		责任人(签名)	

文 件 名	信息系统安全防护措施制定标准		
电子文件编码	AQGL-A01-004	序　码	5 - 1

一、信息系统安全的防御策略

1. 设置阻塞点

阻塞点是在网络系统对外连接通道上，可以被系统管理人员进行监控的连接控制点。

在网络信息安全系统上，位于站点与因特网之间的防火墙就是一个阻塞点的典型例子。任何一个从公共网络侵袭站点的操作都必须通过这个对侵袭起防御作用的阻塞点。系统管理人员应当在网络运行中，监视这些侵袭并在发现他们时进行基于策略的处理，同时不得将企业内部住处系统连接外界。

2. 监测和消除薄弱环节

系统安全链的强度取决于系统链接最薄弱的环节(脆弱性)，墙的坚固程度取决于它的最(脆)弱点。精明的侵袭者总要找出那个最弱点并集中力量对其进行攻击。系统管理人员应意识到网络系统防御中的弱点，以便采取措施进行加固或消除它们的存在，同时也要监测那些无法消除的缺陷的安全态势。

3. 加强多层次垂直防御

安全体系不要只依靠单一安全机制和多种安全服务的堆砌，而是要建立具有协议层次和(信息流方向)纵向结构层次的完备体系。通过多层机制互相提供必要的冗余和备份；提供网络安全、主机安全和人员安全(用户培训、精细的系统管理等)。所有的机制都必须有效，但不要对他们中的任何一个给予绝对的信任。

在建立网络信息系统中，有使用多层次防火墙的必要和可

执行部门		责任人(签名)	

文 件 名	信息系统安全防护措施制定标准		
电子文件编码	AQGL-A01-004	序　码	5 - 2

能，可以用于网络内部与外部以及内部的子网之间的隔离，并满足不同程度需求的访问控制。

4. 鼓励员工普遍参与

为了使安全机制更为有效，绝大部分安全系统要求员工普遍参与，以便集思广益来规划设计网络的安全策略和规则，发现问题，使网络系统的安全设计更加完善。

5. 失效保护

安全保护的另一个基本原则就是失效保护。一旦系统运行错误，当其发生故障时必须拒绝侵袭者的访问，更不允许侵袭者跨入内部网络。当然也存在一旦出现故障，可能导致合法用户无法使用网络资源的情况，但这也是确保系统安全必须付出的代价。

二、信息系统安全策略评价标准

信息系统在安全设计、实施和运行过程中，安全策略应兼顾兼容信息系统安全的系统性、动态性及相关性原则。

1. 系统性规划

信息系统安全需要从技术和管理的结合上，针对信息系统的脆弱性分布和强度关系，将信息现代安全技术(密码技术、访问控制技术和鉴别技术等)机制支撑的安全服务(机密性、完整性、可用性、可审计性和抗抵赖性等)功能，分别作用于TCP／ IP的各个协议层上，最终达到使风险值稳定、收敛且实现安全与风险的适度平衡。

执行部门		责任人(签名)	

文 件 名	信息系统安全防护措施制定标准		
电子文件编码	AQGL-A01-004	序　码	5 - 3

只有经过对信息系统进行安全规划，对信息进行优先级保护分类，对信息系统安全脆弱性(包括漏洞)的分布和强度关系进行分析，对来自内部和外部的威胁手段和技术进行排列，以此评估安全的风险，建立起包括 风险分析、安全需求分析、安全策略制定和评估及其实施、风险监测以及实时响应 '的可适应安全模型，才是符合自身信息系统实际的合理、科学的信息安全体系。

2. 动态性

安全策略必须能根据风险变化进行及时调整。一成不变的静态策略，在信息系统的脆弱性以及威胁技术发生变化时，会降低安全作用或变得毫无安全作用，因此安全策略以及实现安全策略的现代安全技术和安全服务，应具有 风险检测——实时响应——策略调整——风险降低 '的自适能力，这就是信息安全的动态性问题。

3. 相关性和相对性

信息系统涉及安全的各组件之间的关系变化，可能引起安全风险强度及分布的变化，要求安全策略要适应这一变化。忽视或忽略信息系统涉及安全的组件在运行、应用或变更中对信息安全的相互影响，由此制定的安全策略无法获得对信息系统及其应用发生变化所出现的新的安全脆弱性和威胁的认识和理解，这样的安全策略是不完整的，只有充分考虑并认识到信息系统各组件在运行、应用和变更中对安全风险可能产生的相互影响，由此制定的安全策略才是完整的，这就是信息安全的相关性问题。

执行部门		责任人(签名)	

文 件 名	信息系统安全防护措施制定标准		
电子文件编码	AQGL-A01-004	序　码	5 - 4

三、调协各级系统安全管理者

信息系统的运行是依靠系统的管理者来具体实施的，他们既是信息系统安全的主体，也是系统现代安全管理的对象。管理者有系统安全员、系统管理员、信息现代安全管理员、网络管理员、存储介质保管员、操作人员、软硬件维修人员等。

1. 系统安全员

系统安全员负责与计算机、操作系统、数据库和应用软件相关的安全问题，负责安全建设和运营方案的决策，负责安全事故的处理，其余管理者都服从其领导。

2. 系统管理员

系统管理员是指对信息系统实施系统管理的人员或系统管理工程师，负责整个系统的运营管理，参与现代安全管理。

3. 信息现代安全管理员

信息现代安全管理员是负责与通信、计算机网络相关的安全问题的人员，负责安全策略的制定和对安全事件的处理。

4. 网络管理员

网络管理员是指对通信网络和计算机网络实施管理的人员或网络管理工程师。

5. 存储介质保管员

存储介质保管人员是负责保管存储介质，包括磁盘、光盘、纸介质等的人员。

6. 操作人员

执行部门		责任人（签名）	

文 件 名	信息系统安全防护措施制定标准		
电子文件编码	AQGL-A01-004	序　码	5 - 5

操作人员主要执行系统和网络在管理和安全方面的操作工作，也包括办公自动化处理人员。

7. 软硬件维修人员

软硬件维修人员是负责硬件维修和软件维护的人员。

执行部门		责任人（ 签名）	

文 件 名	信息设备安全管理执行标准		
电子文件编码	AQGL-A01-005	序　码	3 - 1

对设备的全方位管理是保证工厂信息系统建设的重要条件。设备管理包括设备的购置、使用、维修管理等几个方面。

一、设备购置

1.设备选型

信息系统采取有关信息现代安全技术措施和采购装备相应的安全设备时，应遵循下列原则：

(1)严禁采购和使用未经国家信息安全测评机构认可的其他信息安全产品，尽量采用我国自主开发研制的信息现代安全技术和设备。

(2)严禁直接采用境外密码设备，如必须采用境外信息安全产品时，该产品必须通过国家信息安全测评机构的认可。

2.设备检测安装

信息系统中的所有设备必须是经过测评认证的合格产品，新选的设备应该符合中华人民共和国国家标准 数据处理设备的安全》,《 电动办公机器的安全》中规定的要求，其电磁辐射强度、可靠性及兼容性也应符合现代安全管理等级要求。

3.设备测试运行

凡购回的设备均应在测试环境下经过连续72小时以上的单机运行测试和联机48小时的应用系统兼容性运行测试。通过上述几项测试后，设备才能进入试运行阶段。试运行时间的长短可根据需要自行确定。通过试运行的设备，才能投入生产系统，正式运行。

执行部门		责任人（ 签名）	