第一章 总则

第一条 目的。为加强\*\*\*\*\*\*\*有限公司安全管理机构管理，规范人员岗位职责，依据《\*\*\*\*\*\*\*有限公司信息安全管理办法》制定本管理制度。

第二条 对象。本制度的对象主要是指\*\*\*\*\*\*\*有限公司信息系统各个方面管理员。

第三条 范围。本制度适用于\*\*\*\*\*\*\*有限公司信息系统相关工作人员。

第四条 要求。\*\*\*\*\*\*\*有限公司信息系统岗位建设安全管理要求统一遵循《GB/T 22239-2008信息安全技术 信息系统安全等级保护基本要求》。

第二章 安全岗位设置

第五条 安全管理员岗位

安全管理员岗位可以是安全管理员角色和安全审计员角色的组合，同时，根据具体需要，可以兼任病毒管理员和密钥管理员的角色。也可以根据具体情况，设置多个安全管理员岗位。

第六条 网络系统管理员岗位

网络系统管理员岗位可以是主机系统管理员角色和网络管理员角色的组合，同时，根据具体需要，可以兼任资产管理员的角色。也可以根据具体情况，设置多个网络系统管理员岗位。

第七条 应用管理员岗位

应用管理员岗位可以是数据库管理员角色和应用管理员角色的组合。也可以根据具体情况，设置多个应用管理员岗位。

对于其他的安全角色需要设置的岗位，可以由相关安全职能部门的人员兼任，也可以单独设置岗位。

第三章 安全岗位设置原则

第八条 为确保单位信息系统的安全，必须加强人事安全管理，提高安全管理人员的技术水平和安全意识，同时在人员岗位的设置方面要遵循以下原则。

(一) 多人负责原则

对一些有较高密级的与安全有关的活动，都必须有两人或多人在场。工作人员必须由系统主管领导指派，且忠诚可靠，能胜任工作；工作人员应该认真记录签署工作情况，以证明安全工作已得到保障。

上述所指与安全有关的活动包括：硬件和软件的维护；系统软件的设计、实现和维护；处理保密信息；系统用媒介的发放与回收；访问控制用证件的发放与回收；重要程序和数据的删除和销毁等。

(二) 任期有限原则

决不能由一人长期担任安全管理职务。对一些重要安全岗位的工作人员应该不定期循环任职，强制实行轮换、休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

(三) 职责分离原则

非经系统主管领导批准，任何信息系统的工作人员都不得打听、了解或参与其职责以外的任何与系统安全有关的事情。安全工作人员活动所涉及的范围应是受到限制的，不能越权限访问。

(四) 工作分开原则

权力不能过于集中在某个人或某些人手里，在信息安全工作中，有的工作不能由一个人担任，工作分开便于相互制约。出于对安全的考虑，下面每组内的两项信息处理工作应该由不同的人员来负责：对计算机操作与计算机编程；机密资料的接收和传送；安全管理和系统管理；应用程序和系统程序的编制；访问证件的管理与其它工作；计算机操作与信息系统使用媒介的保管等。

(五) 权限随岗原则

权限随岗原则。根据岗位变动情况及时调整相应的授权，做到：在岗有权、离岗失权。

第四章 信息安全工作人员的管理要求

第九条 信息安全工作人员应具备的条件：

 政治上可靠，对单位忠诚；

 工作认真负责，有敬业精神；

 处理问题公正严明，不拘私情；

 熟悉业务，具有一定的实践经验。

第十条 信息安全工作人员的管理原则：

 人员审查的原则。对担任信息安全的工作人员，在录用必须进行审查，录用的人员应政治素质高、思想上进、对工作敬业、做事认真负责、处理问题公正严明、业务技术合格。

 人员培训的原则。对从事信息安全的工作人员应进行上岗前的培训，掌握基本的技能；岗中定期培训，不断更新观念，掌握新技术。培训的内容包括法律法规、职业道德、技术、业务、各种操作规程、信息安全方面出现新问题的对策等。

 持证上岗的原则。信息安全管理是一项非常重要的工作，要求工作人员具有较高的政治素质和业务水平，因此各类安全工作人员必须经过认真的培训，严格的考试（考核），取得证书后，才能上岗。没有合格证书的人员不能从事信息安全工作。

 人员考核的原则。对从事信息安全工作的各类人员要从思想作风、工作态度、遵守规章制度、业务能力等方面定期进行考核。合格者表扬或奖励，不合格者，批评教育或调离岗位。

 签订保密协议的原则。信息安全工作涉及单位的秘密，信息安全工作人员必须签订保密协议，要求承担保密义务，对违反协议的要坚决处罚，甚至调离工作岗位。

 两个以上的原则。权利分散有利于抵御来自内部的威胁，在条件可能的情况下，领导者派两个或两个以上的人员共同进行有关信息安全方面的工作，工作之后共同签字。

 经常换岗的原则。任何人都不能在一个与信息安全有关的工作岗位上工作时间过长会产生工作“麻痹症”或被少数不忠诚者钻空子，对信息系统造成威胁，因此工作岗位应经常轮换。

 权力分散的原则。权力不能过于集中一个人或几个人手中，在信息安全工作中，有的工作不能由一个人担任，权力的分散便于相互制约。

 权力最小的原则。安全工作人员活动所涉及的范围应是收到限制的，而且应限制在最小的（权限）范围之内，不能越权限访问。

 人员离岗的原则。因工作需要或因不适合做信息安全管理工作而调离岗位，必须由领导找其谈话，要求履行保密协议，承诺保密事项，并交出有关的资料、证件。

第五章 信息安全工作人员的岗位职责

第十一条 安全管理员的职责

(一) 负责对安全产品购置提供建议，负责组织制定各种安全产品策略与配置规则，负责跟踪安全产品投产后的使用情况；

(二) 负责指导并监督系统管理员（包括主机系统管理员、网络管理员、数据库管理员和应用管理员等）及普通用户与安全相关的工作；

(三) 负责组织信息系统的安全风险评估工作，并定期进行系统漏洞扫描，形成安全评估报告；

(四) 根据单位的信息安全需求，定期提出信息安全改进意见，并上报信息安全管理部门主管；

(五) 定期查看信息安全站点的安全公告，跟踪和研究各种信息安全漏洞和攻击手段，在发现可能影响信息安全的安全漏洞和攻击手段时，及时做出相应的对策，通知并指导系统管理员进行安全防范；

(六) 负责组织审议各种安全方案、安全审计报告、应急计划以及整体安全管理制度；

(七) 负责参与安全事故调查。

第十二条 系统管理员的职责

(一) 负责主机操作系统的安全配置（包括及时修补系统漏洞）和日常审计，系统应用软件的安装，从系统层面实现对用户与资源的访问控制；

(二) 协助安全管理员制定主机操作系统的安全配置规则，并落实执行；

(三) 负责主机设备的日常管理与维护，保持系统处于良好的运行状态；

(四) 为安全审计员提供完整、准确的主机系统运行活动的日志记录；

(五) 在主机系统异常或故障发生时，详细记载发生异常时的现象、时间和处理方式，并及时上报；

(六) 编制主机设备的维修、报损、报废计划，报主管领导审核。

第十三条 网络管理员的职责

(一) 负责网络的部署以及网络产品、网络安全产品的配置、管理与监控，并对关键网络配置文件进行备份，及时修补网络设备的漏洞；

(二) 协助安全管理员制定网络设备安全配置规则，并落实执行；

(三) 为安全审计员提供完整、准确地记录重要网络设备和网站运行活动的运行日志；

(四) 在网络及设备异常或故障发生时，详细记载发生异常时的现象、时间和处理方式，并及时上报；

(五) 编制网络设备的维修、报损、报废等计划，报主管领导审核。

第十四条 数据库管理员的职责

(一) 对数据库系统进行安全配置，修补已发现的漏洞；

(二) 负责数据库系统的用户账号管理，对系统中所有的用户进行登记备案；对数据库系统的用户、口令的安全性进行管理；对数据库系统登录用户进行监测和分析；

(三) 负责业务数据及系统其它重要数据的备份与备份数据管理工作；

(四) 为安全审计员提供完整、准确的数据库系统运行活动的日志记录，详细记载发生异常时的现象、时间和处理方式，并及时上报；

(五) 在发生安全问题导致数据损坏或丢失时，进行数据的恢复；

(六) 根据业务发展的需求，提交数据存储介质购买或存储系统扩容计划。

第十五条 应用管理员的职责

(一) 对业务应用系统进行安全配置；督促软件开发商提供补丁来修补已发现的漏洞；

(二) 对业务应用系统的用户、口令的安全性进行管理；对业务应用系统的登录用户进行监测和分析；

(三) 负责提出数据的备份要求，制定数据备份策略，督促数据库管理员按照备份方案按时完成，并恢复所需数据；

(四) 实施系统软件版本管理，应用软件备份和恢复管理。

第十六条 安全审计员的职责

(一) 组织策划信息中心信息安全审计工作；

(二) 协调有关部门，以获得对信息安全审计工作的理解和支持；

(三) 确定信息安全审计工作的目的、范围和要求；

(四) 负责定期对主机系统、网络产品、应用系统的日志文件进行分析审计，发现问题及时上报；

(五) 负责对信息安全保障管理活动进行独立的监督，提供内部独立的审计和评估工作，并根据需要可以协同外部审计评估机构进行评估和认证，为决策领导提供信息系统和信息安全保障执行状况的客观评价；

(六) 制订信息安全审计工作具体实施计划和有关资源配置；

(七) 负责信息系统交易、传输、认证密钥的管理以及加密机的操作。

第六章 附则

第十七条 对违反本制度的人员，将按照单位有关规定进行处罚。

第十八条 本制度由项目管理办公室负责制定、解释和修改。

第十九条 本制度自发布之日起执行。