1.0目的

为了防止和遏制企业网络各类信息安全事件的发生，及时处理网络出现的各类信息安全事件，减轻和消除突发事件导致的经济损失和社会影响，保证移动通信网络畅通与信息安全，营造良好的网络竞争环境，有效进行企业内部网络信息技术安全整体控制，特制定本规范。

2.0　合用范围

本管理规范合用于四川移动所属系统及网络的信息安全管理及企业内部信息技术整体的控制。

3.0信息安全组织机构及职责：

根据集团企业有关信息安全组织的指导意见，为保证信息安全工作的有效组织与指挥，四川移动通信有限责任企业建立了网络与信息安全工作管理组，由企业分管网络的副总经理任组长，网络部分管信息安全副总经理任副组长，由省企业网络部归口进行管理，省企业网络部门设置信息安全管理专职人员，负责信息安全职能管理和安全技术管理，省监控中心设置安全监控人员，各市州分企业及生产中心设置专职或兼职信息安全管理员，负责全省各系统及网络的信息安全管理协调工作。

网络与信息安全工作管理组组长职责：

负责企业与有关领导之间的联络，跟踪重大网络信息安全事件的处理过程，并负责与政府有关应急部门联络，汇报状况。

网络与信息安全工作管理组副组长职责：

负责牵头制定网络信息安全有关管理规范，负责网络信息安全工作的安排与贯

彻，协调网络信息安全事件的处理。

信息安全职能管理职责：

负责组织贯彻和贯彻各项安全管理规定，制定安全工作计划；制定和审核网络与信息安全管理制度与有关工作流程；组织检查和考核网络及信息安全工作的实行状况；定期组织对安全管理工作进行审计和评估；组织制定安全应急预案和应急演习，针对重大安全事件，组织实行应急处理工作及后续的整改工作；汇总和分析安全事件状况和有关安全状况信息；组织安全教育和培训。

信息安全技术管理职责：

根据有限企业制定的技术规范和有关技术规定，对各类网络、业务系统和支撑系统提出对应安全技术规定，并审核技术方案；牵头对各类网络和系统实行安全技术评估和技术审计工作；公布安全漏洞和安全威胁预警信息，并细化制定对应的技术处理方案；协助制定网络与信息安全的应急预案，参与应急演习；针对重大安全事件，参与实行应急处理，并定期对各类安全事件进行技术分析。

安全监控人员职责：

对全网安全设备进行集中监控；处理平常的安全事件；协助网络安全处分析、处理复杂和重大安全事件。

安全管理员职责：

在省企业及分企业网络部领导下，负责各市州分企业及生产中心网络信息安全的技术工作及有关协调工作，贯彻执行集团企业和省省/市企业网络部下发的有关信息安全技术规范及文献，根据有关安全技术规范和技术规定，对各类网络、业务系统和支撑系统进行包括安全在内的平常维护。协调各有关部门进行详细实行，对各市州分企业及生产中心业务系统、支撑系统网络安全进行分析、审计，减少各市州分企业及

生产中心各业务系统、支撑系统安全隐患，减少信息安全事件的发生，保障其安全运行。

4.0 管理规范

4.1 管理系统

本管理规范合用于四川移动各生产、支撑系统，包括 OA 系统、MIS 系统、BOSS 系统及其子系统、经营分析系统、客户服务系统、MISC系统、互换机系统、智能网系统、彩铃平台等。

4.2网络与信息安全基本规定：

网络与信息的安全工作实行谁主管、谁负责、防止为主、综合诊治、人员防备与技术防备相结合的原则，逐层建立安全保护责任制。

各级网络维护部门应加强对系统管理人员安全意识的培养，建立完善的定期定人负责制，有效明确责任，提高维护管理效率。

4.3 顾客帐号/权限管理流程

顾客帐号/权限管理合用于四川省移动通信有限责任企业及下属各分企业，重要为了规范四川移动各业务系统波及系统级(含数据库级)、应用级层面的的帐号、权限及密码的管理。

系统管理人员逻辑分类

四川省移动通信有限责任企业所属系统及网络(包括 OA 系统、MIS 系统、BOSS 系统及其子系统、经营分析系统、客户服务系统、MISC系统、互换机系统、智能网系统、彩铃平台等)的信息安全管理及企业内部信息技术整体的控制，各系统分别具有

不一样层面管理员及顾客：

岗位	职责	波及有关记录
部门负责人 如各生产中心分管领导	1、需对有关授权表进行审批授权签字，每季度需复核审批 ； 2、需对员工变动状况进行审批 ； 3、需对远程维护接入申请进行审批	《远程维护接入申请和状况登记表》 《员工变动登陆企业网络系统申请表》 《网络/系统层/应用层超级管理员授权表》 《安全管理员授权表》 《顾客帐号审阅表》 《系统预设顾客帐号审阅表》 《超级管理员帐号移交单》
系统层/应用层/网络超级管理员： 1、系统层超级管理员：按各系统进行设置，如智能网、彩铃、BOSS、互换机操作系统及数据库维护管理人员。 2、 应用层超级管理员：按业务应用管理进行设置，如彩铃应用层超级管理员由数据部彩铃管理员负责。 3、 网络超级管理员：按企业网络划分进行设置，省企业及地市各生产中心分别设置网络超级管理员。	系统/应用程序/网络最高权限管理员，负责管理所辖系统的帐号分派和管理，需要部门负责人对其进行授权。 网络超级管理员、系统层超级管理员、应用层超级管理员需由部门领导分别进行授权，可以兼任。	《终端接入企业局域网申请表》 《远程维护接入申请和状况登记表》 《员工变动登陆企业网络系统申请表》 《网络/系统层/应用层超级管理员授权表》 《帐号创立、变更申请表》 《顾客帐号审阅表》 《系统预设顾客帐号审阅表》 《帐号密码更改记录》 《超级管理员帐号移交单》 《账号临时使用申请表》
系统层/应用层一般顾客： 系统层一般顾客：如互换机、智能网、短信等监控、 一般系统维护人员 应用层一般顾客：智能网地市操作人员，彩铃业务操作人员。	系统维护、应用操作执行人员，为一般维护人员及第三方人员，只能申请自身帐号进行操作，不能进行帐号分派管理。	《终端接入企业局域网申请表》 《系统备份记录》 《帐号创立、变更申请表》 《帐号密码更改记录》 《账号临时使用申请表》

安全管理员：各生产中心及地市分企业分别进行设置。	负责所辖各系统及设备的信息安全管理工作。每月检查所辖中心信息安全管理的执行状况，汇总安全分析汇报；负责所辖中心机房管理审查。与网络超级管理员、系统层超级管理员、应用层管理员需职责分离。	《安全分析记录汇报》 《远程维护接入申请和状况登记表》 《员工变动登陆企业网络系统申请表》 《帐号创立、变更申请表》 《安全管理员授权表》 《顾客帐号审阅表》 《系统预设顾客帐号审阅表》 《帐号密码更改记录》

顾客授权管理流程

管理流程	管理规定
开　始 由使用部门(厂商)人员填写变更/申请表 由业务部门主管审批，并考虑不相容职责 Y　　N 报省企业安保部审批 超级管理员按申请进行创立/修改	在发生变动状况时，由使用部门/第三方人员填写《帐号创立/变更申请表》。 各市州分企业、信息技术中心(网管、数据、计费、信息中心)网络超级管理员、系统层超级管理员、应用层超级管理员、安全管理员分别填写《网络超级管理员授权表》、《系统层超级管理员授权表》、《安全管理员授权表》、《应用层超级管理员授权表》,由有关信息系统部门负责人审批并进行授权，并对各清单每季度进行复核并签字确认，对多出或不恰当的账号进行调整。 由应用层超级管理员提交业务部门主管进行书面审批后 创立新顾客角色或对顾客组或顾客角色定义进行修改时，应考虑不相容职责分工原则，由业务部门主管(或授权人员)对顾客角色的权限设定进行审阅并签字确认，以合理保证顾客在系统中的权限与其职责相符。超级管理员根据经审批的顾客角色权限，在系统中设置顾客角色权限。

<table>
<tr><th colspan="4">管理流程</th><th>管理规定</th></tr>
<tr><td colspan="4"></td><td>各部门在发生人员新增、调动及离职状况经部门领导审核盖章后提交省企业安保部审批通过，《员工变动登陆企业网络系统申请表》。</td></tr>
<tr><td colspan="4"></td><td>由超级管理员在系统中创立顾客账号，防止未经授权的账号及权限创立/修改
对系统、数据库、应用层，除查询顾客外应按个人创立单独的顾客账号，并赋予对应的权限，以防止共享账号的产生。</td></tr>
<tr><td colspan="4" rowspan="2"></td><td>各超级管理员每季度形成顾客帐号清单。</td></tr>
<tr><td>业务部门主管对网络、系统顾客的清单每季度进行复核签字确认，对第三方顾客的清单每季度进行复核签字确认。形成《顾客帐号审阅表》、《四川移动通信有限责任企业员工(合作单位员工)登陆企业网络系统审批表》</td></tr>
<tr><td rowspan="3">如发
不恰</td><td colspan="2">现多出或
当的账号</td><td></td><td>《四川移动通信有限责任企业员工(合作单位员工)登陆企业网络系统审批表》由部门领导复核盖章后，提交省企业安保部审批
各部门网络超级管理员每季度准备本部门登陆企业网络系统顾客清单，由部门领导复核盖章后，提交省企业网络部及安保部进行审查。如发现多出或不恰当的账号应进行及时根据规定进行调整并反馈安保部。
各市、州移动分企业登陆省企业网络系统的企业员工和合作单位人员，由安保部门每季度汇总报省企业安保部审核，有关业务部门根据省企业安保部告知予以授权。</td></tr>
<tr><td colspan="2">系统超级管理员进行调整</td><td></td><td></td></tr>
<tr><td colspan="3"></td><td></td></tr>
</table>

管理流程	管理规定
	如发现多出或不恰当的账号系统管理员需进行及时调整，并反馈调整成果。 **超级管理员变更时，应填写《超级管理员帐号移交单》,由对应部门主管进行审批签字，移交双方签字确认。** **—企业业务流程发生重大变更时，由各超级管理员打印系统顾客的访问权限清单，并交由有关业务部门主管，对顾客的权限进行审阅签字，以防止在顾客的权限中有不兼容职责的存在。** **如发现不相容职责，应及时告知超级管理员，对顾客的权限进行调整。**

4.3.4假如存在第三方厂商人员使用超级管理员帐号的状况，应和第三方厂商签订有关的安全保密协议，以合理保证第三方厂商可以执行中国移动的安全管理规定和职责不相容规定。厂商要保留帐号创立，帐号变更，帐号删除和密码变更的记录，供我方人员进行定期的检查。

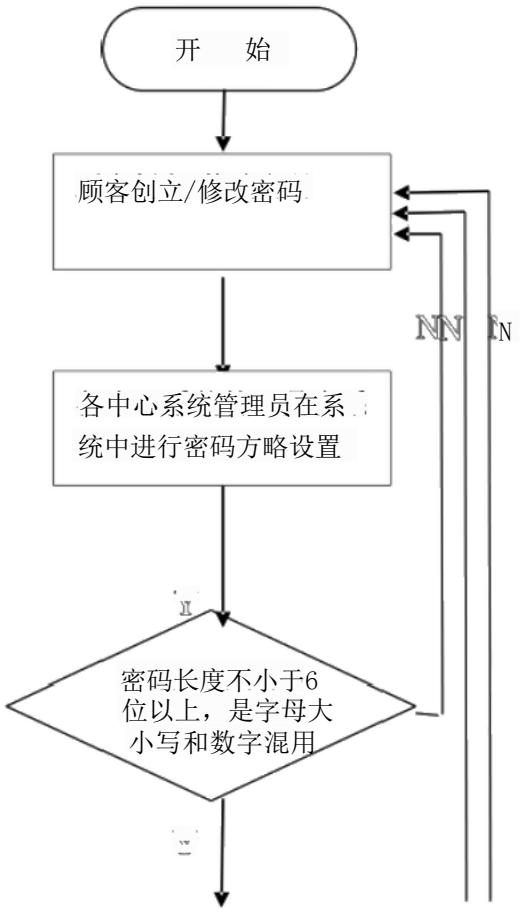
4.3.6各生产、支撑网络系统如因维护规定有第三方远程登陆接入需求，应填写《远程维护接入申请和状况登记表》,经本维护单位安全管理员和部门分管负责人签字后，临时开通远程登录功能，方可接入。操作完毕后，应及时关闭远程维护接入点，并填写《远程维护接入申请和状况登记表》。本维护单位安全管理员及时审阅对应的操作日志记录并签字确认。

4.3.7 各业务及支撑系统的厂商开发人员由于需要进行系统故障处理、检查等原因拥有生产系统的顾客名及口令。企业进行对开发人员(包括外包厂商)对生产系统进行程序更新的控制，只有在有必要时才临时由信息技术部门主管授权开发人员访问并更新生产系统，开发人员访问生产系统时由信息技术部门系统维护人员对其访问进行监督，并在访问结束后及时删除或严禁开发人员在生产系统中的账号。

4.3.8 因系统原因不能按个人创立独立的顾客账号的，由超级管理员按使用权限制定对应账号，授权到到使用部门指定人员。其他维护人员工作若需要使用该账号，每次需要填写《账号临时使用申请表》,由超级管理员审批后，在超级管理员的协助下进入系统进行维护，工作完毕后立即退出系统，保证系统安全。

4.3.9 质量管理和考核措施见6.0

4.4 密码口令管理规定

管理流程	管理规定
	不得使用近来5次以内反复的密码 密码反复尝试5次后来应暂停该帐号登录 密码长度为6位以上，必须是字母大小写和数字混用

管理流程		管理规定
密码生存时间 不不小于90天		密码应至少每90天进行更新 对于设置了有效期的口令，如HLR系统顾客，系统管理员应在口令过期前完毕口令的重新设置工作。
密码更改检查记录		对于因系统限制临时无法在系统中建立密码方略的，各部门安全管理员每季度对本部门各系统密码进行检查，以保证密码政策的有效执行。
密码应以某种介质形式 密封保留至安全可靠处		各市州分企业、信息技术中心系统维护及使用人员根据密码方略定期进行密码修改，更改后密码应以某种介质形式密封保留至安全可靠处。 维护维护终端应设置开机口令、屏幕保护口令。在有人值守机房内，维护终端屏幕保护的时间不能多于15分钟；对于无人值守机房，终端屏保时间不能多于3分钟。六个月至少修改一次开机口令、屏幕保护口令。

4.5 信息安全监控

亲密关注顾客投诉状况，并通过短信监控过滤系统7*24 小时对短信中心中所有短信息进行监控。对更新的关键词在2小时内录入关键词库，对短信进行内容监控。对短信发送的流量进行控制，对个人每小时发送500条或企业每小时发送10000条的要过滤出来，审核内容，如内容合法，可继续发送，否则将主被叫号码、发送时间、信息内容等有关信息进行保留，并上报上级主管单位。对于大量发送有害信息(法轮功：10条和10条以上，其他政治类30条和30条以上)的顾客，应在发现后15分钟内关闭该顾客的短信息业务功能。

移动信使、短信网关、企业网站及WAP二级站点， EMIS系统公告板(包括分企业)、

电子论坛、邮件网关服务器应建立信息监控过滤机制，7*24小时监控，对公布内容先审后发并进行信息巡查，杜绝反动、色情等有害信息出目前网站上。 一旦发现 SP 业务出现非法信息传播，将立即断掉梦网与该SP的连接端口，并立即上报主管部门。企业网站及WAP 二级站点应7*24小时对访问状况进行监控，发现黑客袭击，立即封掉黑客的 IP 地址，同步上报上级主管部门。

4.6 系统信息安全方略

系统信息安全方略表：

安全方略	管理规定	执行周期	检查周期	有关记录
企业内部网络系统与外部网互联方略	应保证采用必要的措施(如防火墙、限制网段和端口、数据加密、虚拟专网或身份认证等技术)限制网外或非法顾客进行穿透访问。	网络割接、系统上线	年	系统设置
设备专机专用方略	不得装入与工作无关的软件。严禁启动RLOGIN服务。严禁ROOT顾客从其他主机登陆。严禁将网管设备挪作他用或私自更改配置。	网络割接、系统上线	年	系统设置
主机防病毒防火墙软件或硬件方略	严禁生产系统与互联网相接，严禁使用来历不明的软件。定期对磁盘、内存进行扫描，及时杀死已驻留的病毒，以免病毒在网上传播导致严重后果。每周使用正版杀毒软件检查在用WINDOWS系统和维护终端软件。每周对杀毒软件进行升级。	周	月	安全维护作业计划
邮件服务安全	数据中心邮件系统维护需负责各系统电子邮件服务器应启动邮件安全应用程序，	网络割接、系统上线	季度	系统设置
SP专线接入方略	各移动梦网SP、专线顾客在连入我企业网络前，应保证业务内容合法，并与我企业签定信息安全协议。各移动梦网SP不得开展与我企业所签协议之外的业务。各SP需安排7*24小时值班人员和值班 ，保证出现信	业务接入	季度	《梦网SP网络运行管理措施》