

中华人民共和国通信行业标准

YD/T 2670-2013

基础电信运营企业移动网络 客户信息安全管理框架

Customer information security management
framework of telecom operators

2013-10-17 发布

2014-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 缩略语	1
4 客户信息的分类及分布客户信息的内容	1
4.1 客户信息的分类	1
4.2 客户信息的分布	2
5 客户信息安全防护管理	3
5.1 账号口令管理	3
5.2 客户信息操作的管理	4
6 客户信息安全审核	5
6.1 客户信息安全审核的内容	5
6.2 操作日志审核	5
6.3 合规性审核	7
6.4 日常例行安全审核与风险评估	8
7 客户信息系统的技术管控	8
7.1 概述	8
7.2 系统安全防护	8
7.3 统一安全管控系统	9
7.4 远程接入管控系统	9
7.5 客户信息泄密防护系统	9
7.6 系统间接口管理系统	10
8 数据存储与备份管理	10

前 言

本标准按照 GB/T1.1-2009 给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国移动通信集团公司、中国移动通信集团设计院有限公司。

本标准主要起草人：张 滨、赵 刚、袁 捷、冯运波、乔 喆、刘 佳、杜雪涛、冀 文、张 晨、吴兴耀。

基础电信运营企业移动网络客户信息安全管理框架

1 范围

本标准规定基础电信运营企业内部移动网络及业务中涉及客户信息操作的各个环节的信息安全保护，内容包括客户信息的分级及分布、客户信息安全防护管理、客户信息安全审核、客户信息系统的技术管控、数据存储与备份管理等内容。

本标准适用于基础电信运营企业移动网络的客户信息安全管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO/IEC 27001:2005 信息安全管理实施指南

ISO/IEC 27002:2005 信息安全管理实施细则

3 缩略语

ADC	Application Data Center	应用数据中心
CRM	Customer Relationship Management	客户关系管理
DCS	Data Center for Short Message Service	短信增值业务平台
DSMP	Data Service Management Platform	数据业务管理平台
MISC	Mobile Information Service Center	数据业务管理系统

4 客户信息的分类及分布客户信息的内容

4.1 客户信息的分类

客户信息包括客户基本资料、客户身份鉴权信息、客户通信信息、客户通信内容信息等四大类。此四大类客户信息按照具体内容又可划分为若干子类，具体划分如下。

客户基本资料包括但不限于：集团客户资料、个人客户资料、各类特殊名单；

客户身份鉴权信息包括但不限于：用户登录各种业务系统的密码；

客户通信信息包括但不限于：详单、原始话单、账单、客户位置信息、客户消费信息、基本业务订购关系、增值业务（含数据业务）订购关系、增值业务信息、客户通讯录等；

客户通信内容信息包括但不限于：客户通信内容记录、移动上网内容及记录、行业应用平台上交互的信息内容。

客户信息的详细内容见表1。

表1 客户信息涵盖的范围

客户信息分类	子 类	内 容
客户基本资料	集团客户资料	集团客户负责人信息、联系人信息、单位成员个人基本信息、业务合同、银行扣费帐户、集团客户编号、集团客户名称、所在省市、所在行业、集团签约时间、集团协议到期时间

表1 (续)

客户信息分类	子 类	内 容
客户基本资料	个人客户资料	客户姓名、证件类型、证件号码、证件影印件、客户手机终端信息、客户职业、工作单位、居住地址、联系地址、联系电话、银行扣费帐户、客户编号、年龄、性别、归属市县营业厅、兴趣爱好、邮寄信息、大客户标识
	各类特殊名单	黑名单、白名单、红名单
客户身份鉴权信息	用户密码	用户服务密码、移动邮箱密码、移动 wlan 密码等
客户通信信息	详单	包括语音、短信、彩信等，内含主叫号码、主叫位置、被叫号码、开始通信时间、时长、流量、金额等信息
	原始话单	客户语音通信的原始话单
	账单	每月出账的固定费用、通信费用、数据费用、代收费用
	客户位置信息	精确位置信息（如小区代码、基站号、基站经纬度坐标等）；大致位置信息（如地区代码等）
	客户消费信息	停开机、入网时间、在网时间、积分、预存款、信用等级、信用额度、缴费情况、付费方式
	基本业务订购关系	品牌、套餐情况定制情况
	增值业务（含数据业务）订购关系	移动邮箱、号簿管家、来电显示、彩铃、手机钱包等增值业务的注册、修改、注销
	增值业务信息	移动邮箱地址、飞信号、手机钱包余额、交易历史记录
	客户通讯录	客户通讯录中存储的信息
	其他	来显号码
客户通信内容信息	客户通信内容记录	短信、彩信、移动即时通信软件、邮件、号簿管家内容
	移动上网内容及记录	移动上网访问内容、上传下载、客户端软件通信记录
	行业应用平台上交互的信息内容	订购关系、用户状态、用户品牌、客户消费记录

4.2 客户信息的分布

存储和处理客户信息的系统包括支撑系统、业务平台、通信系统等3大类。每个系统中都含有客户信息，具体涵盖内容见表2。

表2 系统分类及各系统涉及客户信息内容

大类	原有信息分类	包含的客户信息
支撑系统	业务运营支撑系统	存储的信息： 集团客户资料、个人客户资料、各类特殊名单、用户密码、详单、账单、客户消费信息、基本业务订购关系、增值业务（含数据业务）订购关系、增值业务信息
	经营分析系统	存储的信息： 集团客户资料、个人客户资料、各类特殊名单、用户密码、详单、账单、客户消费信息、基本业务订购关系、增值业务（含数据业务）订购关系、增值业务信息
	客户服务支撑系统	详单、集团客户资料、个人客户资料
	网管系统	客户位置信息
	客户关系管理系统（CRM）	集团客户资料、个人客户资料、业务订购关系信息
	数据业务监测系统	移动上网内容及记录、客户通信内容记录（短彩信发送记录）等

表2 (续)

大类	原有信息分类	包含的客户信息
通信系统	移动业务交换中心 (MSC)	客户位置信息、原始话单
	归属位置寄存器 (HLR)	客户位置信息、用户状态
	WAP 网关	移动上网内容及记录、客户通信内容记录 (彩信记录)
	彩信互通网关	客户通信内容记录 (彩信记录)
	端局	原始话单、客户位置信息
	关口局	原始话单
业务平台	短信中心	客户通信内容记录 (短信记录, 短信内容)
	彩信中心 (MMSC)	客户通信内容记录 (彩信记录, 彩信内容)
	信令监测系统	客户位置信息、客户通信内容记录 (通话记录、短信记录、短信内容)
	垃圾短信监控平台	客户通信内容记录 (短信记录、短信内容)、黑白名单
	行业网关	客户通信内容记录 (短信内容、短信记录)
	短信互通网关	客户通信内容记录 (短信记录)
	梦网短信网关	客户通信内容记录 (梦网业务话单信息)
	企信通	客户通信内容记录 (短、彩信内容)
	位置业务 (LBS)	客户位置信息 (客户当前位置信息)
	彩铃平台	行业应用平台上交互的信息内容 (订购关系)
	手机钱包	行业应用平台上交互的信息内容 (客户消费记录)
	MISC/DSMP	行业应用平台上交互的信息内容 (订购关系、用户状态、用户品牌)
	ADC 位置类系统	客户位置信息 (从 LBS 上获取定位信息)
	ADC 业务平台	行业应用平台上交互的信息内容 (订购关系、消费记录)、集团客户资料
	DCS	客户通信内容记录 (短信内容)
	小区短信	客户位置信息 (CELL ID 类位置信息)
	移动即时软件	客户通讯录 (用户好友列表)
	移动桌面助理	客户通信内容记录 (短信记录、彩信记录)、客户通讯录
	个人信息管理 (PIM) 号簿管家	客户通讯录

5 客户信息安全防护管理

5.1 账号口令管理

5.1.1 账号管理遵循的原则

账号管理贯穿账号创建、授权、权限变更及账号撤销或者账号冻结的全过程。账号的创建、变更、删除应具有严格的审批流程, 需遵循的原则包括:

- 1) 账号设置应与岗位职责相匹配, 并坚持最小授权原则;
- 2) 创建岗位角色与权限对应的矩阵列表, 确保对应准确, 避免超出工作职责的过度授权;
- 3) 账号的申请、修改、删除等应制定严格的审批和授权流程, 授权审批记录应编号、留档;
- 4) 账号的创建、调整和删除申请在审批通过后, 应及时更新系统中的账号状态, 确保与审批结论保持一致;
- 5) 除低权限的查询账号外, 各系统不允许存在其他共享账号, 必须明确每个账号责任人;
- 6) 对于临时账号, 在完成特定任务后, 系统管理员应立即收回临时账号。

5.1.2 口令设置要求

口令设置的合理，能够大大降低客户信息泄露的风险。口令的设置需要遵循以下要求：

- 1) 口令至少由8位及以上大小写字母、数字及特殊符号等混合、随机组成；
- 2) 避免使用弱口令，包括姓名、电话号码以及出生日期等作为口令或者口令的组成部分；
- 3) 应以散列、加盐等加密技术保存口令，不得以明文方式保存或者传输；
- 4) 口令应具有一定的生命周期，每90天至少更换一次口令，5次以内不得设置相同的口令；
- 5) 修改口令时，须将口令修改记录保存在相关日志里，包含账号、修改时间、修改原因等，以备审核；
- 6) 由于员工离职等原因，原账号不能删除或者需要重新赋予另一个人时，应修改相应账号的口令。

5.1.3 系统支持能力

为了降低客户信息泄露的风险，涉及客户信息的系统应具备以下账号口令管理功能：

- 1) 系统账号口令输入尝试次数要做限制，防止口令的暴力破解；
- 2) 对于无法进行定期修改口令的账号，如内置账号、程序账号等，应在系统升级或重启时落实口令修改工作；
- 3) 如发生口令遗忘的情况，账号使用人应提出口令重置申请，由系统管理员进行密码重置，重置完毕后，使用者应马上更改重置后的密码；
- 4) 当程序内的账号密码需要保存在配置文件里时，应只使用适当权限的账号，采用经过验证的算法对账号口令进行加密，并做好账号口令和加密密钥的保护工作。

5.2 客户信息操作的管理

5.2.1 客户信息操作原则

对客户信息操作的人员包括业务人员、运维支撑人员、开发人员等。客户信息操作的总体原则是一切获取客户信息的操作必须经过一定的授权后方可进行。

5.2.2 业务人员对客户信息的操作

业务人员因业务受理、投诉处理等情况需要查询、获取客户信息或对客户信息进行批量操作（包括批量查询、批量导入、批量导出、批量为客户开通、取消或变更业务等），这些操作存在客户信息泄露的风险。因此业务人员对客户信息的操作必须遵循相应的审批流程：

- 1) 涉及客户普通资料的查询，服务营销人员要获得客户的同意，并且按照正常的鉴权流程通过身份认证，鉴权一般采取有效证件或服务密码验证，并保留业务受理单据；
- 2) 涉及客户通话详单、集团客户详细资料等客户信息的查询，服务营销人员只能在响应客户请求时，并且客户自身按照正常流程通过身份鉴权的情况下，协助客户查询，禁止服务营销人员擅自进行查询，查询需保留业务受理单据；
- 3) 除服务营销外的业务人员，因投诉处理、营销策划、经营分析等工作需要查询和提取客户信息的，业务管理部门应建立明确的操作审批流程，定期进行严密的事后审核。

5.2.3 运维支撑人员对客户信息的操作

运维支撑部门一般（包含 / 设置）生产运营、运行维护等岗位，各岗位对客户信息的操作权限应有所区分。因此需制定并维护业务系统的系统层角色权限矩阵，明确各岗位角色对客户信息的访问权限，

明确未经授权的运维支撑人员不允许有客户信息的访问权限。除此之外，运维支撑人员在操作时应遵循以下要求：

- 1) 运维支撑人员对业务系统的应用层的访问权限必须经过该系统的业务管理部门审批，对系统层访问权限必须经过运维支撑部门审批；
- 2) 运维支撑人员因统计取数、批量业务操作需求对客户信息进行查询、变更操作时必须有业务管理部门的相关公文或工单，并需要经过部门审批；
- 3) 运维支撑人员因业务投诉、统计取数、批量业务操作、批量数据修复等进行的客户信息查询、变更必须提交操作申请，按照要求进行操作，不得扩大操作范围，在工单中保留操作原因和来源的工单（公文）编号，并由专人负责审核；
- 4) 运维支撑人员因应用优化、业务验证测试需要查询、修改客户信息数据，只能利用测试号码进行各项测试，不得使用客户号码；
- 5) 运维支撑人员因系统维护进行客户信息的数据迁移（数据导入、导出、备份）必须填写操作申请，并经过部门主管审批；
- 6) 严禁运维支撑人员向开发测试环境导出客户信息，对需导出的信息必须经过申请审批，并进行模糊化处理。

5.2.4 开发人员对客户信息的操作

开发人员在系统开发、测试、上线等环节中，会接触到各类客户信息。因此，开发人员须签订信息安全承诺书，严禁利用系统漏洞、留存后门程序、留存无法删除的超级账户密码等方式窃取、泄露和滥用客户信息。除此之外，开发人员在操作时应遵循以下要求：

- 1) 开发人员的工作区域应与生产、内部办公、维护区域分离，并应采用严格的访问控制策略和管控手段；
- 2) 开发人员使用的测试数据不应当反映用户的真实信息，必须是经过模糊化处理的数据；
- 3) 开发人员进入可能接触到客户信息的生产或维护区域时，应当有相应的审批制度；
- 4) 开发区域的终端接入内部网络应有严格的接入认证，并严格限制U盘等外设拷贝，限制对无线局域网（WLAN）、3G等无线上网的使用，要求统一安装防病毒软件；
- 5) 应定期对现场测试的开发终端进行涉敏感信息审核；
- 6) 开发人员转岗或离岗前，需提交转岗或离岗申请书，由相关部门完成开发人员的账号回收、审核、网络调整等工作，并签署转岗或离岗审批意见。

6 客户信息安全审核

6.1 客户信息安全审核的内容

安全审核主要分为操作日志审核、合规性审核、日常例行安全审核与风险评估。

6.2 操作日志审核

日志审核是对操作日志与工单等原始凭证进行比对，分析查找违规行为。日志审核是发现客户信息泄露的主要途径之一。

6.2.1 日志审核的基本要求

安全员的设置要遵循“职责不相容”原则，即安全员应与系统管理员、业务操作人员分开，由专人担任，安全员应定期开展安全审核。日志要全面记录人员的操作细节，日志内容及日志审核的具体要求，包括：

- 1) 涉及客户信息的各系统应全面记录账号与授权管理、系统访问、业务操作、客户信息操作等行为，确保日志信息的完整、准确；
- 2) 各系统用于安全审核的原始日志记录内容应至少包括操作账号、时间、登录IP地址、详细操作内容和操作是否成功等；
- 3) 日志不应明文记录账号的口令、通信内容等系统敏感信息和客户信息；
- 4) 系统具有日志保护管理功能，即除日志日常维护涉及数据迁移外，任何人不得对日志信息进行更改、删除；
- 5) 用于客户信息安全审核、审核的原始日志必须单独保存，定期对原始日志进行备份归档，所有客户信息操作原始日志在线至少保留3个月，离线至少保留1年；
- 6) 除了系统记录日志外，各使用部门应保留所有客户信息操作的纸质凭据，确保真实有效，相关凭据至少保留1年。

6.2.2 日志审核的策略

公司需指定安全操作日志的审核策略，安全审核策略需明确审核对象、审核频度、审核方法。如需对策略变更必须明确管理流程，详细记录变更起始、终止状态以及变更内容。在日志的抽样频率与抽样比例上应满足但不限于以下原则：

- 1) 在日志审核频度与抽样比例上，要求高价值客户信息访问要求每天进行全量审核；
- 2) 中价值客户信息访问至少按周审核，日志抽样比率不能低于5%；
- 3) 低价值客户信息访问至少按月审核，日志抽样比率不能低于2%。

日志审核人员对所有日志按关键命令、关键账号、关键参数，进行抽样审核，及时发现异常时间登录、异常IP登录、异常的账号增加和权限变更、客户信息增删改查等敏感操作。

由于日志量大，因此掌握日志异常非常重要。安全员需要对可能发生的异常操作行为进行重点审核，可能在日志中记录的异常操作见表3。

表3 常见日志异常特征

异常特征	建议的参考点
日志记录与审核记录不匹配	将相关的审核导入数据库中，将审核记录中的审核手机号码和通过前台免密码的日志记录进行一一比对，查找到查询日志中有，而审核工单中没有的操作
异常的查询频率	一个月内查询号码到达几百次以上的工号和审核记录进行对比
	1. 一个号码在一天之内被查询10次以上或在一个月内查询100次以上的日志和审核记录进行对比；
	2. 对于有密码的查询也需要审核
与岗位职能不相关的操作行为	某些特别号码被一个或几个账号多次查询
	调阅具有详单查询权限的人员清单，IP地址分配表、权限表是否和授权书/权限申请书一一对应
	对免密码查询用户资料的账号进行分析，确认是否真正需要开放该权限
非工作时间及属地外登录等	将前台查询详单日志的工号和权限人员清单进行对比，确认是否一一对应
	主要是针对前台营业人员的免密码查询记录进行重点审核
对客户投诉工单的分析	分析投诉工单中的泄密事件

6.3 合规性审核

合规性审核是根据法律法规、安全策略和标准、技术标准等要求，对客户信息的安全防护工作的符合性进行检查。

客户信息安全防护包括事前预防、事中控制、事后审核3个方面，其包含的范围如图1所示。合规性审核的总体范围涵盖客户信息安全防护的各个方面，其具体内容包括：

- 1) 在进行合规性审核之前应制定明确的工作任务，包括审核目标、具体审核范围、参与人员、任务分工及相应流程等内容；
- 2) 合规性审核目标应根据不同系统存在的客户信息泄露风险进行制定，目的是审核是否存在可能由于违背了各种标准要求而易导致的客户信息泄露的不合规现象；
- 3) 合规性审核的具体范围应基于客户信息安全防护范围、相应规章制度以及根据不同系统情况进行细化和调整；
- 4) 合规性审核参与人员应较为固定，一般由专人负责或采取部门交叉方式；
- 5) 合规性审核的结果应生成报告，并进行归档管理；
- 6) 合规性检查的周期为每半年至少一次。

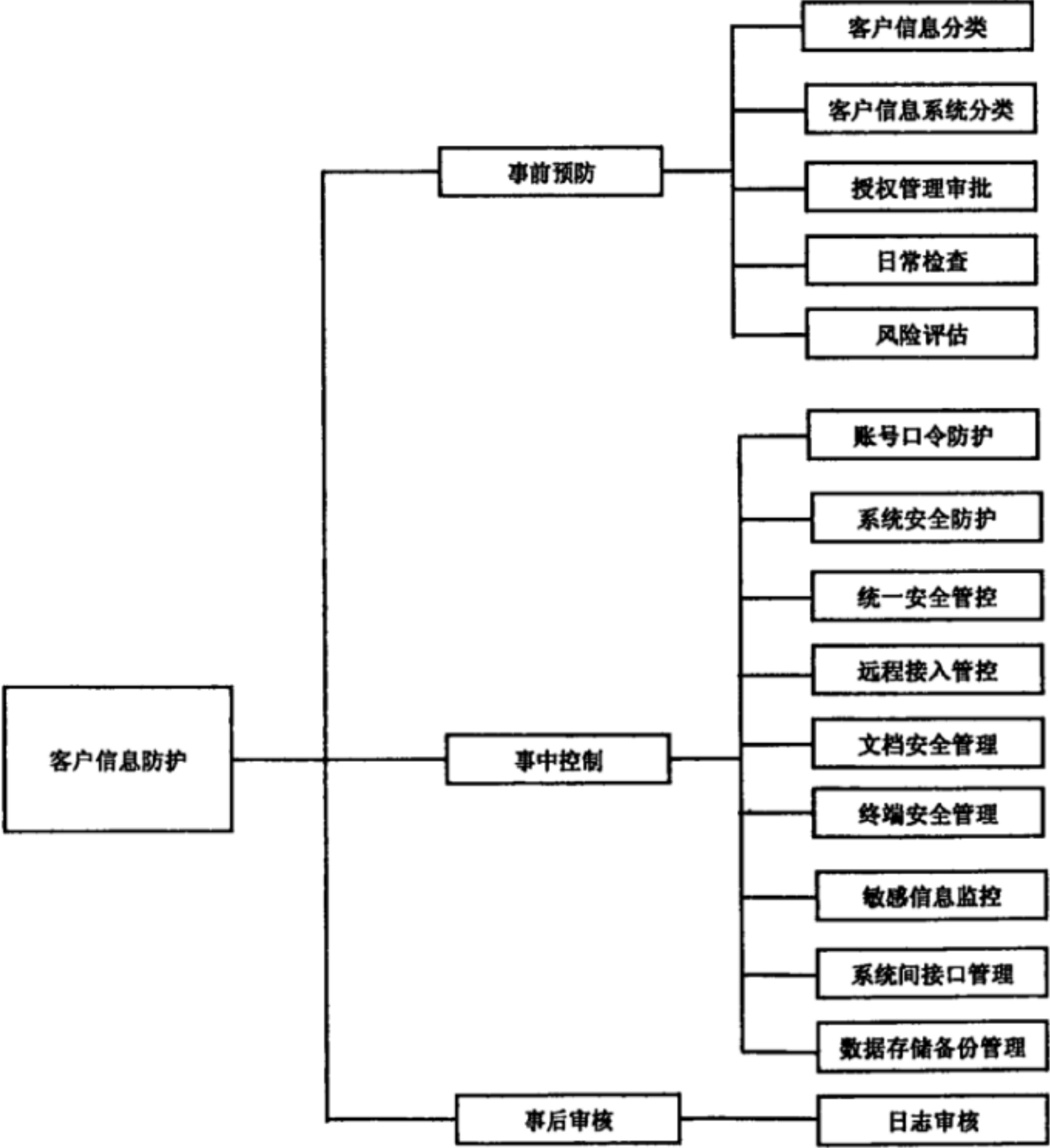


图1 客户信息安全防护范围

6.4 日常例行安全审核与风险评估

日常例行安全审核是指运维支撑部门对所负责维护的系统进行的常规性安全审核，包括日志审核、漏洞扫描、基线审核等。日常例行安全审核属于日常维护审核的范畴，应制定每日、周、月、季度日常检查报表，并按相应频次进行检查。

风险评估是对系统面临的威胁、存在的弱点、造成的影响，以及三者综合作用带来风险的可能性进行评估。所有涉及到客户信息系统的风险评估频次原则上为每半年一次。但在重大活动或敏感时期，应根据要求开展专项风险评估。风险评估侧重通过白客渗透测试技术，发现深层次安全问题，如缓冲区溢出等编程漏洞、业务流程漏洞、通信协议中存在的漏洞和弱口令等等。风险评估以各系统的运维支撑部门自评估为主、信息安全管理责任部门抽查相结合的方式进行。

7 客户信息系统的技术管控

7.1 概述

客户信息系统的技术管控主要包括系统安全防护、用户访问操作安全管控、敏感数据传输安全管控。

系统安全防护是从系统设计到日常运行维护的各个方面采用技术手段对系统进行安全防护。

用户访问操作安全管控包括统一安全管控系统和远程接入管控系统两方面内容。统一安全管控系统从技术上限制非授权用户接触客户信息。远程接入管控系统对远程登录用户的操作进行管控。

敏感数据传输安全管控包括客户信息泄密防护系统和系统间接口管理系统两方面内容。客户信息泄密防护系统对从系统中提取含有客户信息的文件进行泄密防护。系统间接口管理系统对访问敏感信息系统的接入及数据传输进行安全管控。

7.2 系统安全防护

对客户信息系统，应采取必要的安全技术手段，重点防护，主要的防护手段如下：

- 1) 系统应位于核心安全域，安全域边界采用防火墙、入侵检测系统等防护手段；
- 2) 必须严格管理和限制涉及客户信息的系统与其他系统的互联互通的能力和范围；
- 3) 安全边界的网络设备、安全设备应定期进行安全评估和审核，及时修补漏洞，杜绝弱口令；
- 4) 加强系统自身安全：
 - a) 系统在设计阶段，应当根据接口和流程涉及到客户信息的类型和操作类型（查询、修改、增删），来定义安全需求；
 - b) 建立“安全准入制度”，在系统交付阶段分别对系统的接口与流程的安全性进行评估，未达到安全要求的系统原则上不允许上线；
 - c) 做好上线前的安全评估、基线审核，封堵和修补系统、数据库、中间件、应用层的漏洞，升级安全补丁，防止系统被攻击和入侵；
- 5) 客户信息相关系统的变更必须经过相关主管的审批，并详细记录变更过程与变更结果；
- 6) 做好日常安全运维：
 - a) 做好客户信息相关系统的日常安全监控，完善告警分析与应急响应流程；
 - b) 定期审核客户信息相关系统的安全性（重大变更与系统升级后也需进行），及时修补发现的安全漏洞以及配置不符合项。

7.3 统一安全管控系统

为了从技术上限制非授权用户接触客户信息，涉及客户信息的支撑系统、业务平台、通信系统等应纳入统一安全管理。

统一安全管理系统是运维人员访问敏感信息系统后台资源（包括主机、数据库等）的唯一入口，运维人员应先登录统一安全管理系统，进行强认证后，才能访问后台系统。

应通过统一安全管控系统集中控制合法用户能访问敏感信息的权限，同时通过统一安全管控系统实现对用户访问客户信息操作日志的审核。

统一安全管控系统应实现基于主账号的集中强身份认证，应保存用户的完整操作日志，并能对用户的异常操作行为以及高敏感数据的访问行为进行预警。

7.4 远程接入管控系统

原则上，远程接入账号只能授予企业内部员工，如因特殊情况有非内部人员（开发、维护工作）需要通过远程登录访问系统，应严格限制其接触客户信息的范围，可根据系统主管授权，临时开通远程登录功能，并对远程登录操作进行监控或事后及时审阅相应的操作日志记录。

远程登录必须通过统一安全管控系统进行集中认证、授权和审核，应遵循权限最小化原则，开放用户能访问的系统及权限。

应对远程接入用户的登陆过程、操作行为进行记录，记录内容包括但不限于用户名、操作内容、登陆方式、登入时间、登出时间等信息。

7.5 客户信息泄密防护系统

从支撑系统、业务平台或通信系统中提取客户信息时，应从技术手段上防止其被泄密。可以采用防泄密技术手段包括文档安全管理、终端安全管理、敏感信息监控等。

7.5.1 文档安全管理

文档安全管理系统应实现如下防护功能：

- 1) 透明的文档加密解密；
- 2) 通过采用加密、授权、数字水印、数字签名等技术手段对文档进行安全保护，能够基于用户角色或主机的进行文档授权，使其成为受控文档，仅有被授权的特定用户或终端才能打开受控文档，未被授权的人或终端无法打开文档；
- 3) 实现文档权限控制，包括阅读、编辑、复制、拖放、打印、保存、另存为、阅读时间、打印次数及文档有效期等。

7.5.2 终端安全管理

终端安全管理系统应实现如下防护功能：

- 1) 对能处理客户信息的终端，应有终端安全管理措施；
- 2) 应统一安装防病毒软件，限制移动存储介质的使用，限制无线网络的使用；
- 3) 应有统一的接入控制，执行统一的安全策略；
- 4) 定期对扫描终端漏洞，及时升级补丁。

7.5.3 敏感信息监控系统

敏感信息监控系统应具备如下防护功能：

- 1) 定期扫描或审核终端上是否存在涉及客户信息的文件；
- 2) 防止通过移动硬盘、U盘、光驱、软驱等外设途径泄密；

- 3) 防止通过网络打印、本地打印等途径泄密;
- 4) 防止通过截屏、录像等途径泄密;
- 5) 在业务支撑网和办公自动化网(OA)内,对传输客户信息,可在网络或终端侧进行敏感信息监控;
- 6) 对通过QQ、MSN、飞信、电子邮件、HTTP等网络途径泄密客户信息进行监控;
- 7) 对监控到的批量传输客户信息的行为进行预警。

7.6 系统间接口管理系统

被访问敏感信息系统应具备安全可靠的接入鉴权机制。只有通过鉴权后才能访问接口,对于非法的访问能够进行告警并有完整的日志记录。

提供完善的数据传输保护机制,包括数据加密、完整性校验等手段。对于跨越互联网或不同等级安全域之间的数据传输,必须进行加密,以实现数据传输的安全。

对接口的所有请求和响应都要进行详细的日志记录,便于后期的故障分析和审核。

8 数据存储与备份管理

数据的存储与备份是客户信息泄露途径之一,包括电子数据和纸质文档两类数据的管理。为阻断这类泄露途径,应对该环节提出如下要求:

1) 对于存有客户信息的物理介质(磁阵、硬盘和磁带等)的维护、更换、升级和报废等操作,必须有严格的管理办法。对于要离开系统的物理介质,必须采用有效的手段由专人彻底删除客户信息后,才可离开其所在的安全区域。如果要将存有客户信息的介质交给第三方,必须得到主管领导的审批;

2) 应采取有效的技术、管理手段加强对涉及客户信息的系统使用移动存储介质的管控。应记录移动介质输出客户信息和文件的详细信息,并定期审核;

3) 应制定管理规定对存放客户信息的电子文件资料进行有效管理,规定其保存、传输、销毁等流程,防止客户信息泄露;

4) 有明确的系统数据备份计划,并且留有备份日志,以供审核使用,能够及时正确对备份异常(失败、受损)进行告警;

5) 严格限制可访问备份数据的人员和帐户,对于直接访问备份或恢复系统数据的操作,必须得到主管领导的审批,由超级用户来执行;

6) 应制定涉及客户信息的纸质文件的收集、归档及保存的管理制度。所谓纸质文件是指企业各级公司、人员在对客户进行信息传递与沟通过程中所使用书面文字形式表达的各种含有客户信息的文件。集团客户纸质文档资料、营业厅业务办理纸介资料等应按保密级别统一集中管理。纸介资料不应明文记录客户服务密码等敏感信息。

中华人民共和国
通信行业标准
基础电信运营企业移动网络客户信息安全管理框架
YD/T 2670-2013

*

人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100064
宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2014年2月第1版
印张：1 2014年2月北京第1次印刷
字数：25千字

15115·366

定价：10元

本书如有印装质量问题，请与本社联系 电话：(010)81055492