泰康人寿保险股份有限公司

客户信息安全管理暂行办法

第一章　总则

第一条　为加强泰康人寿保险股份有限公司（以下简称为公司）客户信息的安全管理，有效保护客户隐私，防止客户信息泄露，提升客户信息安全性，保障客户合法权益，特制定本办法。

第二条　本办法所称客户，不仅包括已经购买过公司任一产品的客户，也包括通过电话、邮件、信函、内外勤员工等各种合法、合规途径与公司接触过的准客户。

第三条　本办法所称客户信息是经公司各级机构在日常经营管理活动的各个环节中所接触和采集的，以各种存储形式（文档、数据、音频、视频、图片等）存储在公司的与客户相关的所有信息。

第四条　泰康人寿保险股份有限公司客户信息安全管理遵循以下原则：

（一）客户授权原则：客户信息的采集及后续存储、管理、使用都应事先获得客户有效授权，并严格遵循客户意愿予以妥善管理。

（二）封闭式管理原则：客户信息均应在公司系统内存储与调用。各单位在任何系统、任何流程中、以任何形式对客户信息的任何访问都应保留书面文档或者电子文档记录。

（三）最小暴露原则：各单位应基于职责、基于角色、基于内容对客

户信息的调用设定严格的权限管理要求，仅将工作所需的最小范围的客户信息向指定人员适当披露。

（四）全流程管理原则：各单位应对客户信息的采集、存储与调用流程进行全流程管理，做到前期有授权、过程有记录、后期有追踪。

（五）人人有责原则：客户信息安全人人有责。凡是与客户信息接触的各级岗位人员都对各自接触到的客户信息负有安全管理责任，不得擅自篡改、记录、泄露所接触到的客户信息。

（六）鼓励使用原则：客户信息需通过有序、有效使用才能最大化地转化为客户价值，助力公司业务发展。各单位应建立规范、统一、便利的客户信息调用通路，在安全可控的前提下，鼓励和促进客户信息的使用。

第五条　本办法适用于泰康人寿保险股份有限公司总公司各部门、各子公司及各分公司（以下简称各单位）。

第二章　客户信息安全管理的职责分工

第六条　客户信息归公司所有，总公司客户管理部代表公司负责管理客户信息，是客户信息安全管理的统筹、协调部门。总公司客户管理部以保障客户信息安全和有序、有效应用为原则，负责制定公司客户信息安全管理的规章制度，负责梳理公司客户信息安全管理现状，建立公司客户信息安全管理管控流程，并负责对公司客户信息安全管理情况开展定期检查与评估。同时，总公司客户管理部还负责监督各单位客户信息安全管理工作开展情况，包括调阅和审查各单位制定的客户信息安全管

理相关制度、客户信息安全相关流程与权限规则等，并负责对各单位提出的客户信息调用需求的合理性、安全性进行审批。

第七条　总公司数据信息中心是客户信息安全管理的技术保障部门，对公司客户信息技术环节的安全负责。总公司数据信息中心负责制定与实施公司客户信息安全管理技术保障方案，对客户信息采集、存储、调用等各环节提供安全技术支持，系统监控公司客户信息安全状况，并根据总公司客户管理部的审批意见，向各单位提供具体的客户信息。

第八条　各单位是客户信息的采集部门与使用部门，更是客户信息安全的具体责任部门。各单位根据各自职责分工，负责在日常经营活动中采集准确、完整的客户信息，真实的记录和保存客户信息，对客户信息的真实性、完整性负责，在此基础上各单位享有合理使用客户信息的权利。各单位应根据本办法的原则和要求，制定各单位的客户信息安全管理实施细则，建立本单位客户信息安全的宣传培训机制，完善和细化客户信息安全管理流程，监控客户信息调用过程，并保障客户信息的安全。其中，总公司幸福有约（F1）部对公司高端客户信息安全负有管理、协调、监督的职责。

第九条　总公司内控合规部、稽核监察部是客户信息安全管理的合规管理和监察管理部门，负责对公司客户信息安全管理工作的合规性提出要求，给予指导，并对公司客户信息安全管理工作中发现的问题进行处罚、追责等。

第十条　为加强公司客户信息安全管理，总公司各部门应指定一名客户信息安全管理负责人和一名客户信息安全管理联系人；各分公司、各

子公司应指定专门部门作为负责分公司、子公司及下辖机构客户信息安全管理的牵头主管部门，并同样指定一名客户信息安全管理负责人和一名客户信息安全管理联系人。

第三章　客户信息的安全级别设置

第十一条　根据客户信息安全管理要求的不同，公司根据客户信息的安全级别对客户信息予以划分，具体划分标准如下：

（一）一级客户信息：指所有客户的联系方式信息（电话、通讯地址、邮箱等）、身份证件信息、银行账号信息等具有识别客户唯一性功能的信息，通常称为敏感信息。

（二）二级客户信息：指客户的健康信息、家庭状况、理财信息、行为信息、保单信息等不具备识别客户唯一性功能，但可以据此掌握客户一定隐私的信息。

（三）三级客户信息：指不能辨识客户唯一性，又不涉及任何客户隐私的通用信息，例如性别、年龄等信息。

第十二条　根据客户信息的安全级别划分，各单位应对不同安全级别的客户信息采取不同的安全管理措施，以确保客户信息安全。

（一）对于一级客户信息：在存储和调用时需进行脱敏处理，不得批量浏览、复印、打印、扫描、下载、转发；仅可根据最严格的权限管理措施与安全管理措施，向拥有查看与调用权限的岗位人员逐条予以展示。其中，脱敏处理指存储在系统中的每一一级客户信息需屏蔽部分关键字段。其中，客户联系方式字段，需至少屏蔽中间四位；客户身份证件信

息字段，需至少屏蔽最末四位；客户银行账号信息，需至少屏蔽中间四位。凡是涉及一级客户信息的完整调用以及批量调用等需求，必须通过专项事务申请予以申请，审批获准后方可实行。

（二）对于二级客户信息：在系统中存储和调用时勿需进行脱敏处理，但也需设定严格的权限管理措施与安全管理措施。除根据职责需要，为客户直接提供服务的销售人员、服务人员和管理人员外，其余人员无权查看以及批量调用二级客户信息。

（三）对于三级客户信息：在系统中存储时勿需进行脱敏处理，可依据岗位工作需要直接调用，包括批量调用。

（四）对于一级客户信息与二级客户信息，各单位应基于当前业务发展需要，更新完善既有纸质清单下发客户信息的流程，改造为具备系统授权、系统调用、系统监控的闭环流程，逐步减少直至杜绝纸质清单的使用。

（五）超出上述客户信息安全级别设置及安全管理措施要求的任一公司客户信息的存储、调用，均需经过审批与授权。经相关流程审批授权同意的，方可实施。

第四章　基于职责、角色、内容的权限管理

第十三条　原则上，各单位可调用本单位采集、存储的客户信息，但必须制定严格的客户信息权限管理办法。

第十四条　各单位应对直接或者间接接触客户信息的岗位人员进行角色划分，根据工作需要，按照最小暴露原则限定可查看客户信息内容

范围与相应权限，不同角色的岗位人员应在可浏览和可操作的客户信息内容方面有所区隔。各单位应将各流程和各环节中与客户信息接触的人员情况、权限情况进行系统化的管理与记录。

第十五条　各单位中能接触客户信息的岗位和人员，在发生岗位人员轮换或人员离职等情况时，应对其负责的客户信息安全事宜进行严格交接。在原岗位涉及的客户信息安全事宜未得到有效确认前，不得办理换岗或者离职手续。

第十六条　各单位能接触客户信息的岗位人员均应严格遵守各单位制定的权限管理办法，既不得超出既有权限范畴调用不属于自己职责范畴中可查看的客户信息，更不得将自己的权限移交他人使用。

第十七条　原则上，各单位仅可调用由该单位采集、存储的客户信息，不得擅自调用由其他单位采集、存储的客户信息。如需调用其他单位采集、存储的客户信息，需报总公司客户管理部，经与客户信息提供方就客户信息调用达成一致意见后方可实施。

第五章　基于客户信息接触流程的安全管理

第十八条　采集流程。与客户接触的各岗位人员应在接触客户并采集客户信息后，及时通过各种方式将客户信息予以真实、完整的记录，并提交至公司统一存储与管理，不得提供虚假、不真实的客户信息。与客户信息采集相关的销售、录入、承保、档案管理等岗位人员应及时将记录有客户信息的原始文档提交至公司，不得擅自复印、刻录保留有客户信息的原始资料，更不得将这些原始信息挪作他用，严禁泄露和倒卖客

户信息。同时，在客户信息采集时，需通过书面的方式获取客户关于其信息采集、留存、保管、使用的有效授权。各单位不得通过非法途径或者非合规途径采集客户信息。

第十九条　存储流程。客户信息在存储时，需根据客户信息的安全级别划分，进行相应的权限管理与系统加密处理。对于以纸质档案形式在系统外保管的客户信息，需建立严格的调用权限、审批权限与档案管理制度，并对调用情况登记造册。

第二十条　变更流程。客户信息存储进入公司后，各单位、各级人员不得在客户不知情的情况下擅自修改客户信息，更不得违背客户意愿故意用虚假信息替换真实信息。客户信息的变更需经过客户本人同意或者授权。

第二十一条　调用申请。公司客户信息的调用流程可以分为常规需求和非常规需求两大类。常规需求是指各单位在日常经营管理工作中基于岗位职责需要，需定期（每日、每月、每季度、每年）调用客户数据用于公司日常运营、服务、管理等工作需要而产生的需求。例如两核、保全、个银续期分单等工作涉及的需求。非常规需求是指区别于常规需求，各单位不定期产生的客户信息调用需求。对于常规需求，总公司客户管理部将定期梳理，合理授权，以保障公司日常经营管理工作的正常开展。经授权确定的常规需求，可不再单独提交应用申请。而非常规需求及新增常规需求需提交应用申请，经审批同意后方可实施。

各单位的非常规类需求，在调用客户信息时，需提交专项申请，提供审批所需的相关材料，并经审批通过后，方可调用相关客户信息（具体

的申请流程详见附件）。对于各种类型的非常规类客户信息调用需求，具体要求如下:

（一）内部调用需求:

1.提交内部调用需求时，各单位需提供包含如下内容的书面材料:

（1）客户信息调用范围，明确涉及哪一级别的客户信息;

（2）客户信息调用的目的;

（3）客户信息使用方案，包括使用人、使用方式、使用目标、使用期限、客户信息传递方式、客户信息安全管理责任人、客户信息安全管理措施等。

2.内部调用时,各单位客户信息使用方案中指定的客户信息安全管理责任人以及与客户信息接触的相关人员应确认已签订公司统一制定的《保密协议书》。

3.各单位因为内部需求申请调用的客户信息,应优先考虑在公司系统环境中，通过各类销售/服务工具，点对点向销售/服务人员传递，尽量避免清单方式、纸质方式传递。

4.各单位因为内部需求申请调用的客户信息,必须按照申请时提供的客户信息使用方案予以使用，不得挪作他用；使用期限完毕后需及时销毁，逾期不得转移、保存。

5.各单位的内部调用需求，均需报各单位负责人知晓并审批。其中，分公司的需求需报分公司总经理审批；总公司各部门的需求需报部门总经理审批。

6.各单位的内部调用需求需提交至总公司客户管理部审批。总公司客

户管理部根据各单位提交的申请材料，视情况分别加签相关部门会签后，统一出具审批意见。其中，若需求中涉及高客信息，需报总公司幸福有约（F1）部会签。

7. 各单位应严格按照客户信息申请流程（详见附件）提出内部客户信息申请需求。

（二）外部调用需求（政府机构、监管机构、司法机关调用类）

1. 提交此类调用需求时，各单位需提供包含如下内容的书面材料:

（1）相关机构带有公章的书面公函;

（2）客户信息调用范围，明确涉及哪一级别的客户信息;

（3）客户信息内外部接收人、客户信息传递方式等。

2.各单位应积极配合政府机构、监管机构、司法机关的要求，但同时也必须充分考虑公司保护客户信息安全的职责，与政府机构、监管机构、司法机关等协调沟通将所需提供的客户信息范围减少至最少。

3.各单位因为政府机构、监管机构、司法机关需求申请调用的客户信息，应根据相关机构的要求予以妥善传递、保管。各单位应指定专人负责管理此类客户信息，除此指定人员外，其余人员不得接触此客户信息。指定人员接收到的客户信息在传递至相关机构前，需注意客户信息的安全管理；客户信息传递至相关机构后，指定人员需即时销毁其所接收到的客户信息，不得逾期保存，更不得转移客户信息。

4.此类客户信息的申请流程与内部申请流程一致。

（三）外部调用需求（兼业代理机构合作需求类）

1. 提交此类调用需求时，各单位需提供包含如下内容的书面材料:

（1）兼业代理机构带有公章的书面公函;

（2）客户信息调用范围，明确涉及哪一级别的客户信息;

（3）兼业代理机构与公司签订的合作协议、保密协议;

（4）兼业代理机构拟采取的客户信息安全管理措施、兼业代理机构指定的客户信息安全管理责任人（包括姓名、办公电话、部门、职位、工作邮箱等）、与兼业代理机构约定的客户信息传递方式。

2.各单位与兼业代理机构签订的合作协议中应约定双方接触、使用客户信息的范围，双方接触、使用客户信息的机构、部门、岗位和人员的权限以及客户信息传递方式。可提供给兼业代理机构的客户信息需视双方合作协议中约定内容执行，未在双方合作协议中提及的客户信息不得提供。

3.与兼业代理机构之间的客户信息传递应优先采用系统对接方式，其次应选用总对总电子数据传递方式，最后才能选择通过各单位专人传递的方式。如果选择通过各单位专人传递方式，指定人员接收到的客户信息在传递至兼业代理机构前，需注意客户信息的安全管理；客户信息传递至兼业代理机构后，指定人员需即时销毁其所接收到的客户信息，不得逾期保存，更不得转移客户信息。

4.各单位与兼业代理机构的合作事宜中若涉及客户信息事宜，应第一时间告知总公司客户管理部，并在明确客户信息交互事宜前书面获得总公司客户管理部意见。

5.此类客户信息的申请流程与内部申请流程一致。

（四）外部调用需求（与第三方服务机构合作事宜类）

1.各单位与第三方服务机构开展合作时，在合作初期就应考虑客户信息安全事宜。各单位与第三方服务机构的合作谈判中应将需提供给第三方的客户信息缩减到最少。原则上，一级客户信息不得提供。如必须提供，则必须通过屏蔽部分字段等方式提升安全级别后方可提供。二级客户信息则需按照“最小暴露原则”，根据与第三方服务机构的合作范围约定，提供最小范围的信息。对于确需提供完整的一级客户信息、二级客户信息，方可有效开展合作的此类需求，需专项申请，经审批授权同意后方可实施。

2.各单位与第三方服务机构签订的合作协议中应包含保密条款，约定双方接触、使用客户信息的范围，双方接触、使用客户信息的机构、部门、岗位和人员的权限以及客户信息传递方式。可提供给第三方服务机构的客户信息需视双方合作协议中约定内容执行，未在双方合作协议中提及的客户信息不得提供。

3.与第三方服务机构之间的客户信息传递应优先采用系统对接方式，其次应选用总对总电子数据传递方式，最后才能选择通过各单位专人传递的方式。如果选择通过各单位专人传递方式，指定人员接收到的客户信息在传递至兼业代理机构前，需注意客户信息的安全管理；客户信息传递至兼业代理机构后，指定人员需即时销毁其所接收到的客户信息，不得逾期保存，更不得转移客户信息。

4.与第三方服务机构的合作若涉及客户信息向第三方提供，应在提供给第三方服务机构客户信息前，书面征求客户意见。若客户不同意，则不得提供该名客户信息至第三方。

5.各单位与第三方服务机构的合作事宜中若涉及客户信息事宜，应第一时间告知总公司客户管理部，并在明确客户信息交互事宜前书面获得总公司客户管理部意见。

第二十二条　客户信息的提取与下发。本文所指提取，不仅仅指客户信息从公司系统中批量导出，也包括在公司系统中的调用、展示。各单位的信息技术部门是公司客户信息的唯一提取部门与下发部门。无论是常规类需求，还是非常规类需求，各单位的信息技术部门应根据总公司客户管理部的审批意见进行提取和下发。各单位的信息技术部门均应确保对提取的客户信息进行了相应的加密处理，设定了严格的权限管理措施，对接收客户信息的单位或个人电脑采用了严格的域管理，同时提取后的客户信息是优先通过公司系统传递，并保留了接触轨迹记录。

第二十三条　客户信息下发后的追踪管理。无论是常规类需求，还是非常规类需求，各单位获得数据后应按照公司客户信息安全管理要求妥善保管客户信息，并对客户信息调用后的使用情况、使用效果进行及时评估、总结。总公司客户管理部可联合总公司内控合规部对各单位提取的客户信息进行追踪抽查，评估客户信息安全状况与使用效果。对于检查中发现有违规使用客户信息，或者存在客户信息泄露等情况的机构，可要求该单位进行整改并在整改未完成前暂停该单位的客户信息调用权限。

第二十四条　客户信息的销毁。各单位应在客户信息调用申请中明确客户信息使用期限。超过使用期限的客户信息应第一时间销毁，不得逾期使用，更不得擅自转移。

第六章　客户信息安全的技术保障

第二十五条　总公司数据信息中心以及各单位的信息技术部门(以下简称各级信息技术部门)是公司客户信息安全的技术保障部门。各级信息技术部门应加快客户信息安全保障措施的部署，提升公司客户信息安全水平,确保公司客户信息存储在公司各类系统中(纸质文档信息除外),并按照客户信息的安全级别设置采取了相应的安全管理措施，包括但不限于脱敏、加密、域管理、轨迹记录等。

第二十六条　各分公司的信息技术部门不得在总公司不知情或者未授权的情况下擅自存储公司一级客户信息,使其脱离公司系统监控使用。

第二十七条　各级信息技术部门应为各单位客户信息的调用需求建立系统化通路，确保各级客户信息可方便、快捷地在公司系统中流转，逐步减少直至取消系统外流转途径。

第二十八条　各级信息技术部门应根据各单位制定的客户信息权限管理办法，对各单位与客户信息相关的系统、流程进行相应的权限设置。同时公司各个信息系统均应能完整记录与客户信息安全相关的用户（账户）登录和浏览信息的痕迹。总公司数据信息中心应将客户信息浏览、查询、下载等情况定期告知总公司客户管理部、内控合规部，用于评估客户信息安全状况。根据工作需要，总公司客户管理部、内控合规部可组织临时抽检，并有权对异常情况开展调查。

第二十九条　各级信息技术部门在非常规类客户信息提取和下发后，应对所下发的客户信息的存储与管理情况进行追踪、记录。各级信息技

术部门应将监控到的客户信息存储与管理情况定期告知总公司客户管理部、内控合规部用于评估客户信息安全状况。

第三十条　各级信息技术部门均应对于本单位人员接触客户信息的权限进行设置与管理，指定专人负责接触、管理客户信息。各级信息技术部门根据工作需要聘请的外包人员一律不得接触一级客户信息。

第三十一条　各级信息技术部门应在系统开发阶段就应考虑客户信息安全事宜。若系统开发过程中涉及客户信息安全事宜，应第一时间告知总公司客户管理部，并在书面获得总公司客户管理部意见后方可实施开发。

第三十二条　各级信息技术部门同时承担着客户信息安全风险提示的责任。鉴于对新科技、新技术掌握的先见性，各级信息技术部门应及时向各单位通报客户信息安全相关科技发展趋势，提示客户信息使用安全方面的技术漏洞，并提出改善建议。

第七章　系统外客户信息存储文件的管理

第三十三条　鉴于公司当前日常经营活动的现状，在实际经营活动中，不可避免地仍然会有客户信息存储文件的传递环节。例如保单或缴费通知单递送、客户问卷回收等。此类系统外客户信息存储文件也属于客户信息安全管理范畴，需加强管理。

第三十四条　各单位对存储于系统外的客户信息存储文件应采用档案管理之方式，由专人对查阅、携带、递送等环节进行严格审批与登记。未经授权，不得擅自复印、刻录保留有客户信息的原始资料，更不得将

这些原始信息挪作他用。

第三十五条　系统外客户信息存储文件调阅时，应有负责管理的专人陪同查阅；查阅期间，除非事先经审批同意，否则不得篡改、复印、记录任何客户信息。

第三十六条　对于使用完毕或已以电子形式进行系统存储的纸质文件，应建立销毁制度。

第八章　关于高端客户信息安全管理的特别要求

第三十七条　本文所指高端客户，是指在公司拥有钻石卡以上贵宾身份的客户。

第三十八条　各单位不得擅自存留高端客户信息，不得擅自调用、使用高端客户信息，更不得擅自与高端客户接触。

第三十九条　高端客户的敏感信息、隐私信息均属于公司一级客户信息，应当按照一级客户信息的安全管理要求进行最高级别的保护和管理。

（一）公司各个系统应对高端客户进行标识，在各个流程节点上实现对高端客户身份的识别。

（二）对于高端客户信息，在公司各个系统中不可直接显示如下信息：客户姓名、客户联系方式（手机、固话、email、通讯地址）、客户身份证件号码、客户银行账号等。在系统中显示时，需进行加密处理，加密原则同一级客户信息加密原则。其中，客户姓名的加密原则为，仅显示姓氏，屏蔽名字。但公司部分岗位因工作需要，经授权批准后可不受此限。

（三）高端客户敏感信息，尤其是客户姓名、客户联系方式（手机、固话、email、通讯地址）、客户身份证件号码、客户银行账号、保单号此五类信息，不得以清单方式批量查询、提取、下载。对于需要批量查看、调用高端客户敏感信息和隐私信息的需求，应当报总公司客户管理部，会签总公司幸福有约（F1）部后，报公司管委会审批同意方可实施。

（四）高端客户的统计类信息，也需严格管理。各单位需指定专人获取、保管高端客户的统计类信息，以开展相关分析工作，为更好的服务高端客户提供数据支持。

（五）高端客户信息仅可通过公司系统中的销售支持类工具（例如 MSS 等）点对点传递至其指定业务人员和服务人员之中。因此，在开展高端客户活动之前，各单位应确保发布高客信息的销售支持类工具开发完毕。

（六）记载有高端客户信息的所有纸质档案，包括投保单、确认函、财务证明资料、健康证明资料、理赔/保全等环节提交资料等，均应视为公司重要纸质档案，需单独存放，由档案管理专人负责，不得擅自复印、刻录，更不得将这些原始信息挪作他用。除非有总公司幸福有约（F1）部授权，否则不得提供查询、复印、扫描之用。

（七）各单位应建立高端客户信息权限管理办法，严格限定可接触高端客户信息的岗位及人员。根据各单位的工作需要，基于职责、流程和权限，可允许各单位一至两名指定人员有权限查看高端客户的敏感信息和隐私信息。同时，直接为高端客户提供一对一服务的人员，可通过公司系统中的销售支持类工具获得所需服务对象的相关信息。除上述两类

人员，其余人员不得接触、查询高端客户具体信息。

第四十条　对于高端客户，应指定一对一的业务人员或者服务人员为其提供专业服务。关于高端客户业务人员的指定规则由总公司幸福有约（F1）部发文公布。关于高端客户服务人员的指定规则由总公司运营中心发文公布。仅有这些指定的业务人员和服务人员在为高端客户提供服务时，才能在公司提供的工具中依活动内容的需要获得一定的高客信息。具体可提供信息依活动方案而定。

第四十一条　各级信息技术部门对于本单位人员接触高端客户信息的权限应进行更严格的设置与管理。

第四十二条　关于高端客户信息安全事宜未尽之处，由总公司幸福有约（F1）部另行发文公布。

第九章　客户信息安全管理的规范要求

第四十三条　除保监会颁布的《保险公司信息披露管理办法》规定应披露的客户信息之外，公司任何单位及个人未经授权，不得以任何方式在任何公众平台、公众场合及办公场合擅自谈及、发布和泄露任何公司客户信息，更不得将公司客户信息用于其他商业用途。

第四十四条　对于各单位与客户信息安全相关的人员，均应要求其签订《保密协议书》及《保密工作责任书》，并定期对其开展客户信息安全教育。

第四十五条　各单位应对各自经营活动中所采集、存储、调用的客户信息的安全负责。各单位应对各自经营活动中客户信息采集、存储、调

用的各个流程环节制定客户信息安全管理规范，组织客户信息安全管理培训，制定客户信息安全监控流程，并严格实施，确保公司客户信息安全。

第四十六条　总公司客户管理部、内控合规部、稽核监察部有权对各单位客户信息安全管理工作的完整性、规范性、有效性进行评估，并调用各单位关于客户信息安全事宜的相关工作材料，包括但不限于制度规范、流程权限、培训情况等。

第四十七条　一旦发生客户信息泄露事件，各单位应立即采取补救措施，尽量减少泄露事件造成的损失。各单位发生客户信息泄露事件应在发现后 24 小时内，书面向上级单位报告，并同时报至总公司客户管理部、内控合规部、稽核监察部。书面报告客户信息泄露事件的内容包括：被泄露客户信息的内容、范围、数量及其载体形式；客户信息泄露事件的发现经过；客户信息泄露当事人的基本情况；客户信息泄露事件发生的时间、地点及经过；客户信息泄露事件造成或可能造成的危害；已进行或拟进行查处的工作情况；已采取或拟采取的补救措施。

第四十八条　对于违反本办法规定的，无论是否产生客户信息安全事件的，均可按照本办法及《泰康人寿保险股份有限公司保密管理规定》、《泰康人寿保险股份有限公司处罚管理规定》、《泰康人寿保险股份有限公司案件责任追究规定》等相关办法对当事机构、当事人予以严肃处理。情节严重的，公司将保留追究其相关法律责任的权利。同时，除当事机构、当事人承担相关责任外，根据客户信息安全事件的产生缘由以及事件严重程度，公司可对当事人所在单位以及上级单位以及相关人员进行

问责。

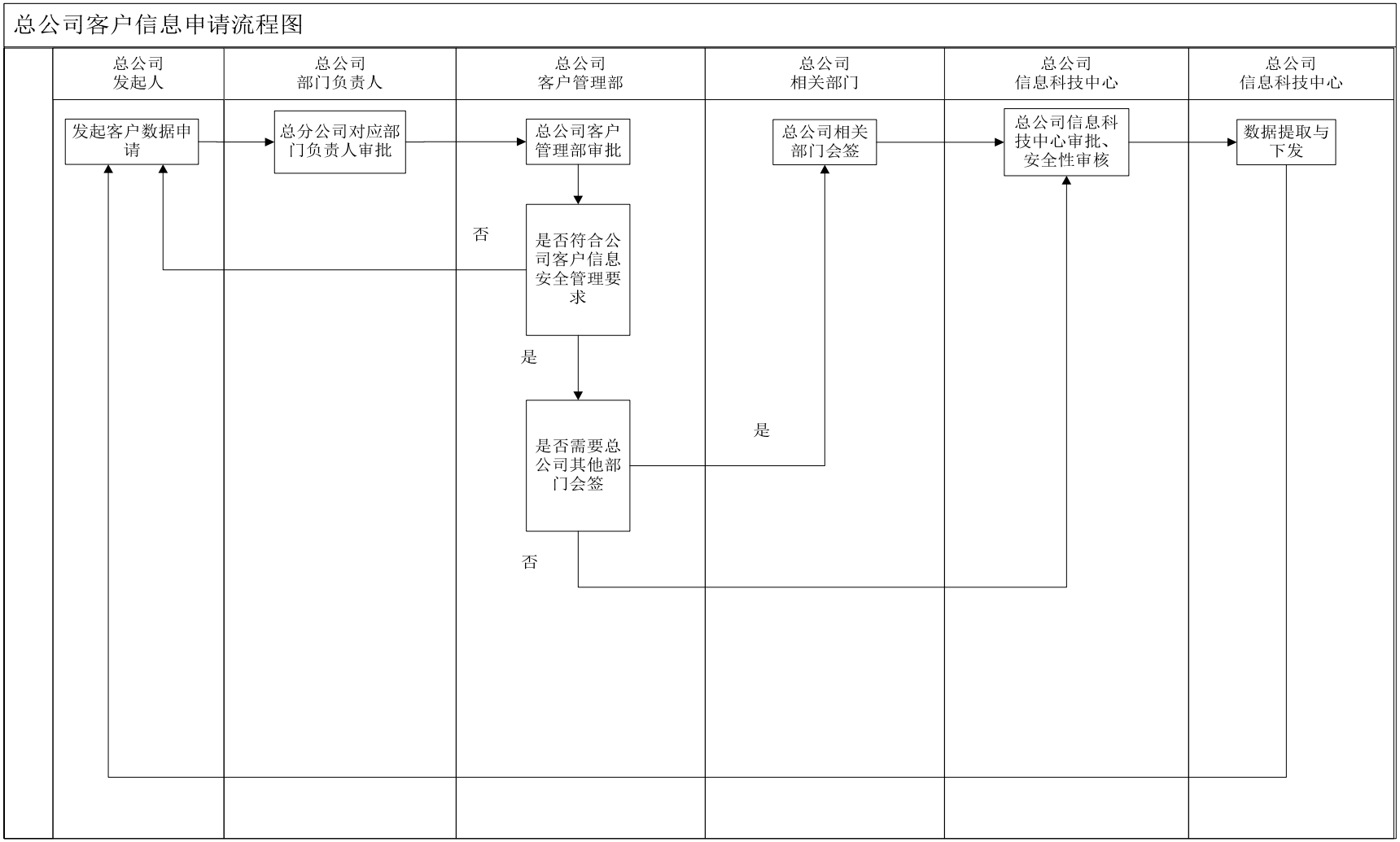
十、附则

第四十九条　本办法的解释权归总公司客户管理部。

第五十条　本办法中相关规定如与《泰康人寿保险股份有限公司客户数据管理暂行办法（2012版）》中规定有冲突的，以本办法为准。

第五十一条　本办法自印发之日起执行。

附件一：总公司客户信息申请流程图



附件二：分公司客户信息申请流程图