中国太平洋财产保险股份有限公司

宁波市网络安全保险条款

总则

第一条 本保险合同由保险条款、投保单、保险单、保险凭证以及批单组成。凡涉及本保险合同的约定，均应采用书面形式。

第二条 凡在中华人民共和国境内（**不包括港、澳、台地区**）依法设立并合法经营、拥有、管理、使用或提供网络服务的企业或机构，均可作为本保险合同的投保人或被保险人。

保险责任

第三条 在保险期间内，被保险人在合法使用或提供网络服务时，因被保险人拥有、租赁、由被保险人书面委托的第三方为其代管、被许可使用或控制的组成网络的各计算机系统（**以下简称计算机系统**）发生**网络安全事故**，导致被保险人的下列经济损失，保险人按照保险合同的约定负责赔偿。

（一）营业中断损失

在保险期间内，因发生网络安全事故，造成被保险计算机系统全部或部分中断，导致被保险人营业受到干扰或中断，由此而产生赔偿期内的毛利润损失，保险人按照本保险合同的约定负责赔偿。

本保险合同所称赔偿期是指自网络安全事故发生之日起，被保险人的营业结果因网络安全事故而受到影响的期间，但该期间最长不得超过本保险合同约定的最大赔偿期。最大赔偿期由投保人和保险人协商确定，并在保险单中载明。

（二）网络勒索损失

在保险期间内，因计算机系统遭受安全威胁产生勒索损失，保险人按照本保险合同的约定负责赔偿。

第四条 在保险期间内，被保险人在合法使用或提供网络服务时，因被保险人拥有、租赁、由被保险人书面委托的第三方为其代管、被许可使用或控制的组成网络的各计算机系统（以下简称计算机系统）发生经政府主管部门认定的**网络安全事件**，导致被保险人的经济损失，保险人按照保险合同的约定负责赔偿。

第五条 其他费用

在保险期间内，因系统存在高风险漏洞且被政府相关部门进行通报以及发生以上保险事故而需要的数据修复费用、硬件改善费用和事故响应费用，以及保险人、被保险人为查明和确定保险事故是否发生、事故性质、原因和损失程度所支付的必要的、合理的调查费用，及保险事故发生后和被保险人为防止或者减少损失所支付的必要的、合理的减损费用，保险人按照本保险合同的约定负责赔偿。

责任免除

第六条 下列原因造成的损失、费用和责任，保险人不负责赔偿：

（一）投保人、被保险人或其雇员、IT 外包商及其雇员的欺诈、违法行为、犯罪行为、重大过失行为或故意行为（包括但不限于故意或明知的违反义务、合同的行为）；

（二）战争、入侵、敌对行动、军事行为、武装冲突、罢工、骚乱、暴动、间谍行为；

（三）除网络恐怖主义活动外的其他恐怖主义活动；

（四）核辐射、核爆炸、核污染及其他放射性污染；

（五）大气污染、土地污染、水污染及其他非放射性污染；

（六）任何基础设施故障或供应中断，包括：

1.机械故障，包括但不限于任何计算机及周边设备有形财产本身的物理性故障、腐蚀、磨损或失窃；

2.电气故障，包括但不限于电力或电压突然升高、过载、短路等；

3.公共供应系统故障，包括但不限于供电、供水、供气中断等；

4.第三方通讯系统、电信系统、卫星系统等的中断或故障；

5.空调系统故障；

（七）任何国际国内官方机构、政府、军队及其所属机构所组织、实施的网络攻击、侵入等引起的网络安全事故；

（八）被保险人未经授权、私下进行或不当收集个人数据；

（九）超越被保险人的营业执照或执业许可证确定的经营范围，或者在无有效营业执照或执业许可证期间提供的服务和行为；

（十）侵犯知识产权或商业秘密造成网络风险事故导致的信息泄露；

（十一）被保险人及其雇员未经对方授权，主动攻击、潜入他人网络所引起的对方防御、反攻击等行为所导致的网络安全事故；

（十二）被保险人在得知其 IT 外包商提供的服务处于非正常状态的情况下，未及时处理并通知保险人所导致的网络安全事故；

（十三）拒绝服务攻击。

第七条 下列损失、费用和责任，保险人不负责赔偿：

（一）通过攻击在案漏洞库（即保险事故发生时，至少在 CVE、CNVD、CNNVD 三个安全漏洞库之一中有记录在案）之外的漏洞造成的保险事故导致的损失、费用和责任；

（二）任何人身损害及有形财产的实际损害；

（三）因有形财产损失导致的营业中断损失；

（四）被保险人应该承担的合同责任，但无合同存在时仍然应由被保险人承担的经济赔偿责任不在此限；

（五）罚款、罚金及惩罚性赔偿；

（六）精神损害赔偿，包括法院判决的精神损害赔偿；

（七）任何自然灾害或火灾意外事故导致的损失和费用；

（八）投保人、被保险人在投保前已获悉或可以合理预见的网络事件或索赔；

（九）因网络繁忙造成的相关损失和费用；

（十）任何违反有关反垄断、限制性交易行为或消费者保护的法律法规而引起的损失或费用；

（十一）任何由于计算机系统或其组成部分的计划停机、预期检修及空档期而导致的损失或赔偿责任；

（十二）因被保险人自身原因，导致异地设备未设置网络安防系统，提出的相关索赔申请；

（十三）被保险人及其代表、雇员的个人信息泄露所造成的损失、费用和责任；

（十四）被保险人的计算机系统未达到网络安全行业的合法认证所造成的损失、费用和责任；

（十五）本保险合同中载明的免赔额或按本保险合同载明的免赔率、免赔期计算的金额；

（十六）合法拥有被保险人内部系统访问权限的外部合作伙伴的故意行为或违法行为而导致的损失。

第八条 **出现下列情形之一，保险人不负责赔偿：**

（一）被保险人主动关闭网络安防系统；

（二）被保险人使用了无合法有效授权的软件与程序而导致的无法升级、缺陷、漏洞及质量问题。

赔偿限额、保险金额、免赔额（率）与免赔期

第九条 除另有约定外，网络安全事故、网络安全事件和其他费用各项保险责任的赔偿限额包括每次事故赔偿限额和累计赔偿限额，各项保险责任的赔偿限额由投保人和保险人协商确定，并在保险单中载明。同时，保险人按照本保险合同在约定的赔偿限额内负责赔偿。

第十条 营业中断损失责任的保险金额和最大赔偿期限，以及其他各项保险金额由投保人和保险人协商确定，并在保险单中载明。

第十一条 每次事故免赔额（率）、免赔期由投保人与保险人在签订保险合同时协商确定，并在保险单中载明。

第十二条 免赔期、免赔额（率）适用于营业中断责任的免赔设置；免赔额（率）适用本条款其他责任的免赔设置。同时约定免赔额、免赔率的，免赔金额以免赔额、按照免赔率计算的免赔额或按免赔期计算的免赔额中的高者为准。

保险期间

第十三条 除另有约定外，保险期间为一年，以保险单载明的起讫时间为准。

保险人义务

第十四条 本保险合同成立后，保险人应当及时向投保人签发保险单或其他保险凭证。

第十五条 保险事故发生后，投保人、被保险人提供的有关索赔的证明和资料不完整的，保险人应当及时一次性通知投保人、被保险人补充提供。

第十六条 保险人收到被保险人的赔偿请求后，应当及时就是否属于保险责任作出核定；情形复杂的，应当在**三十日**内作出核定，但本保险合同另有约定的除外。

保险人应当将核定结果通知被保险人；对属于保险责任的，在与被保险人达成赔偿保险金的协议后十日内，履行赔偿保险金义务。本保险合同对赔偿保险金的期限另有约定的，保险人应当按照约定履行赔偿保险金的义务。保险人依照前款的规定作出核定后，对不属于保险责任的，应当自作出核定之日起三日内向被保险人发出拒绝赔偿保险金通知书，并说明理由。

第十七条 保险人自收到赔偿保险金的请求和有关证明、资料之日起六十日内，对其赔偿保险金的数额不能确定的，应当根据已有证明和资料可以确定的数额先予支付；保险人最终确定赔偿的数额后，应当支付相应的差额。

投保人、被保险人义务

第十八条 投保人应履行如实告知义务，如实回答保险人就被保险人网络运营情况、网络安全防护措施以及其他有关情况提出的询问，并如实填写问卷调查表及投保单。

投保人故意或者因重大过失未履行前款规定的如实告知义务，足以影响保险人决定是否同意承保或者提高保险费率的，保险人有权解除保险合同。

投保人故意不履行如实告知义务的，保险人对于合同解除前发生的保险事故，不承担赔偿保险金的责任，并不退还保险费。

投保人因重大过失未履行如实告知义务，对保险事故的发生有严重影响的，保险人对于合同解除前发生的保险事故，不承担赔偿保险金的责任，但应当退还保险费。

第十九条 除本保险合同另有约定外，投保人应当在本保险合同成立时一次性交清保险费，保险费交清前，本保险合同不生效，保险人不承担赔偿责任。采用分期支付保险费的，投保人应按照本保险合同的约定，按时支付保险费。若投保人未按照本保险合同的约定支付保险费的，则保险人有权通知投保人解除本保险合同，该保险合同自保险人发出解除书面合同通知时解除。

第二十条 被保险人应严格遵守国家法律法规及政府有关部门制定的有关互联网及网络安全建设的各项规定，加强管理，采取合理的预防措施，尽力避免或减少责任事故的发生。

保险人可以对被保险人遵守前款约定的情况进行检查，向投保人、被保险人提出消除不安全因素和隐患的书面建议，投保人、被保险人应该认真付诸实施。如保险人指派第三方专业机构，被保险人应给予配合。

投保人、被保险人未按照约定履行上述安全义务的，保险人有权要求增加保险费或者解除合同。

除投保人与保险人事先书面约定外，被保险人应至少对中国国家信息安全漏洞库、CVE公开发布的1个月及以上的高危安全漏洞进行修补，且对操作系统、软件、其他系统进行及时升级，否则由此导致的损失、费用及责任，保险人不予赔偿。

被保险人应始终设置或主动开启网络安全防御措施、网络安全防御措施使其不低于保

单生效前的约定标准。同时应当履行如下安全义务，否则，保险人不承担赔偿责任：

（一）所有通过外网可以访问或存储重要数据的服务器及电脑终端已安装病毒及恶意程序防护软件，并开启实时防护功能和病毒库自动更新功能。

（二）被保险人所有通过外网可以访问的网络及网络组件应部署有网络防火墙（软硬件防火墙），已正常配置并始终处于开启状态。

第二十一条 在保险合同有效期内，发生不限于下列情形而导致被保险人计算机系统的危险程度显著增加的，被保险人应当按照合同约定及时通知保险人，**保险人可以按照合同约定增加保险费或者解除合同。**

（一）被保险人收购或组建子公司；

（二）被保险人的子公司被收购；

（三）被保险人被收购或破产。

被保险人未履行前款约定的通知义务的，因保险标的的危险程度显著增加而发生的保险事故，保险人不承担赔偿保险金的责任。

第二十二条 知道保险事故发生后，被保险人应该：

（一）尽力采取必要、合理的措施，防止或减少损失，**并须在 2 小时之内报案，否则，对因此扩大的损失，保险人不承担赔偿责任；**

（二）无论被保险人是否提出赔偿请求或者是否造成实质损失，被保险人都应及时通知保险人，并书面说明事故发生的原因、经过和损失情况；**故意或者因重大过失未及时通知，致使保险事故的性质、原因、损失程度等难以确定的，保险人对无法确定的部分，不承担赔偿责任，但保险人通过其他途径已经及时知道或者应当及时知道保险事故发生的除外；对于事故发生的原因，被保险人应及时进行排查，并尽力采取必要、合理的措施进行应对和整改，直到保险人认可相关整改措施已足以防范同类事故。**

（三）及时对事故现场取证，被保险人应保护好相关的硬件、软件、数据及文件等证明材料；允许并且协助保险人或事故鉴定人进行事故调查；**对于拒绝或者妨碍保险人或事故鉴定人进行事故调查导致无法确定事故原因或核实损失情况的，保险人对无法确定或核实的部分，不承担赔偿责任；**

（四）涉及违法、犯罪的，应立即向公安部门报案，**否则对因此扩大的损失，保险人不承担赔偿责任。**

（五）被保险人应积极配合保险公司指定的机构对受感染或被攻击系统进行解密和恢复运行。**在确保受损计算机系统功能尽快恢复运行的前提下，被保险人应当会同保险人检测、协商确定恢复项目、方式和费用。对未协商确定的，保险人及保险人指定的机构可以重新核定。**

第二十三条 被保险人获悉可能发生诉讼、仲裁时，应立即以书面形式通知保险人；接到法院传票或其他法律文书后，应将其副本及时送交保险人。保险人有权以被保险人的名义处理有关诉讼或仲裁事宜，被保险人应提供有关文件，并给予必要的协助。

对因未及时提供上述通知或必要协助导致扩大的损失，保险人不承担赔偿责任。

第二十四条 被保险人请求赔偿时，应向保险人提供下列证明和资料：

（一）保险单正本；

（二）索赔申请书；

（三）如发生网络安全事件，须提供政府认定的证明材料；

（四）经判决或仲裁的，应提供判决文书或仲裁裁决文书；

（五）投保人、被保险人所能提供的其他与确认保险事故性质、原因、损失程度等有关的证明和资料；如被保险人和保险人就相关证明和资料无法达成一致的，需要提供双方认可的第三方专业机构作为咨询顾问或事故处理专家出具的与确认保险事故性质、原因、损失程度等有关的证明和资料。

投保人、被保险人未履行前款约定的索赔材料提供义务，导致保险人无法核实损失情况的，保险人对无法核实部分不承担赔偿责任。

第二十五条 发生保险责任范围内的损失，应由有关责任方负责赔偿的，被保险人应行使或者保留向该责任方请求赔偿的权利。

赔偿处理

第二十六条 在保险期间内，发生保险责任范围内的网络安全事故导致的营业中断损失，**保险人和被保险人同意按照以下方式计算赔偿，但以对应的赔偿限额为限，确定赔偿金额的方法如下：**

（一）根据营业中断时长，赔付金额以赔偿期内的毛利润损失为限，按照实际损失赔偿。

毛利润损失为“标准营业收入与赔偿期内的实际营业收入的差额”与“毛利润率”的乘积，即：毛利润率×（标准营业收入－赔偿期内的实际营业收入）

其中，营业收入是指被保险人在营业过程中，因销售商品、提供劳务或者让渡资产使用权等实现的收入金额。

毛利润率是指发生保险事故之日前最近一个完整的会计年度内的毛利润与营业收入的比率。

标准营业收入是指发生保险事故之日前十二个月中与赔偿期对应的日历期间的营业收入。

在赔偿期内，被保险人或他人代其从事经营业务而取得的营业收入，应计算在赔偿期内的实际营业收入内。

（二）或经投保人与保险人协商确定，根据企业营业收入区间，赔付金额按照保险单载明的保险金额为限，按照实际损失赔偿。

投保人与保险人商定赔付方式，以上可二选一，并以保险单载明的赔付方式为准。

第二十七条 在保险期间内，发生保险责任范围内的网络安全事故导致的网络勒索损失，保险人和被保险人同意按照以下方式计算赔偿，但以对应的赔偿限额为限，确定赔偿金额的方法如下：

（一）保险人在**扣除每次事故免赔额或根据每次事故免赔率计算的免赔额**后，依照本

条第二款进行赔偿；

（二）每次保险事故造成的网络勒索损失，保险人在保险合同载明的网络勒索损失每次事故赔偿限额内据实赔偿；

（三）**在保险期间内，保险人对多次事故损失的累计赔偿金额不超过保单累计赔偿限额。**

第二十八条 在保险期间内，发生保险责任范围内**经政府主管部门认定的网络安全事件导致的损失，保险人和被保险人同意确定赔偿金额的方法**如下:

根据网络安全事件等级，分等级设置赔偿限额，赔付金额以各等级赔偿限额内按照实际损失赔偿，且总赔付金额以保险单载明的保险金额为限。

网络安全事件分为四级：1.特别重大网络安全事件；2.重大网络安全事件；3.较大网络安全事件；4.一般网络安全事件。

第二十九条 在保险期间内，发生保险责任范围内的网络安全事故、网络安全事件导致的其他费用损失，保险人和被保险人同意按照以下方式计算赔偿，但以对应的赔偿限额为限，确定赔偿金额的方法如下：

（一）保险人在**扣除每次事故免赔额或根据每次事故免赔率计算的免赔额**后，依照本条第二款进行赔偿；

（二）每次保险事故造成的其他费用损失，保险人在保险合同载明的其他费用损失每次事故赔偿限额内据实赔偿；

（三）**在保险期间内，保险人对多次事故损失的累计赔偿金额不超过保单累计赔偿限额。**

第三十条 保险人履行赔偿义务后，保险金额自网络安全事故发生之日起按保险人的赔偿金额相应减少，**保险人不退还保险金额减少部分的保险费。如投保人请求恢复至原保险金额，应按原约定的保险费率另行支付恢复部分从网络安全事故损失或网络安全事件损失发生之日起至保险期间届满之日止按日比例计算的保险费。**

第三十一条 保险事故发生时，如果被保险人的损失在有相同保障的其他保险项下也能够获得赔偿，保险人按照本保险合同的相应赔偿限额与其他保险合同及本保险合同相应赔偿限额总和的比例承担赔偿责任。

其他保险人应承担的赔偿金额，本保险人不负责垫付。被保险人未如实告知导致保险人多支付赔偿金的，保险人有权向被保险人追回多支付的部分。

第三十二条 发生保险责任范围内的损失，应由有关责任方负责赔偿的，保险人自向被保险人赔偿保险金之日起，在赔偿金额范围内代位行使被保险人对有关责任方请求赔偿的权利，被保险人应当向保险人提供必要的文件和所知道的有关情况。

被保险人已经从有关责任方取得赔偿的，保险人赔偿保险金时，应相应扣减被保险人已从有关责任方取得的赔偿金额。

保险事故发生后，在保险人未赔偿保险金之前，被保险人放弃对有关责任方请求赔偿权利的，保险人不承担赔偿责任；保险人向被保险人赔偿保险金后，被保险人未经保险人同意放弃对有关责任方请求赔偿权利的，该行为无效；**由于被保险人故意或者因重大过失**

致使保险人不能行使代位请求赔偿的权利的，保险人可以扣减或者要求返还相应的保险金。

争议处理和法律适用

第三十三条 因履行本保险合同发生的争议，由当事人协商解决。协商不成的，提交保险单载明的仲裁机构仲裁；保险单未载明仲裁机构且争议发生后未达成仲裁协议的，依法向保险单载明的人民法院起诉。

第三十四条 与本保险合同有关的以及履行本保险合同产生的一切争议处理适用中华人民共和国法律（不包括港、澳、台地区法律）。

其他事项

第三十五条 保险责任开始前，投保人要求解除保险合同的，**应当向保险人支付相当于保险费 5%的退保手续费**，保险人应当退还剩余部分保险费。

保险责任开始后，投保人要求解除保险合同的，自通知保险人之日起，保险合同解除。**对保险责任开始之日起至合同解除之日止期间的保险费，保险人按照《短期费率表》的短期费率计收**，并退还剩余部分保险费。

释义

第三十六条 本保险合同涉及下列术语时，适用下列释义：

（一）**网络**：指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）**计算机系统**：指由被保险人拥有、操作、管控或租赁，或由被保险人书面委托的第三方在从事各项经营活动时需要为被保险人代管的，可用于实现创建、访问、处理、保护、监视、存储、检索、显示或传输数据的计算机硬件、软件、固件、通信系统及相关电子组件、基础设施、移动设备及网络系统。

（三）**网络安全事故**：指由于下列情形未能采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性，导致服务中断、数据丢失或信息泄露：

1.恶意软件或恶意攻击行为，其中，恶意软件指可能破坏、损害、阻止访问或以其他方式破坏软件或计算机系统的操作或其中数据的恶意程序、文件或指令，包括但不限于恶意代码、勒索软件、电脑病毒、特洛伊木马、逻辑炸弹或时间炸弹等；

2.黑客行为：以创建、删除、抹去、收集、破坏、泄露、中断或损坏被保险人数据或服务为目的，恶意进入被保险人计算机系统的行为；

3.拒绝服务攻击：恶意导致被保险人计算机系统暂时性地完全或部分无法提供服务，但不包括改动或毁坏被保险人的信息技术设备、通讯设备或基础设施（包括附随的软件资源）；

4.非法使用或访问：未经授权的一方进入或访问被保险人的计算机系统。

（四）**网络安全事件**：分特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

（1）符合下列情形之一的，为特别重大网络安全事件：

①重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

①重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

①重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

（4）除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

（五）**安全威胁**：指为了向被保险人索取金钱、有价证券或其它有价动产或不动产，通过（或声称将通过）当地、跨境或多国对计算机系统实施攻击的威胁或与之有关的一系列威胁。

（六）**勒索损失**：指被保险人为了终止或结束可能引致对其损害的安全威胁，按照当地法律规定，经保险人书面同意所支付的款项，包括谈判、斡旋以及危机管理的费用；或为确定安全威胁的原因所发生的调查费用。

（七）**数据**：指使得计算机和其配件可运行的任何硬件或软件上所存储、创建、使用或传输的任何信息、内容，以及在硬盘或软盘、光盘驱动器、磁带、驱动盘、蜂窝、数据处理设备、电子控制的媒体设备或其他电子备份设备中存储的任何信息、内容。**数据不构成有形财产。**

（八）**网络恐怖主义活动**：指为了政治、宗教、意识形态等目的，企图影响恐吓政府或公众，而由任何恐怖组织或代表恐怖组织的个人利用网络和计算机系统实施的、网络攻击或使用网络暴力的行为。

（九）**数据修复费用**：被保险人在保险期间或保险单载明的追溯期内因发生网络安全事

故，产生的与下述事项有关的合理、必要的费用。

1.评估数据是否能够恢复、重建或重新收集；

2.恢复、重建或重新收集数据；

3.从被保险人的计算机系统移除恶意软件或程序；

（十）硬件改善费用

发生网络安全事故后，在满足以下全部条件的前提下，被保险人安装更加安全和更高效率版本的计算机系统而发生的必要的硬件改善费用：

（1）被保险人书面申请，保险人书面同意；

（2）发生网络安全事故时，安装的相关计算机系统相较于原计算机系统的进步基于普遍技术水平进步；

（3）安装的相关计算机系统对于防止相同网络安全事故再次发生是必要的。

但支付给下列人士的费用除外：

1.被保险人的内、外部审计师；

2.被保险人的内部员工；

3.保险人的内部员工。

（十一）事故响应费用

被保险人在保险期间或保险单载明的追溯期内因保险单列明投保的保障项目发生保险事故，为避免和减少损失扩大，保险人可以指派经被保险人和保险人双方认可的第三方专业机构作为咨询顾问或事故处理专家，对被保险人提供计算机系统的事故处理、名誉恢复等应急服务及解决方案，由此产生的下列必要、合理的费用，保险人依据本保险合同约定的负责赔偿。

被保险人对被指定的专业机构开展工作应给予相应配合。如保险合同未列明第三方专业机构，保险人可以指派经保险人与被保险人双方认可的具有合法执业资格的专业机构。

1.名誉恢复公关费用

被保险人因保险事故引发负面媒体事件所直接导致自身的声誉损害，在公关期限内为恢复被保险人的声誉而聘请相关媒体提供服务的必要、合理的费用。

本保险合同所称公关期限是指保险事故引发负面媒体事件发生之日起90个（含）自然日。

此项费用不包括与保险事故无关的企业广告、传播、宣传、新闻发布活动。

2.通知费用

被保险人需要通知下列一方或多方所产生的费用：

（1）依法应通知履行个人信息保护职责的部门：1）国家网信部门；2）依法负责个人信息保护和监督管理工作的国务院有关部门；3）依法负责个人信息保护和监督管理工作的

县级以上地方人民政府有关部门。

（2）主动通知数据被不当泄露的个人或公司；

（3）聘请第三方提供通知服务（包括提供呼叫中心支持服务），以主动通知数据被不当泄露的个人或公司。

3.监测费用

被保险人因发生个人信息泄露，为用户提供信用监测、身份盗窃监测、社交媒体监测、信用冻结、欺诈预警服务或防欺诈软件等所需的必要、合理的监测费用。

（十二）**网络繁忙：**指网络和计算机系统在未受到外部影响或未发生任何故障的情况下，无法接受正常访问和服务请求，或无法以正常的响应速度提供正常的访问和服务。

（十三）**异地设备：**区别于生产中心的处于不同网络、服务器、数据库等的专属服务器或云服务器，其与生产系统应该在管理员、域名、网关等方面具有显著独立性。

（十四）**个人信息泄露：**指在网络安全事故中被保险人负责保管的非公开个人信息被盗取、丢失或未经授权披露。其中，个人信息指适用的当地法律或法规要求予以保护、以免有人未经授权地访问、获取或披露的，以及以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，包括但不限于自然人的姓名、出生日期、有效身份证件号码、个人生物识别信息、住址、电话号码等。

附录：短期费率表

保险期间	一个月	二个月	三个月	四个月	五个月	六个月	七个月	八个月	九个月	十个月	十一个月	十二个月
年费率的百分比	10	20	30	40	50	60	70	80	85	90	95	100

注：不足一个月的部分按一个月计收。