太平洋安信农业保险股份有限公司

太平洋安信农险网络安全应急响应保险（2022版）条款

总则

第一条 本保险合同由保险条款、投保单、保险单或其他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 符合下列条件的单位可以作为本保险的被保险人:

（一）计算机系统通过信息安全等级保护二级及以上测评;

（二）计算机系统经由保险公司指定的信息及网络安全服务商进行漏洞扫描，系统不存在高危漏洞。

高危漏洞是指：软件系统中存在极其严重的漏洞，这些漏洞很容易被病毒、木马、黑客等侵入，导致软件系统崩溃或者被盗取重要信息、密码等。

第三条 被保险人本人，或者对被保险人具有保险利益的其他单位和个人可以作为本保险的投保人。

保险责任

第四条 基础保险责任

在保险期间内，当被保险人计算机系统发生网络安全事件或被保险人认为其计算机系统网络存在经保险人认可的计算机网络系统风险事件，视为保险事故发生，保险人按照本保险合同约定承担下列基础保险责任:

（一）网络安全应急基础服务。经保险人和被保险人双方认可的网络安全服务商提供的网络安全服务费用，包括为客户提供网络安全应急响应服务、网络安全专项测评服务、深度漏洞扫描服务和针对网络安全事件的处置方案的费用。

（二）网络勒索费用。事先经保险人书面同意支付的情况下所发生的可直接归因于网络勒索威胁的合理且必要的费用。

（三）安全认证监测费用。保险期间开始后，为降低网络安全事件的发生，由保险人认可的网络安全服务商对被保险人的计算机系统提供安全认证监测服务费用，包括安全认证服务、基础漏洞扫描服务和网络日常监测的服务，因此而产生的相关费用，在不超过约定额度的情况下，保险人按照本保险合同约定负责赔偿。

第五条 选择保险责任

保险人提供下列可选保险责任，由投保人根据需要自行选择投保，但须缴纳相应的保险费。投保下列可选保险责任的，在保险期间内，当被保险人计算机系统发生网络安全事件，视为保险事故发生，保险人按照本合同约定承担下列选择保险责任。

（一）网络安全应急专项服务。当被保险人的计算机系统发生网络安全事件后，经保险人和被保险人双方认可的网络安全服务商提供的安全渗透测试服务、抗拒绝服务测试服务、安全众测服务、以及源代码检测服务的费用。

（二）法律费用。被保险人或其代表在对发生网络安全事件后的索赔进行诉讼或仲裁的过程中发生的应由被保险人支付的仲裁或诉讼费用以及事先经保险人书面同意支付的其他必要的、合理的费用（以下简称“法律费用”），保险人按照本保险合同约定也负责赔偿。

法律费用不包括与被保险公司的董事、高管或员工相关的薪水、工资、营运费用或福利费用。

责任免除

第六条 保险公司在下列情况不承担赔偿责任：

（一）投保人、被保险人及其雇员、代理人的故意行为、犯罪行为或重大过失行为；

（二）被保险人明知或应当知道其提供的软件存在的既有缺陷、漏洞；

（三）被保险人安装或使用的安全软件已给予必要提示或警示后，被保险人仍进行使用的；

（四）被保险人安装或使用的软件非合法渠道提供(如盗版)；

（五）被保险人更新、调整软件版本、功能导致风险实质性增加未及时通知保险人或取得其书面同意的；

（六）被保险人进行软件测试或调试期间发生的损失或责任；

（七）被保险人知道或应当知道其软件存在缺陷、漏洞后，未及时采取有效措施导致的扩大部分的损失；

（八）被保险人修复、更新软件缺陷或为修复、更新软件缺陷而采取紧急措施发生的费用；

（九）被保险人在法律上对其负有责任的某人或服务提供商导致触犯被保险人网络安全的任何实际的或声称的行为、过错、失职、疏忽或违反义务，导致的安全事件；

（十）被保险人不如实提供或伪造保险标的投保信息；

（十一）被保险人未按照保险公司要求调整保险标的系统安全策略和服务；

（十二）其他第三方已向索赔人履行部分或赔偿责任的部分；

（十三）经被保险人及其代表许可或者授权实施的行为；

（十四）任何机械或电子故障、中断或断供，而不论其如何造成，包括任何电力中断或浪涌、电压管制、停电管制、短路、超电压或电力波动，或天然气、水利、电话、电缆、卫星、电信、互联网或其中任何组件（包括硬件或软件或任何其他基础设施）断供；

（十五）政府有关部门行政命令造成的计算机系统扣押、没收、征用、国有化或损毁;

（十六）非法、未经授权或不当收集个人信息，包括使用访问记录程序或恶意代码收集个人信息;

（十七）自然灾害或意外事故;

（十八）大气、土地及水污染或其他各种污染;

（十九）战争、类似战争行为、敌对行为、军事行动、武装冲突、恐怖活动、罢工、骚乱、暴动;

（二十）核裂变、核聚变、核武器、核材料、核辐射及其他放射性污染。

第七条 下列损失、费用和责任，保险人不负责赔偿:

（一）保险生效日之前发生的网络安全事件或者网络勒索事件;

（二）任何计算机系统的正常磨损或自然损耗;

（三）罚款、罚金、惩罚性赔偿;

（四）精神损害赔偿;

（五）任何间接损失;

（六）按照本保险合同的约定应当由被保险人自行承担的免赔额（率）。

第八条 其他不属于保险责任范围内的损失、费用和责任，保险人不负责赔偿。

赔偿限额与免赔额

第九条 本保险各项赔偿限额包括网络勒索费用每次事故赔偿限额和法律费用每次事故赔偿限额，以及网络安全应急基础服务累计赔偿限额、网络安全应急专项服务累计赔偿限额、网络勒索费用累计赔偿限额、安全认证监测费用累计赔偿限额和法律费用累计赔偿限额，由投保人和保险人协商确定，并在保险合同中载明。

第十条 每次事故免赔额（率）由保险人和投保人协商确定，并在保险单中载明。

保险期间

第十一条 除另有约定外，本保险合同的保险期间为一年，以保险单中载明的起讫时间为准。

保险人义务

第十二条 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。

第十三条 保险人依据第十七条所取得的保险合同解除权，自保险人知道有解除事由之日起，超过三十日不行使而消灭。

保险人在合同订立时已经知道投保人未如实告知的情况的，保险人不得解除合同；发生保险事故的，保险人应当承担赔偿责任。

第十四条 保险人按照第二十一条的约定，认为被保险人提供的有关索赔的证明和资料不完整的，应当及时一次性通知投保人、被保险人补充提供。

第十五条 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，并将核定结果通知被保险人。情形复杂的，保险人在收到被保险人的赔偿请求后三十日内未能核定保险责任的，保险人与被保险人根据实际情形商议合理期间，保险人在商定的期间内作出核定结果并通知被保险人。对属于保险责任的，在与被保险人达成有关赔偿金额的协议后十日内，履行赔偿义务。

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。

第十六条 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

第十七条 订立保险合同，保险人就保险标的或者被保险人的有关情况提出询问的，投保人应当如实告知。

投保人故意或者因重大过失未履行如实告知义务，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，保险人对于保险合同解除前发生的保险事故，不承担赔偿责任，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，保险人对于保险合同解除前发生的保险事故，不承担赔偿责任，但应当退还保险费。

第十八条 投保人应在保险合同成立时交清保险费。

第十九条 在保险期间内，如发生被保险人的等级保护降级或其他导致保险标的危险程度显著增加的情形，被保险人应及时书面通知保险人，保险人有权要求增加保险费或者解除保险合同。

被保险人未履行通知义务，因保险标的危险程度显著增加而发生的保险事故，保险人不承担赔偿责任。

本条第一款所称的危险程度显著增加是指与保险人承担的保险责任有密切关系的因素和投保时相比，发生了足以影响保险人决定是否继续承保或是否增加保险费的情况。

第二十条 保险事故发生时，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，**否则，对因此扩大的损失，保险人不承担赔偿责任；**

（二）立即通知保险人，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；

（三）允许并且协助保险人进行事故调查；**对于拒绝或者妨碍保险人进行事故调查导致不能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。**

第二十一条 被保险人向保险人请求赔偿时，应提交如下单证资料：

（一）保险单正本；

（二）网络安全事件或网络勒索事件证明材料；

（三）出险/索赔通知书；

（四）相关费用票据；

（五）经判决、仲裁或行政调解的，应提供判决文书或仲裁裁决文书或调解文书；

（六）投保人、被保险人所能提供的其他与确认保险事故的性质、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单证提供义务，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，被保险人应行使或保留向该责任方请求赔偿的权利。

保险事故发生后，保险人未履行赔偿义务之前，被保险人放弃对有关责任方请求赔偿的权利的，保险人不承担赔偿责任。

保险人向被保险人赔偿保险金后，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，被保险人未经保险人同意放弃对有关责任方请求赔偿的权利的，该行为无效。

在保险人向有关责任方行使代位请求赔偿权利时，被保险人应当向保险人提供必要的文件和其所知道的有关情况。

由于被保险人的故意或者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赔偿金额。

赔偿处理

第二十三条 保险人对多次安全认证监测费用的累计赔偿金额不超过安全认证监测费用累计赔偿限额。

第二十四条 当被保险人的计算机系统发生网络安全事件，保险人按以下方式计算赔偿：

在保险期间内，保险人对多次网络安全应急基础服务的累计赔偿金额不超过网络安全应急基础服务累计赔偿限额；保险人对多次网络安全应急专项服务的累计赔偿金额不超过网络安全应急专项服务累计赔偿限额。

若同时发生保险责任范围内的网络勒索事件或法律事件，保险人按以下方式计算赔偿：

（一）**保险人在扣除每次事故免赔额（率）后，**依照本条第（二）项计算赔偿；

（二）对于每次事故的网络勒索费用，保险人在每次事故网络勒索费用赔偿限额内赔偿；对于每次事故的法律费用，保险人在每次事故法律费用赔偿限额内赔偿；

（三）在保险期间内，保险人对多次事故网络勒索费用的累计赔偿金额不超过网络勒索费用累计赔偿限额；保险人对多次事故法律费用的累计赔偿金额不超过法律费用累计赔偿限额。

第二十五条 发生保险事故时，如果存在重复保险，**则本保险人按照本保险合同的赔偿限额与所有有关保险合同的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。**

被保险人在请求赔偿时应当如实向保险人说明与本保险合同保险责任有关的其他保险合同的情况。**对未如实说明导致保险人多支付保险金的，保险人有权向被保险人追回多支付的部分。**

第二十六条 被保险人向保险人请求赔偿的诉讼时效适用于现行有效法律规定。

争议处理

第二十七条 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，依法向中华人民共和国人民法院起诉。

第二十八条 本保险合同的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

第二十九条 保险责任开始前，投保人要求解除合同的，保险人按照合同约定退还全部保险费。

保险责任开始后，**投保人未向保险人报案或索赔、未开始接受各项网络安全服务的方可退保。**投保人要求解除合同的，**可提前十五日向投保人发出解约通知书，保险人按照保险责任开始之日起至合同解除之日止期间与保险期间的日比例计收保险费，并退还剩余部分保险费。**

在本保险合同成立后，投保人可以书面形式通知保险人解除合同，但保险人已根据本保险合同约定给付保险金的除外。

投保人解除本保险合同时，应提供下列证明文件和资料：

（1）保险合同解除申请书;

（2）保险单原件;

（3）保险费缴付凭证;

（4）投保人有效身份证件。

投保人要求解除本保险合同，自保险人接到保险合同解除申请书之时起，本保险合同的效力终止。

第三十条 保险期间不足一年的，保险人将按照附表一《短期费率表》所列标准收取保险费。

释义

【网络安全事件】是指在保险期间内，被保险人的 IT 资产（包含 WEB 服务器、应用服务器、数据库系统、操作系统、网络设备、应用系统、应用中间件、固件）在运营期，被蓄意攻击，导致服务不可用、未经授权访问、未经授权使用、企业数据盗窃、企业数据丢失、用户隐私信息泄露曝光等。

【安全应急响应服务】当投保的联网计算机系统受到来自外部人员（不包括投保的联网计算机系统所属单位人员）攻击导致计算机系统不能正常运行和使用时，根据保险合同约定制定一整套合理的安全事件应急响应预案，依据预案来处理发生的各类安全事件。

【网络安全专项测评服务】针对投保的联网计算机系统进行专项安全检测，检测内容包括网络安全、主机安全、应用安全、数据安全及备份恢复和特殊指标安全等服务。

【深度漏洞扫描服务】针对投保的联网计算机系统进行全面深度漏洞扫描服务，深度漏洞扫描覆盖的内容包括：OWASP TOP10 漏洞、WEB 扫描覆盖安全测试检查、主机扫描覆盖安全测试检查。

【网络勒索威胁】指投保的联网计算机系统受到来自外部人员（不包括投保的联网计算机系统所属单位人员）攻击导致计算机系统不能正常运行和使用，同时攻击者利用此类攻击来勒索威胁达到相应的目的。

针对网络勒索威胁提供安全应急响应服务恢复网站正常运行和使用，另外提供技术支持协助被保险人获取攻击相关信息，以便被保险人采取相关法律手段应对攻击者。

【安全认证服务】通过对网站开展的安全服务工作的深度和广度等审核认定，对网站的安全等级状态进行标识，颁布公安部第三研究所（国家网络与信息系统安全产品质量监督检验中心）安全认证标识服务，从而明确网站的真实性和安全现状，体现网站运营者采取的具体安全服务和措施，提升网站的可信任程度，增强网站使用者的访问信心。

【网络日常监测服务】针对指投保的联网计算机系统进行监控，当网站发生故障时能及时告警，并以邮件，短信，电话的方式通知被保险人的指定人员。网站日常监控服务内容包括：网站状态监控，服务端口监控，DNS 劫持监控，网站

挂马监控，疑似篡改监控，关键内容监控，敏感字监控，钓鱼网站监控。

【安全渗透测试服务】采用完全模拟入侵者可能采用的攻击技术和漏洞发现技术，利用专家经验对投保的联网计算机系统进行非破坏性质的模拟攻击，发现系统最脆弱环节和弱点等安全问题，为进一步加固计算机系统提供了依据。

【抗拒绝服务测试服务】针对投保的联网计算机系统的并发连接数、网站响应时间、点击率、网站吞吐量进行压力测试，发现网站的安全瓶颈，提出安全解决方案。

【安全众测服务】公安三所信安在线平台认可的国内顶级团队参与投保客户网站的安全测试，全程引入高私密性的保护和风险控制机制，提升客户网站的安全防护能力。

【源代码检测服务】通过对源代码安全测试，降低源代码出现的安全风险，构建安全代码，提高源代码可靠性，提高应用系统自身 安全防护能力，帮助开发人员提高源代码质量，从底层保障应用系统本身的安全，从早期降低应用系统的安全维护成本。

附表一:《短期费率表》

保险期间（月）	1	2	3	4	5	6	7	8	9	10	11	12
短期费率百分比（%）	20	30	40	50	60	70	75	80	85	90	95	100

注：保险期间不足 1 个月的，按 1 个月计算；保险期间在 1 个月以上，不足 2 个月的，按 2 个月计算；保险期间在 2 个月以上，不足 3 个月的，按 3 个月计算，依此类推。