中国太平洋财产保险公司厦门分公司文件

厦太保产发〔2023〕9号

关于印发《中国太平洋产险厦门分公司数据防泄漏管理细则》的通知

各机构、各部（室）：

为加强分公司数据防泄漏管理体系建设，有效降低分公司保密电子数据外泄风险，经研究，分公司制定《太平洋产险厦门分公司数据防泄漏管理实施细则》。现予以印发，请认真学习并遵照执行。

特此通知。

中国太平洋保险股份有限公司

厦门分公司

2023年2月23日

太平洋产险厦门分公司数据防泄漏管理实施细则

第一章　总则

第一条　为加强分公司数据防泄漏管控体系建设，有效降低保密电子数据（以下简称为“保密数据”）外泄风险，根据集团关于印发《中国太平洋保险（集团）股份有限公司数据防泄漏管理办》的通知（太保产发〔2022〕105号）文件要求，结合分公司实际特制定本细则。

第二条　本细则适用于分公司所辖各单位。

第二章　数据防泄漏的管控目标和原则

第三条　数据防泄漏的目标，是通过技术或管理手段，防止保密数据被有意或无意的外泄。

第四条　保密数据的定级依据《中国太平洋保险（集团）股份有限分公司保密工作规定》（太保发〔2018〕106号）中分公司商业秘密分级标准，分为两个安全等级：

（一）重要商业秘密数据

对应分公司商业秘密“重要商业秘密”等级，是指具有重大商业价值，并直接影响企业竞争力和正常运营的数据，一旦泄密，会给分公司带来较大经济损失，严重影响分公司运转，必须予以特别保护。

（二）一般商业秘密数据

对应分公司商业秘密“一般商业秘密”等级，是指对竞争对手有价值的数据，泄密后会给分公司造成一定的经济损失，但不会严重影响分公司正常运转。

第五条　数据防泄漏管控原则建立在保密数据安全等级的基础上。重要商业秘密数据严格控制，原则上优先选择阻断控制方式；一般商业秘密数据适度控制，原则上优先选择告警控制方式，必要时选择阻断控制方式。

第六条　重要商业秘密数据和一般商业秘密数据以外的电子数据也可根据业务需要申请作为其他保密数据纳入数据防泄漏保护。

第七条　数据防泄漏的管控范围是保存在PC终端和移动终端上的分公司数据。

第三章　数据防泄漏基准策略

第八条　分公司内部产生的各类数据，数据归属部门承担数据管理职能，按照分公司数据防泄漏基准策略（见附件）定义数据防泄漏需求。

第九条　数据防泄漏基准策略是对分公司不同安全等级的数据对象在各个外发传输渠道所采用的控制方式进行定义的集合，以实现数据防泄漏的目标。

第十条　数据防泄漏基准策略由三部分组成：数据保护对象、传输渠道和控制方式。

（一）数据保护对象：指分公司保密电子数据，包括重要商业秘密数据、一般商业秘密数据，以及其他保密数据。

（二）传输渠道：指可以将数据传输至分公司外部网络或人员的网络通信协议或应用程序。常见传输渠道包括：

1、分公司邮件：通过分公司邮件向外部邮件地址发送信息或文件；

2、Internet访问：通过分公司提供的Internet链路，向互联网上的BBS、微博、Webmail、文库等发布信息或上传文档；

3、打印：通过打印，将电子文件转化为纸质文件，传递给他人或带离分公司；

4、移动存储介质：将电子文件拷贝到移动存储介质，传递给他人或带离分公司；

5、移动智能终端：通过移动智能终端上运行的分公司E端应用（如手机邮箱、太保E办等）外发数据；

6、其他传输渠道，如电子传真、FTP、文件共享、即时通信软件、网盘等。

（三）控制方式：指数据防泄漏系统平台在监测到被保护数据对象通过传输渠道从事传输行为时的响应动作。

1、日志审计：数据防泄漏系统平台在监测到被保护数据对象的传输行为时进行后台日志记录，采用事后审计的方式发现数据外泄行为。

2、告警：通过告警方式提醒用户当前的行为可能导致数据外泄并进行日志记录，以警示的方式提高用户的安全意识。

3、阻断：通过终止用户当前的文件使用和外发行为，阻止违反分公司策略的数据外泄事件的发生，告知用户并进行日志记录针

对PC端的外发行为阻断并提示；针对移动端分公司E端应用的外发行为采用禁止截屏、禁止对外分享或审计等措施。

第十一条　数据防泄漏基准策略在定义时，应遵循以下原则：

（一）只能选择与数据防泄漏管控原则相同的或更为严格的控制方式；

（二）对于同一类保护数据对象，应在不同的传输渠道采用统一的控制方式；

（三）对于存储在数据库中的数据，应明确定义需要保护的数据字段名称。

第四章　职责与分工

第十二条　信息技术部主要承担以下职责：

（一）负责数据防泄漏例外权限的申请，例外权限人员离职、调岗或权限到期等应及时联系太保科技关闭权限申请；

（二）负责回顾例外岗位人员清单；

第十三条　各部门主要承担以下职责：

（一）严格控制例外岗位数量，加强对本部门数据防泄漏例外申请的明确性、合理性和完整性审核；

第五章　数据防泄漏例外管理

第十四条　因工作需要外发保密数据的岗位人员可以申请例外权限，例外权限人员在规定范围内的保密数据外发行为将不被阻断，同时将被日志记录。

第十五条　数据防泄漏例外权限分为两种：

（一）长期例外权限：员工因工作岗位需要，向监管机构或合作伙伴（如人民银行、银保监、审计机构等）发送保密数据，可申请长期例外权限；

（二）临时例外权限：员工因临时工作需要，向监管机构或合作伙伴（如人民银行、银保监、审计机构等）发送保密数据，或分公司设备间临时数据转移，可申请临时例外权限。申请时需明确例外有效时间，最长不超过7天，到期及时关闭。

第十六条　申请例外权限应按照流程，由申请人提出申请，经部门负责人-信息技术部负责人-总经理室审批通过后提交至太保科技设置权限。

第六章　数据防泄漏事件管理

第十七条　各部门应对数据防泄漏平台事件清单进行自查审核，如发现数据泄漏或存在违反本细则的情况，应及时向分公司信息技术部报告。

第十八条　分公司的数据防泄漏事件管理参照公司要求执行，由信息技术部按需统计数据防泄漏事件，提交各部门及辖内单位自查审核。一旦发现数据泄漏事件，应及时向其信息技术部报告。

第十九条　数据防泄漏事件日志需保存至少1年。

第七章　附则

第二十条　如发生数据泄漏事件，按照《太平洋产险厦门分公司员工奖惩管理规定》对违规行为的相关责任人实施责任追究。

第二十一条　本细则由信息技术部负责解释。

第二十二条　本细则自印发之日起施行。

附件：数据防泄漏基准策略

中国太平洋财产保险公司 厦门分公司办公室	2023年2月23日印发
编录：曾秀玲	校对：邱丹丹