数盾风险处理及审计大纲

1. 风险分类及概述

集团在《阿里巴巴集团数据安全规范（总纲）》对数据生命周期（数据生产、数据存储数据使用、数据传输、数据传播、数据销毁）各环节提出了数据安全管理要求，数盾产品在基于数据安全管理需求，会识别并推送员工不符合数据安全大纲的行为，主要包含如下几类：

1.1 数据不当存储

公司的敏感数据仅允许存储在集团的内部应用、云存储或配发的终端计算机设备中，禁止存储在外部存储应用中（如百度云盘、印象笔记等），禁止存储在个人移动存储设备中。因电脑故障或更换电脑而需使用移动存储备份数据，需要向 IT 服务台报备后使用，并遵守使用要求。

故当员工有如上操作而未进行相关报备时，数盾产品会识别并推送该类风险，风险中会明确提供员工通过何种渠道进行传输具体的文件明细。具体风险类型包含：终端操作（USB 拷贝等），钉盘下载（钉盘下载到非办公设备），文件上传到外部网盘（如百度云盘）等

1.2 数据不当传输

员工无论通过集团的官方途径，或于与朋友沟通、跟商户交流或其他方法直接或者间接把数据对外披露，均需遵守数据对外披露的规定，无业务场景下，员工不允许将公司相关业务数据进行披露。对外数据披露指把数据披露给第三方，即集团以外的任何个人、法人、公司、企业、政府部门或其他法律实体或组织。

故当员工通过邮箱或其他方式外发给到非公司相关业务人员时，数盾产品会识别并推送该类风险，具体风险类型包含： 云邮箱文件外发等。

1.3 数据不当使用

员工不得利用工作权限查询与工作无关的信息，数据按需申请，秉承最小够用原则，谁用谁申请。

故当员工未经报备查询进行查询敏感信息时，数盾产品会识别并推送该类风险，具体风险类型包含：定向查询。

1.4 其他风险操作

公司规定公司账号、权限不可互借且系统账号/密码不可在任何地方明文存储或展示，故数盾同样会推出账号借用、账号/密码外泄等风险事件。

2. 风险角色及协查流程

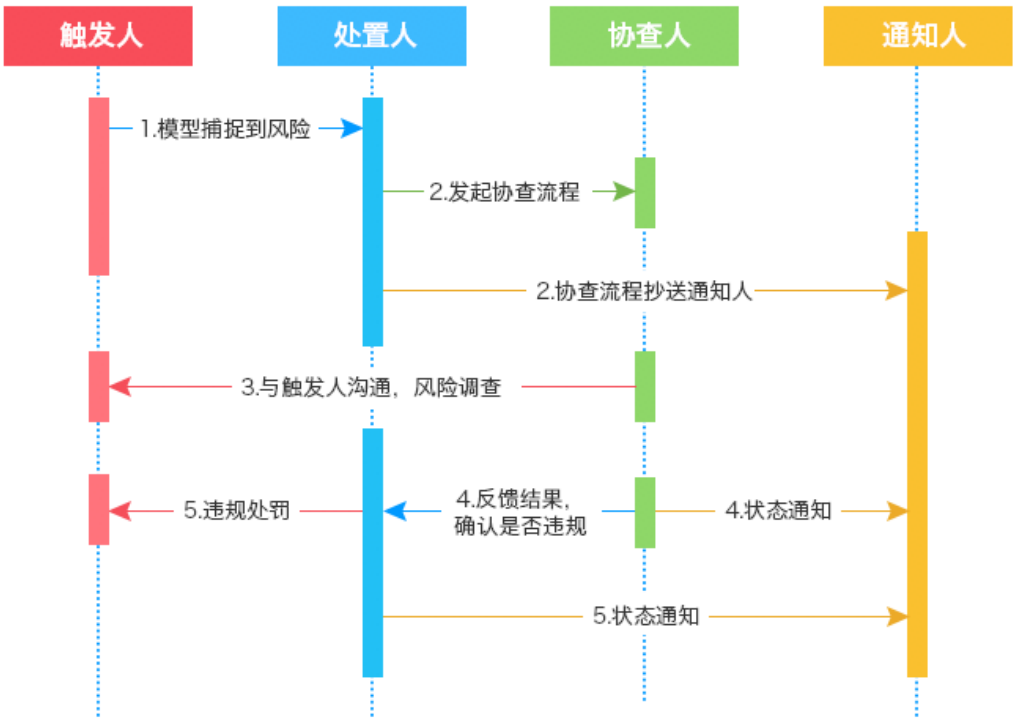
2.1 风险角色

集团或者 BU 的安全运营同学（风险处置人）通过数盾运营平台进行风险管理，新风险产生后处置人通过平台将风险信息推送给风险触发人主管或者上级（风险协查人）进行协助调查，届时协查人将同时收到风险提示邮件和对应的阿里内外工作流通知。风险协查人需帮助核实并在 3 天以内反馈结果，以便尽早控制数据安全风险隐患。

角色	说明
风险触发人	触发数据安全风险的员工
风险处置人	在数盾上认领风险并推送给到相关协查人，一般是安全运营，BU 内控或部门数据安全接口人

风险协查人	由风险处置人指定的，协助调查风险的人员，多为员工的主管，HRG 及数据安全接口人，负责调查员工行为及数据泄露情况，返回影响面、违规等级及处罚结果
风险通知人	由风险处置人指定的，接收风险处置进展更新的人员。

2.2 协查流程



3. 风险结果返回及违规定级

风险协查人（风险触发人主管、HRG 及部门数据安全接口人）基于数据等级、数据泄露情况、业务影响及结合员工是否有合理场景进行综合判定，返回最终处罚结果，同时将相关信息在数盾上进行沉淀记录。BU 可基于违规等级及事件情况进行升级处罚。

3.1 数据分类及分级

3.1.1 数据分类

客户数据 (简称 C)

客户的数据：客户的基本信息和客户提供给集团使用的数据；

如：例如个人信息（姓名、生日、出生地、信用卡号、身份证号等）、商品详情、交易评价等用户输入数据。

业务数据(简称 S)

业务数据：集团业务开展所需要的数据；

例如客户的行为数据、根据客户数据和客户行为数据加工获得的数据（例如 GMV、PV、类目、商品属性等）。

公司数据(简称 B)

a.公司的财务数据、管理数据及运营数据（如：业务规划、分析报告、未申请专利的发明创造、尚未公布的并购计划和财务报告、法律文件及员工个人数据等）；

b.集团的服务、内部系统、软件等产生的数据，各种系统的账户和密码；

c.集团员工在所有的工作中产生的数据，包含但不限于：和工作相关的数据，如源代码（含工作中产生的程序代码）、操作记录、crm 小记、项目文档（含产品设计图、改版设计图）等；

d.以及由上述数据衍生的所有数据或文档。

3.1.2 数据分级

默认的信息安全级别：任何没有标识的信息，客户信息默认为：客户隐私信息（默认 C3)；

业务信息默认为：业务保密信息(默认 S3)； 公司信息默认为：公司内部信息(默认 B2)

具体数据分类分级可参考：

https://meta.dw.alibaba-inc.com/old/portal/secret_level.html?spm=0.0.0.0.LZvqUY

3.2 违规行为的定义

一类违规行为：

1. 以谋利为目的，获取、使用、泄露、传播、出售任何敏感数据或试图从事此行为的，均需定义为一类违规行为。
2. 违反数据安全大纲，造成（1）P1 级生产事故，（2）L4 级数据泄露，（3）造成 L2 或 L3 级数据泄露并造成经济损失或声誉损失，（4）以不正当手段获取、使用 L4 数据。

二类违规行为:

1. 未经授权获取、使用、泄露、传播敏感数据，或未妥善保存数据，引发泄露风险
2. 违反数据安全大纲，造成（1）P2 级生产事故，（2）造成 L2 或 L3 数据泄露，（3）以不正当手段获取、使用 L2 或 L3 数据

三类违规行为：

违反数据安全操作规范要求，引发影响日常工作运行的风险。

3.3 集团建议及历史违规 case

违规定责依据：以风险场景+数据等级为基础判据，基于数据量级、风险行为次数、泄露影响等确定最终违规等级， 最终违规等级低于基础判据时需要走审批流。

a. 有合理场景但未进行报备：审批流：主管---HR---数据安全接口人---集团数据安全内部风险治理小二

b. 无合理场景：审批流：主管---HR---数据安全接口人---BU owner

集团建议的基于风险场景及数据等级的基础判据表：

场景	**数据最高等级**	**建议违规等级**
文件外发 （对象：非公司员工，移动硬盘，非办公设备，员工自己的微信/QQ 号，微信/QQ 等文件小助手等）	L2	三类及以上
	L3	二类及以上
	L4	一类
定向查询字段等级	L2	三类及以上
	L3	二类及以上
	L4	一类
员工信息查询（查询手机号）	L3	二类及以上
员工信息查询（查询组织架构）	L2	三类及以上
外部开源网站代码泄露	/	三类及以上
内部账密泄露（账号：如员工账密，阿里云的 AK 账密等）	/	三类及以上

历史违规 case 参考

一类违规 case 举例：

事件描述： 邱某在待离职期间通过私人电脑下载、手机拍照等方式违规获取的公司工作文档总数超 500 个，其中包含保密数据（L3）和机密数据（L4），其目的是在以后工作使用，目前数据已在其主管和安全团队的监督下删除，该行为违反了数据安全规范制度中离职前不

得将工作文档带离公司的规定，处以一类违规。

评估标准：数据等级（L4）+业务影响

事件描述：张某将接近 1000 条非公开客户信息（含手机号码）进行外传，给业务带来极大风险，给予一类违规，辞退且永不录用。

评估标准：数据等级（L3）+业务影响

二类违规 case 举例：

事件描述 姜某在没有提交申请和报备的情况下 ,擅自拷备 L3 等级的保密数据和信息资料，违反数据安全制度中禁止将工作文档存储在个人移动存储设备的规定，带来数据泄露风险，处以二类违规。

评估标准：数据等级（含 L3）+业务影响

事件描述：任某在待离职期间通过微信发送工作文档，其中包含公司保密数据（L3），相关文件在监督下已删除，行为违反数据安全规范制度中不得将工作文档带离公司的规定，处以二类违规。

评估标准：数据等级（含 L3）+业务影响

三类违规 case 举例：

事件描述：程某通过微信从 PC 端将部分 L2 级公司内部数据发送到个人手机微信中，违反了数据安全规章制度中不得使用非公司产品传输和讨论工作内容的规定，处以三类违规。

评估标准：数据等级（含 L2）+业务影响

事件描述：丁某在无业务场景的情况下使用 CRM 查询自己亲属的收货地址，违反数据安全规范制度中非业务场景下不得查询客户个人信息的规定，处以三类违规。

评估标准： 数据等级（L3）+业务影响

事件描述：邹某将内部配置信息和代码上传到外部开源代码库 Github 上，虽然此次事件上传信息为测试环境并需要内网链接，未完成实际上传动作和造成实质的信息泄露，但此行为已经违反了数据安全规范制度中不得将工作文档上传至外部网盘或开源代码库的规定，处以三类违规。

评估标准：数据等级（L3）+业务影响

更多历史违规 case 详见：http://df.alibaba-inc.com/#/df/violationOfPublicity

附件：

数据分类分级：

https://meta.dw.alibaba-inc.com/old/portal/secret_level.html?spm=0.0.0.0.LZvqUY

阿里巴巴集团数据安全规范（总纲）

http://df.alibaba-inc.com/?spm=a1z2e.8101737.webpage.dtitle3.30916a6cK6KPnu#/df/lawsAndRegulations/detail?type=REGULATIONS&id=192