**日志安全建议规范**

安全人员在日志审核工作中发现部分厂商日志含有异常数据，为防止数据的泄露，对于日志规范提出以下原则：

1. 在日志中不能包含二级或三级敏感度的信息，厂商日志中只输出报错信息和运行信息；
2. 第二，禁止在日志中出现明文用户名、口令等敏感配置信息。

请存在问题的厂家尽快将代码修改完成，交由测试组测试，测试通过后允许厂家提取日志。

厂商申请提取日志，请产品运营同事向平台部门提出申请提取日志，不需要经过安全部门审批，但安全人员会定期对日志进行审计，建议日志保留一个月以上时间，一旦发现日志存在问题，安全部门有权暂时停止提取日志的工作，根据审计的结果做相应的操作（如流程图所示）。

一级信息：主要包含用户的消费信息与业务/合作信息；

二级信息：主要包含用户的身份信息，如用户姓名、证件号码、地址信息、银行账号信息等；

三级信息：主要包含用户通信信息，如用户通信详单、定位（位置）信息、用户身份鉴权信息等。（关联了用户真实身份之后是敏感信息）

特定信息：此外还须考虑云公司与某些数据提供方签署的数据安全保密协议（合同）中有关数据保存、应用、合作提供过程中的保证性要求和限定条款。这类数据应单独按要求分级管理。这类信息也会包含了二、三级的数据管理要求。

