灵析安全策略说明书

引言

灵析以打造 NPO 领域最佳 IT 服务商为使命，借助现在云计算以及 WEB 技术的发展，通过 SAAS 方式为基金会、公益组织提供筹款、传播、数据分析、利益相关方（捐赠人，志愿者等）、数据管理的多方位服务。截止到 2018 年，灵析累计为超过 50000 多家机构与组织提供服务，管理数百万的联系人。灵析团队在保证系统高效，稳定运行，功能迭代，用户体验提升的同时，“安全”从系统开发初始的架构到每个环节，都是首要和关键组件。本文将介绍灵析在安全方面采用的方法，包括安全策略，物理安全，软件安全，组织安全等。当然，随着时间推移，安全策略会随着技术革新和服务创新而改变。

一．基础安全策略

灵析是一款 SAAS 产品，安全策略的目标是保证用户数据的保密性，完整性，可用性。保密性是通过技术手段和规章制度防范数据泄露和篡改；完整性是确保用户数据不丢失，误操作后可恢复；可用性是确保用户随时随地可以读取、修改、拿走自己的数据。

在实际工作中的任何时间，一旦有安全隐患，灵析团队会第一时间响应（常规响应时间小于 15 分钟），永远把安全放到第一位。

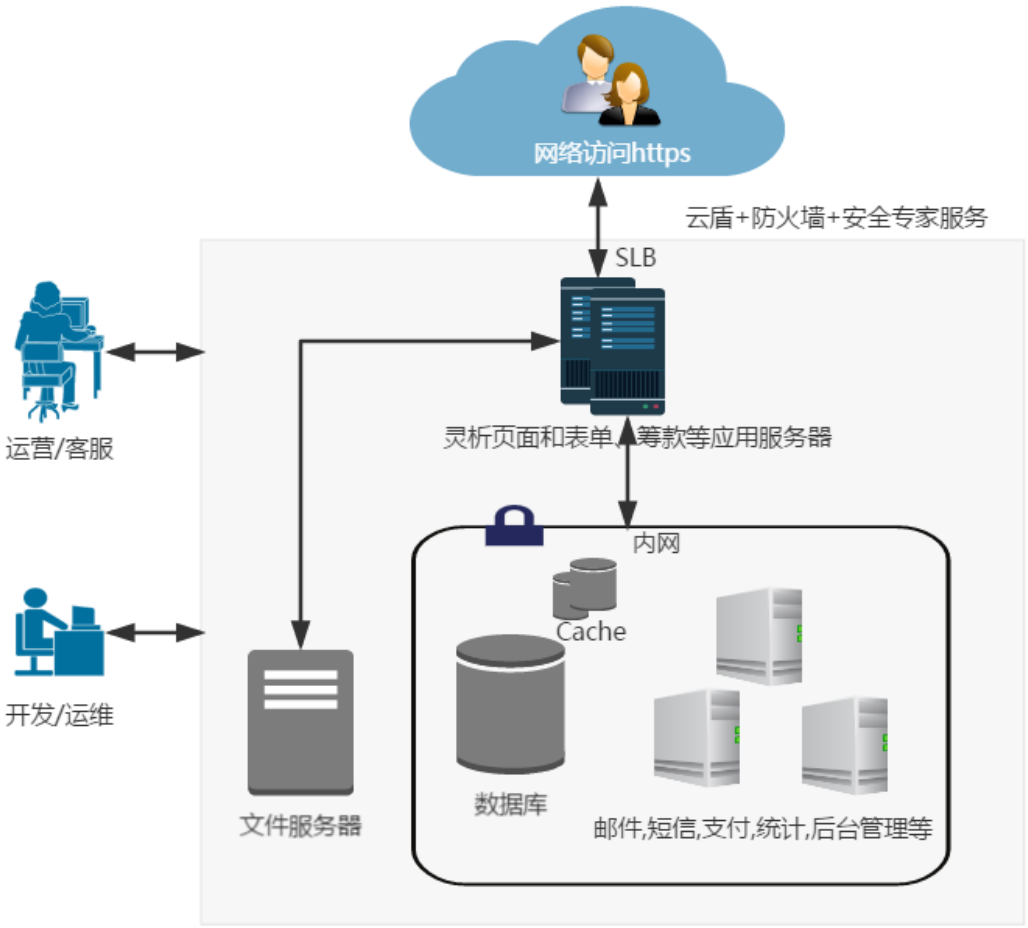
二．物理安全

灵析在硬件上采用阿里云产品（https://www.aliyun.com），包括但不限于：服务器 ECS，数据库 RDS，对象存储 OSS，负载均衡 SLB，消息队列 MQS，数据缓存，云盾（包括专家服务），云安全等。阿里云以阿里巴巴公司的多年技术为沉淀,在物理硬件架构的分

布式部署和存储、WEB 安全防范和容灾等安全方面上已经构建了坚实的基础，从这方面来考虑，我们选择与阿里云合作，而不是自建服务器。下面两个链接说明了目前阿里云在安全方面的保障：

1. 安全解决方案：https://www.aliyun.com/solution/security
2. 阿里云安全白皮书：https://help.aliyun.com/knowledge_detail/5975221.html

下面是灵析采用阿里云产品后整体网络拓扑结构图：



三．软件安全

灵析所有对外的页面请求都采用 https 方式，以确保数据传输安全。对外业务分三种，

灵析业务本身、表单/筹款、还有 API 接口（对应上图中网络访问 HTTPS）。对于灵析业务本身，所有操作需要强制登陆后才可以进行，且只能访问、操作自己相关的数据，表单筹款对外页面是放开对外访问的，二者安全重点有所侧重，但具体策略本质是一样的，包括但不限于以下：

- 全程 HTTPS 请求
- 需要登录的页面：
    - 登录验证码三次尝试登录后自动启用
    - 强制密码需要保证数字大小写混合，双层 md5+salt 存储，对于初始设置的弱密码，每次登陆都提示用户修改
- 所有的展示数据只能通过混淆加密 ID 去访问，比如访问联系人详情页链接：https://demo.lingxi360.com/contact/detail/LXEOBAU6U4th，访问填写表单的连接：https://f.lingxi360.com/f/k9ap2q
- 针对服务器和应用程序的每日安全漏洞扫描
- 异常请求实时告警
- 及时升级操作系统和业务框架的版本，确保安全的同时也提高效率，关注安全动态及时修复大的公共漏洞（比如 OpenSSL Heartbleed）
- 针对所有自主开发和采用的第三方软件，灵析团队在开发时随时关注但不限于如下的可能问题：https://help.aliyun.com/knowledge_list/9006066.html
- Code Review 机制，所有待提交的代码和待部署到生产环境的代码都要经过核心研发团队双重检查，从底层代码层面保证系统的安全性；
- API 访问采用 AccessKey 和 AccessSecret 安全加密对来对接口访问进行身份验证

除上面所述的对外业务部分，其它灵析服务器和数据库均限于内网访问，运维和调试时

通过阿里云管理控制台或者给核心开发运维人员临时 IP 白名单授权访问，用完后及时收回权限。

四．组织安全

组织安全主要是说灵析团队内部工作人员在访问灵析资源的权限划分以及针对员工的访问权限（访问权限及等级是基于员工工作的功能和角色，最小权限和职责分离是所有系统授权设计基本原则）。

灵析安全团队由有法律背景的 CEO 和 3 位有多年开发经验的工程师直接负责，在安全策略流程设计与执行，软硬件系统架构选型，网站安全开发和代码审核，防范攻击和入侵等方面扮演重要角色。

针对灵析员工：为了保护灵析用户和自身的数据资产安全，灵析采用一系列控制措施，以防止未经授权的访问。员工入职后，都必须签署保密协议，确认收到并遵守灵析的安全政策和保密要求，灵析要求员工以诚信，敬业的态度来管理用户资源。人力资源给每位员工根据岗位类别（主要分开发/运维、技术支持/客服、运营/传播/市场）和职位级别（总监、经理、主管、员工，实习生）分配账户和相应权限（员工离职后，人力资源将通过禁止账户访问所有灵析资源），确保员工在在访问资源时都拥有唯一的账户，并且系统会自动永久保留访问日志。

针对灵析用户：无论收费还是免费用户，灵析对所有用户在法律层面，进行数据产权与安全服务的承诺。包括：

- 双方应当对本协议的内容、因履行本协议或在本协议期间获得的或收到的对方的商务、财务、技术、产品的信息、用户资料或其他标明保密的文件或信息的内容(简称“保密资料”)保守秘密，未经信息披露方书面事先同意，不得向本协议以外的任何第三方披露。

资料接受方可仅为本协议目的向其确有知悉必要的雇员披露对方提供的保密资料，但同时须指示其雇员遵守本条规定的保密及不披露义务。

- 除非得到另一方的书面许可，甲乙双方均不得将本合同中的内容及在本合同执行过程中获得的对方的商业信息向任何第三方泄露。

- 保密义务在协议期满、解除或终止后仍然有效。

- 灵析通过阿里云服务器存储、SSL 数据加密传送以及高级密码设置等方式竭尽全力保证灵析用户在灵析中的数据的安全，如因灵析单方技术或人为原因导致乙方数据泄露，灵析将承担带来相应后果的法律责任。

以上从法律层面陈述我们对灵析数据的安全承诺，在实际使用中，我们也会给机构提供安全指导建议，以便机构更安全地使用灵析。

针对第三方软硬件系统：灵析团队在开发灵析核心业务同时，也使用多款第三方软/硬件系统，包括但不限于：企业邮箱，阿里云系列产品（服务器，数据库，存储等），邮件/短信群发服务，支付宝微信等第三方支付系统，统计系统等，每款软件的选择我们都确保该软件在其服务领域的影响力和首要地位，他们也是灵析安全的重要保障之一。针对这些第三方软件的账户密码，我们都以对方的最高标准执行，包括但不限于：高强度密码且定期更新；手机校验登录；面向灵析员工职责设置不同资源访问权限；禁止员工在公共电脑上登录第三方系统；最高管理员（公司创始人）随时可监督员工访问日志；调用第三方数据自己都留有备份等；所有以上这些措施都为了确保我们在第三方软件自身安全的基础上，我们可以安全使用。

五．总结

灵析目前是一个快速迭代更新的产品，团队也在快速成长。但无论何时，保证安全永远

是灵析团队的首要任务。随着时间推移，安全策略会随着技术革新和服务创新而改变，团队会不遗余力继续加大投入，让用户放心使用灵析。

佳信德润（北京）科技有限公司

附件一： ISO27001 认证

Certificate of
Management System Certification

This is to certify the information security management system of

JUSTERING (BEIJING) TECHNOLOGY CO., LTD.

Unified Social Credit Code:91110114587705260 9

REGISTRATION ADDRESS: ROOM 101, NO. 12, TAIHU ROAD, SHISANLING TOWN, CHANGPING DISTRICT, BEIJING P.C.:102200

MANAGEMENT ADDRESS: 801/809, BLOCK A, OCEAN EXPRESS APARTMENT, DONGSANHUAN NORTH RD, CHAOYANG DISTRICT, BEIJING P.C.:100027

Is in conformity with

GB/T 22080-2016/ISO/IEC 27001:2013

This certificate covers the following area

(Applicability statement version: A/0)

LOCATED AT 801/809, BLOCK A, OCEAN EXPRESS APARTMENT, DONGSANHUAN NORTH RD, CHAOYANG DISTRICT, BEIJING ENGAGED IN AND LINGXI WISDOM AND PUBLIC WELFARE SOFTWARE DEVELOPMENT AND SERVICE RELATED INFORMATION SECURITY MANAGEMENT ACTIVITIES

Initial Certification Date: FEB.08,2018 **Issue Date: From FEB.08,2018**

Validity Period: From FEB.08,2018 To FEB.07,2021

Certificate No.: 04518120007R0S **Signer:** 韩海华

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C045-M

Certified client shall receive at least one surveillance audit every year within the validity period, the certificate shall only be valid when used in conjunction with the Notice Letter of Annual Surveillance Certification Decision. Information on this certificate could be verified on the official website of Certification and Accreditation Administration of the People's Republic of China (www.cnca.gov.cn) and www.cnas.org.cn and www.hxqc.cn

Beijing Daluhangxing Quality Certification Center Co., Ltd.

Address: No. Jia 12, Yuquan road, Haidian district, Beijing, P.R. China P.C.: 100143

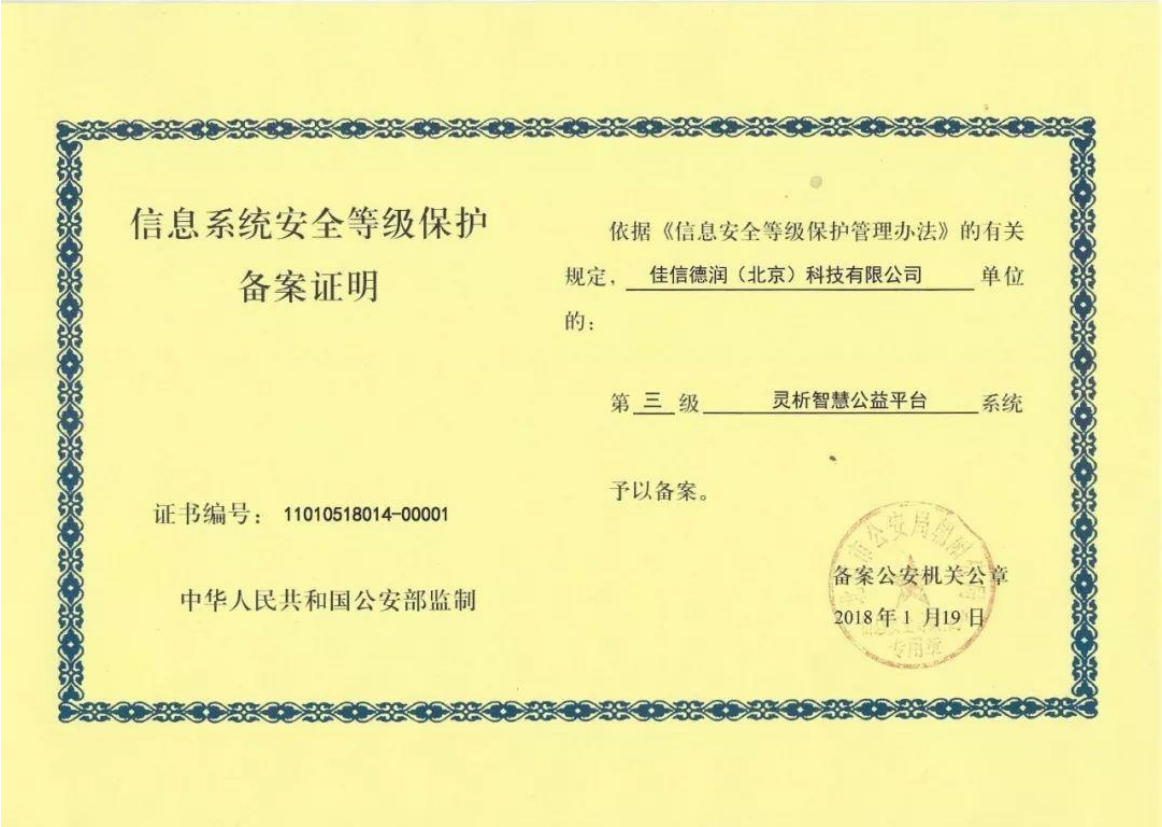
ISO27001 认证——信息安全管理体系(ISO27001 Information security management system)是国际公认解决信息安全认证体系。由 1998 年英国发起的信息安全管理体系制定

信息安全管理方针和策略，采用风险管理的方法进行信息安全管理计划、实施、评审检查、改进的信息安全管理执行的工作体系。

灵析正式通过 BSI 国际权威审核认证，获颁 ISO 27001(信息安全管理体系标准)认证证书。

此次通过国际信息安全认证，意味着灵析将信息安全管理标准提升到更高水平，实现国际接轨。

附件二：信息系统安全等级保护三级认证



信息系统安全等级保护

备案证明

依据《信息安全等级保护管理办法》的有关规定，佳信德润（北京）科技有限公司 单位的：

第 三 级 灵析智慧公益平台 系统

予以备案。

证书编号： 11010518014-00001

中华人民共和国公安部监制

备案公安机关公章

2018 年 1 月19 日

信息系统安全等级保护是国家信息安全保障的国家级标准。由公安机关依据国家信息安全保护条例及相关制度规定，按照管理规范和技术标准，对机构的信息系统安全等级保护状况进行认可及评定。

等保三级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统，是国家对非银行机构的，最高级信息安全登记保护认证。也是互联网公开募捐信息平台申请的必备技术标准。灵析经过第三方机构测评，满足等级保护三级对应的安全指标要求。