法大大信息安全白皮书

2024 年 01 月

法律声明

版权声明

©2024 深圳法大大网络科技有限公司。版权所有

在未经深圳法大大网络科技有限公司（下称"法大大"）事先书面许可的情况下，任何单位（组织）及个人不能以任何形式复制、传递、分发或存储本文档中的任何内容。

本文档描述的产品中，可能包含法大大及第三方享有版权的软件。除非获得相关权利人的许可，否则，任何单位（组织）及个人不能以任何形式对软件进行复制、分发、修改、摘录、反编译、反汇编、解密、反向工程、出租、转让、分许可等侵权行为。法大大保留追诉其法律责任的权利。

责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿。
- 本文档中描述的产品均 "按照现状" 提供，在适用法律允许的范围内，本公司对文档中的所有内容不提供任何明示或者暗示的陈述或保证。

关于本文档

您购买的产品或服务等特性应受公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务和特性可能不在您的购买或使用范围。

由于产品版本升级或其他原因，本文档内容会不定期进行更新，修改的内容将会在本文档的新版本中加入，不再另行通知。

本文档可能包含技术不准确的地方或与产品功能及操作不相符合的地方，以本公司最终解释为准。

修订记录

V1.0 2020 年 10 月 初次发布
V1.1 2021 年 01 月 资质清单增加 ISO22301
V1.2 2021 年 07 月 更新可信云证书
V1.3 2021 年 10 月 更新等保测评证书
V2.0 2022 年 05 月 信息安全部重新修订

V2.1 2022 年 07 月 更新可信云证书
V2.2 2023 年 01 月 更新等保测评证书，ISO 四大体系证书，新增云安全联盟大中华区会员单位
V2.3 2023 年 11 月 更新可信云证书、等保测评证书、云安全联盟大中华区会员单位证书，新增数据安全管理能力认证（DSMC）证书
V2.4 2024 年 01 月 更新 ISO27001、ISO27701、ISO27018 及 ISO22301 四大体系证书，商用密码产品认证证书

目录

法律声明 2

版权声明 2

责任声明 2

关于本文档 2

修订记录 2

目录 4

1 信息安全概要说明 6

1.1 信息安全组织架构与职能 7

1.2 信息安全管理体系图 8

2 信息安全管理保障 9

2.1 人员安全 9

2.2 办公安全 9

2.3 可用性与业务连续性管理 10

2.4 个人可识别信息 PII 与隐私保护 11

2.5 符合性、合规性管理 15

2.6 信息安全事件管理 15

2.7 第三方供应商管理 16

3 信息安全技术保障 17

3.1 物理安全 （公有云服务商合规） 17

3.2 网络安全 17

3.3 主机安全 18

3.4 应用安全 20

3.5 数据安全 23

3.6 业务安全 27

4 信息安全运行保障 28

4.1 安全运营 28

4.2 安全运维 30

5 安全软件开发生命周期 SDLC 33

5.1 安全培训 33

5.2 需求分析 33

5.3 软件设计 33

5.4 程序编码 34

5.5 软件测试 34

5.6 发布/维护阶段 34

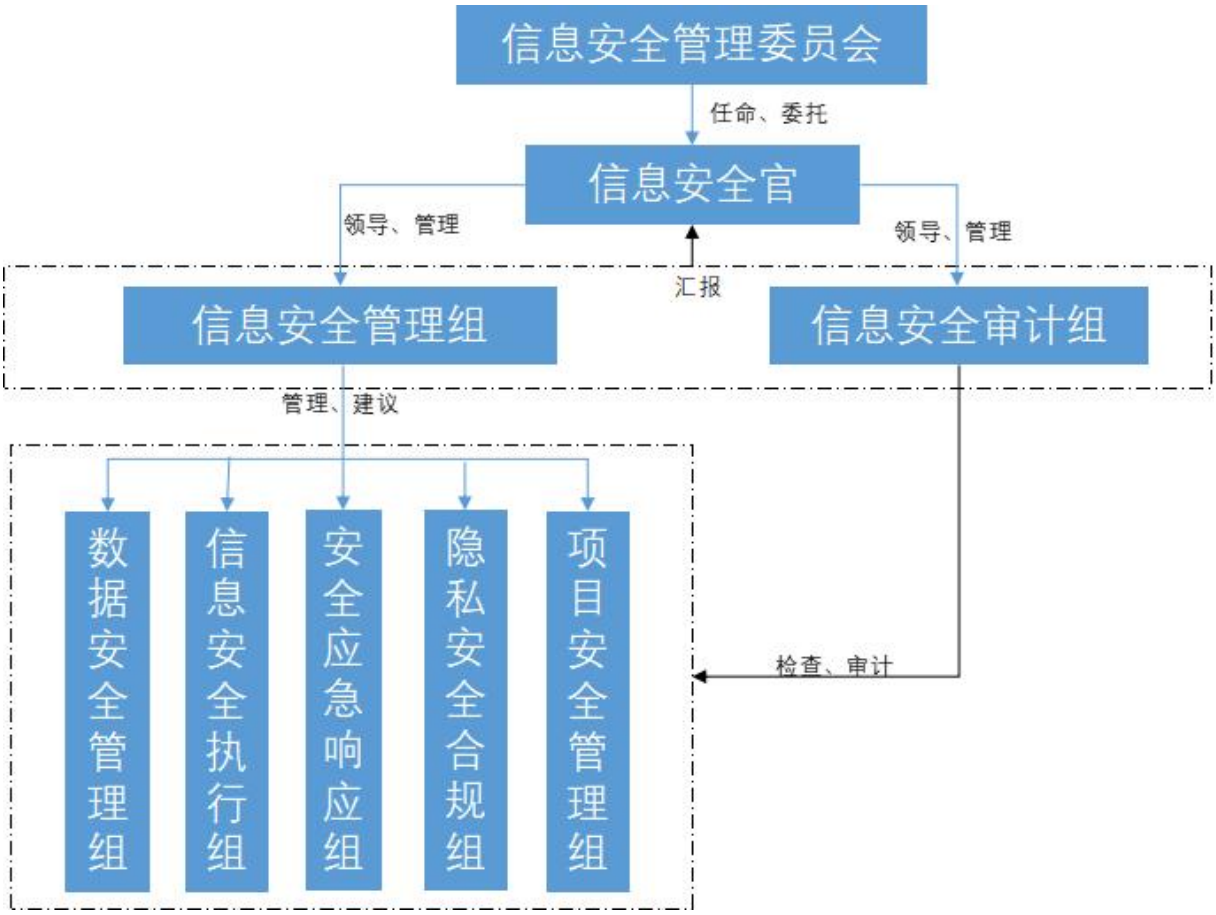
6 信息安全资质介绍 35

1 信息安全概要说明

深圳法大大网络科技有限公司是国内领先的第三方电子合同平台，主要为金融、房地产、汽车、人力资源服务、教育、保险、第三方支付、旅游、医疗、物流、供应链、B2B、B2C 线上交易平台等行业以及政府机构提供电子合同、电子文件签署及证据保全服务，同时整合提供司法鉴定和律师服务等增值服务。

作为国内领先的第三方电子合同平台，法大大充分理解电子合同产品中存在的安全风险，我们的服务旨在为企业及个人客户提供较传统合同更为出色的安全性。我们将安全性作为优先重要事务加以考量，我们期望客户能够从我们的产品及服务中获益。正因为如此，我们高度关注安全问题，同时在产品设计标准内充分考虑数据安全保护需求。安全贯穿我们的整个组织结构、培训、招聘、入离职、调岗、考核、办公、产品研发、质量、交付、运营、维护、售后等各项工作活动中。安全性是我们日常运营及灾难恢复规划工作的核心，包括指导我们如何应对潜在的威胁。安全是法大大的根基，法大大会使用国内外先进的安全技术手段、安全产品来尽最大努力来保护用户的数据安全。法大大在产品中不可避免的会使用到第三方服务或产品，我们会在合作初期对供应商开展尽职调查，合作前签署数据保密协议及合作中止后销毁或归还数据的协议等来保障第三方服务的安全。

1.1 信息安全组织架构与职能



法大大安全组织采用顶层设计原则，从上至下进行传输宣贯。

法大大成立了 CEO 为首的信息安全管理委员会，委员会成员由公司 CTO(首席技术官)、CISO(信息安全官)、各业务部门和支撑部门负责人组成，自上而下贯彻公司信息安全的整体方针政策，对公司整体信息安全负责，定期召开会议跟进信息安全问题。法大大为全体员工建立起充满活力及包容性的安全文化。

1.1.1 专项信息安全团队

信息安全部作为组织内独立的信息安全部门，配备具有专业资质的信息安全工程师。我们的安全团队是由行业内信息、应用与网络安全专家组成。这支团队的成员均具备岗位相关专业安全认证资质如 CISSP、CISP 等国内外权威安全资质证书。这支团队的主要任务在于建立法大大的防御感知体系、开发安全审查流程、制定安全策略并确保内部落地，及对内开展合规建设，确保法大大的安全文化落地。我们的安全团队会主动利用各类工具进行黑盒、灰盒及白盒等测试方法及手段检测扫描各类安全威胁因素并进行风险识别分析，并设计合理的风险消减措施，确保落地。

1.1.2 数据安全管理团队

法大大成立了数据安全管理团队，牵头承担企业数据安全管理工作，识别与遵守数据安全处理相关的所有适用的法律法规，包括但不限于制定数据安全合规性评估、安全审计管理、安全事件应急处置、教育培训等。

1.1.3 个人隐私保护团队

法大大成立了个人隐私保护团队，由隐私保护领域专家、安全工程师、法务人员等组成，同时指定了一位法务专家为个人信息与隐私保护负责人，并在对外披露的隐私政策中予以声明和告知，对法大大整体的个人信息保护负责。

1.2 信息安全管理体系图

法大大信息安全体系参考国际标准 ISO27001:2013 进行设计，其中对 14 个安全域进行拆分，主要分为三大体系，信息安全管理体系、信息安全技术体系、信息安全运行体系，其中管理体系是技术与运行体系的基础，技术体系支撑管理与运行体系的高效的运行，运行体系为管理体系和技术

体系提供保障。三大体系齐驱并驾共同融入日常的安全运维保障活动中，形成保护、预防、监控、响应、恢复为一体的纵深防御的法大大安全防护体系，为法大大平台的信息安全保驾护航。三大体系的具体控制措施参考以下各模块具体描述。

2 信息安全管理保障

2.1 人员安全

法大大员工从聘用、入职、在职、调离职进行全生命周期的管控，具体包括：

➢ 聘用

聘用前经过用人部门和人事部门的严格筛查确保人岗匹配，通过背景调查方可录用。

➢ 入职

全员签署保密协议，关键岗位员工额外签署竞业协议、关键岗位责任书，涉及处理用户信息的岗位还需签署个人信息隐私保护责任书、明确保密和用户信息保护职责；实施新员工试用期考察管理机制，试用期过后新员工需提交转正答辩材料，经过上级和人事的双重考核，答辩通过后方可正式转正。

➢ 在职

开展新员工培训，从员工入职之初就让其通晓公司内部的信息安全管理制度；研发人员还需额外参与公司应用开发安全相关培训，熟悉公司通用的安全开发流程；针对内部员工定期开展信息安全意识和隐私保护培训及宣贯。同时也会根据需要引进外部专家进行信息安全风险和数据隐私保护的培训与交流，不断提高员工的安全意识和安全岗位人员的专业技能水平。

➢ 调离职

离职和调岗通过审批流程来控制每个关键节点，主要包含岗位工作交接、账号权限的清除或调整、资产的返还等。

2.2 办公安全

法大大通过统一控制平台对员工办公终端进行管控，控制平台下发策略实现对口令复杂度、口令更新频度、自动锁屏、补丁更新、系统服务、命令指示符等进行统一设置，保障员工基本的终端安全，策略组由 IT 人员根据需要进行定期更新维护，确保适用性和全面性。并在员工的办公终端统

一安装数据防泄漏（DLP)客户端对员工敏感数据外发、网络上传、拷贝、打印等行为进行阻断与审计，任何移动介质的拷贝敏感数据会受 DLP 客户端阻断拦截，个别有业务需求人员需报备 IT 人员并以白名单形式放行；软盘、光盘等移动介质媒体，以及软件下载等要先进行计算机病毒查杀，确认无病毒后才可以使用。

另外，法大大制订了 IT 安全管理制度，软件实施标准化管理，规范员工软件安装管理规则，员工不得私自安装盗版、破解软件，拟定软件安装白名单控制软件的安装；默认设置开启系统自带病毒和威胁防护，安装防病毒软件，实时阻断和停止恶意软件在办公设备上的安装和运行，保护终端安全。

对员工的上网行为管控，法大大部署了上网行为管理系统，制定访问控制规则对员工在办公时间段内的网络访问行为进行管控。

同时对网络进行准入认证，需安装指定杀毒软件且进行身份核验通过后才可接入办公网络。

邮箱安全方面，法大大的员工邮箱默认开启使用 SSL/TLS 协议进行传输加密以保证员工传输数据的机密性和完整性；邮箱对于异地登录（非此前常用 IP）等异常登录行为会邮件提醒用户，方便用户及时采取修改密码等安全应对措施；定期开展管理人员操作日志审计和员工异常登录、使用行为审计，保障邮箱使用安全。

2.3 可用性与业务连续性管理

法大大所有核心服务从存储、服务器、软件到网络（负载均衡、交换机、防火墙等）等层面均遵循高可用、冗余设计原则，通过跨可用区部署与服务冗余等技术手段消除单点故障，确保服务达到同城双活、异地容灾。

法大大对接的第三方服务机构，使用服务均采用主备机制，保证所有业务的稳定性及可靠性，如 CA 机构、可信时间戳服务机构、短信服务商、数据认证服务商等都配置多个备用服务提供商，如主服务商出现故障后台可进行自动切换，确保业务连续性。

法大大配备 7×24 小时的运行维护人员，具备完善的故障监控、业务可用性监控、即时通讯软件机器人/短信/邮件/电话多重告警、快速定位、快速恢复等一系列故障响应机制。故障快速恢复手段包括限流、故障隔离、降级、自动扩容、自愈、自动切换等。

建立生产事件管理机制，定义不同事件级别的解决时效，从事件的发生、问题定位到解决关闭

和预防措施进行全流程记录追踪和管理。

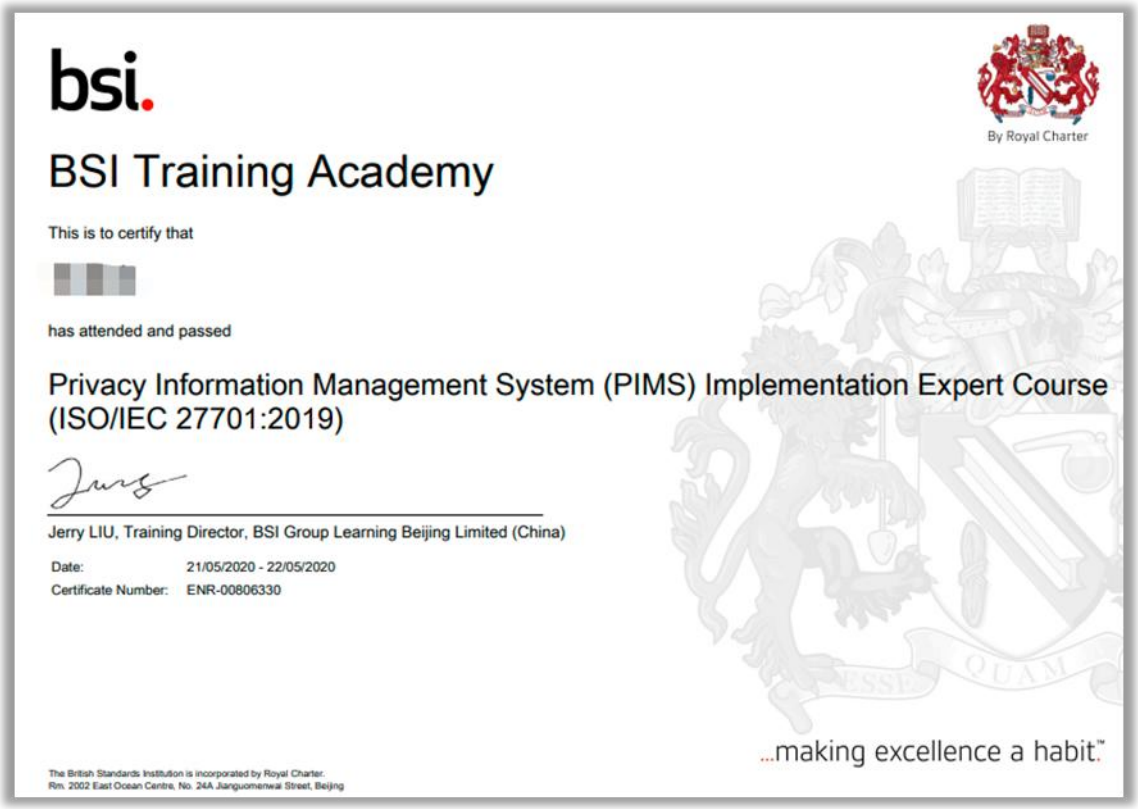
根据业务影响分析（BIA)结果，确定恢复时间目标（RTO）及恢复点目标(RPO)，制定完善的应急预案来快速响应突发生产事件，确保关键业务的可用性，并通过定期的应急演练验证预案的可操作性和适用性，便于更快速熟悉地应对各种可能的突发的生产事件。法大大承诺服务可用性高达99.95%以上。

2.4 个人可识别信息 PII 与隐私保护

用户数据是法大大的生命线，保障用户隐私信息是法大大义不容辞的责任，法大大不断引进先进国际标准，从 ISO27018 公有云个人信息保护认证，云端用户隐私数据的保护到 ISO27701 隐私信息管理体系认证，法大大参考业界隐私保护最佳实践建立了一套独有的隐私信息管理体系来保障平台用户隐私安全。具体包括：

2.4.1 隐私保护组织

法大大成立了个人隐私保护团队，由隐私保护领域专家人员、安全工程师、法务人员共同组成，为确保所有人员均具备相关隐私保护能力，在隐私信息管理体系建立之初法大大就聘请了 BSI 资深讲师开展了隐私保护专家课程，所有人员都通过考核并取得合格证书（参考下图证书）。个人隐私保护团队负责公司整个隐私安全管理体系的建立、实施、维护和监视，保障法大大各项隐私保护活动的顺利开展与实施。组织内部经常开展不同形式的交流与讨论，共同探讨和解决隐私相关问题。



bsi.

By Royal Charter

BSI Training Academy

This is to certify that

has attended and passed

Privacy Information Management System (PIMS) Implementation Expert Course (ISO/IEC 27701:2019)

Jerry LIU, Training Director, BSI Group Learning Beijing Limited (China)

Date: 21/05/2020 - 22/05/2020

Certificate Number: ENR-00806330

...making excellence a habit.™

The British Standards Institution is incorporated by Royal Charter.
Rm. 2002 East Ocean Centre, No. 24A Jianguomenwai Street, Beijing

隐私信息管理体系实施专家课程培训证书

2.4.2 隐私保护责任

法大大明确指定了 1 位法务专家为个人信息与隐私保护负责人，并在对外披露的隐私政策中予以声明和告知，对法大大整体的隐私安全和合规安全负责。组织内部对于可接触和处理用户个人信息，尤其是隐私信息的岗位人员除了签署基础的《保密协议》外还需额外签署《个人信息隐私保护责任书》明确岗位中的个人信息和隐私保护责任。对于违反相关隐私保护制度和要求的任何行为进行违规追责。

2.4.3 隐私保护意识培训

法大大建立了完善的信息安全培训体系，新员工入职时需进行包括隐私保护的信息安全意识培训，使其了解组织内部的隐私保护要求。信息安全部定期开展组织内的面向产品与开发的隐私保护培训和个人信息、隐私法律法规解读培训与考核，指导员工将隐私保护需求融入产品的设计与开发中，保障产品的隐私安全与合规。

2.4.4 隐私影响分析（PIA）

为有效的识别和控制隐私风险，法大大结合自身业务流程从用户注册、实名认证、合同签署、

客户服务等涉及处理用户个人信息的场景开展隐私影响分析，识别各业务流程中个人信息的采集、传输、使用、存储、对外提供、销毁等数据处理环节中存在的隐私安全与合规风险。并提出具体的改进措施与方案降低隐私风险。

2.4.5 个人信息生命周期管理

法大大遵从数据保护生命周期来保护用户的个人信息和隐私信息，从用户信息的采集、传输、存储、使用、共享、披露、删除等关键节点采取有效的管理与技术手段保护用户个信息和保障用户隐私权利。

- 个人信息的采集

法大大仅在获得客户的明确授权同意后，采集提供产品和服务所必须的个人信息，个人信息和隐私信息的采集通过公开发布的隐私政策（https://legal.fadada.com/policy/1597793752477609984）明确告知个人信息主体，采集的个人数据类型、采集目的、处理方式和范围等取得个人信息主体的明确授权同意。法大大收集个人信息遵循最小必要原则，收集的个人信息类型是与实现产品或服务的业务功能所必须的。

- 个人信息的传输加密

法大大提供的应用服务全站使用 https，采用权威 CA 机构（DigiCert）签发的 SSL/TLS 证书加密传输，确保个人信息在传输过程中的机密性、完整性；

- 个人信息的使用控制

法大大内部对于个人信息的访问与使用有严格的限制，内部访问控制遵循 RBAC(基于角色的访问控制)确保只有业务需求的人员通过申请审批后方可访问涉及用户个人及隐私信息的相关系统。操作人员需要通过 VPN 登录访问，所有操作行为都会被记录及定期审计；对于后台类系统中个人信息的展示会采用掩码和水印技术，保障个人数据使用过程中的安全与可追溯；

测试规范中明确严禁使用用户真实信息进行测试；内部实施数据分级分类管理规定，用户隐私数据归属数据机密级别，任何形式的拷贝、上传、对外发送都会被阻断和限制；

- 个人信息的存储加密

法大大对于个人信息的存储在满足相关法律法规的要求下，遵循存储时间最小化原则；对用户隐私信息如身份证、手机号码等敏感数据进行高强度加密后再存储。包括但不限于数据库、对象存储等。

- 个人信息的共享

法大大仅会出于产品或服务需要与第三方共享用户信息，并在隐私政策中告知用户主体共享的目的，取得用户的授权同意。法大大制定了第三方供应商管控流程，严格筛选和业务所必须的合作伙伴，同时对第三方开展尽职调查评估个人信息隐私保护能力，并与合作的第三方服务供应商签署保密协议和个人信息和数据保护承诺函明确个人信息和隐私保护责任。

- 个人信息的披露

法大大原则上不会随意披露用户的个人及隐私信息，除非法律、法规或强制性的执法机构要求所必须披露的情况下，法大大会事先征得用户主体的同意，并告知具体披露的用户信息。

- 个人信息的删除

当客户注销其账号或明确告知法大大需要删除其个人信息时，法大大在满足法律法规及监管前提下，自动或在约定期限内彻底删除或匿名化处理。

2.4.6 用户主体权利响应

法大大制定用户主体权利响应流程，保障用户权利的及时响应。法大大用户享有个人信息的查

询权、更正权、撤回同意、索取副本、删除、注销账号等权利，法大大承诺尽量从产品功能上实现用户主体权利响应，个别无法从功能上实现的会统一通过客服受理窗口接收用户关于个人信息权利的诉求，同时与内部产品和技术人员联动，在规定时间内完成响应和请求处理，反馈处理结果给客户。

2.4.7 隐私法律法规遵循

法大大严格遵循国内相关个人信息、隐私保护法律法规。隐私合规专家与法务人员共同解读，对标《信息安全技术 个人信息安全规范》、《个人信息保护法》等个人信息、隐私保护法律法规，并提出可落地的合规遵循方案，确保满足合规要求。同时积极应对有关部门监管要求，开展自查自纠，主动满足合规要求。

2.4.8 隐私默认设计（PbD Privacy by Design）原则

法大大隐私保护的控制不仅体现在数据流转的各个环节，同时将隐私保护要求内嵌于产品需求设计、开发、测试、发布、运维各生命周期中，实现默认隐私保护。同时由安全工程师全流程保驾护航，经过严格测试和安全审查，确保隐私合规需求得到实现方可上线。针对产品和开发人员不定期开展产品设计中的隐私保护和隐私保护法律法规培训，提升产品的隐私保护水平。

2.5 符合性、合规性管理

法大大组建了隐私安全合规团队，团队成员由法务与信息安全专家构成，负责及时识别和梳理适用的行业法律法规、信息安全法律法规和隐私保护法律法规，如《网络安全法》、《个人信息保护法》、《数据安全法》、《GB/T 35273—2020 个人信息安全规范》开展解读与差距分析，推进差距的整改，复核整改结果确保产品及内部管理制度确实满足法律法规的要求；与外部监管机构保持联系，积极配合监管机构的调研和审查，同时及时跟进监管机构的监管趋势及监管要求，定期开展自查与自评估，确保满足监管合规要求；定期开展第三方的独立审查，评估和验证现有信息安全体系运行的有效性和适宜性，审查发现的问题都及时跟进处理，确保体系的有效运行和持续改进。

2.6 信息安全事件管理

法大大的信息安全事件包括内部通过监控工具或日志审计主动发现的和外部或员工上报的所有信息安全事件，包括但不限于系统遭受入侵、感染病毒、数据泄露、网络钓鱼事件等。法大大内部

制订了信息安全事件的管理程序文件，文件明确定义了事件的等级和事件的处理流程，事件处置流程统一遵循识别分类--调查取证--抑制或根除和恢复--通知相关部门--总结归档。处理的最重要原则是采取有效的应急措施控制事态的发展，最大程度减轻事件给法大大和客户带来的影响。涉及影响客户服务可用性和客户切身利益的信息安全事件，法大大会及时通过公告或其他有效方式告知客户。

法大大重视用户数据的安全，保障了用户数据泄露的闭环管理，针对用户 PII 数据泄露的事件制订了 PII 数据泄露的处置预案，在发生 PII 信息泄露的突发事件时，法大大提供了一个明确的、可操作的处理流程和处置方案，同时定义了各部门在预案中承担的具体职责，并定期组织相关人员开展演练，熟悉预案的处置流程和具体职责。

法大大关注事后应急处置的同时也不断加强员工安全意识培训、部署监控审计和告警工具，提高主动识别发现、预警和感知信息安全事件能力，最大限度降低信息安全事件给客户和法大大带来的影响。

2.7 第三方供应商管理

法大大制订了第三方服务供应商管理流程从供应商的选型准入、服务期间的供应商考核评估及最终的供应商合作退出的全生命周期进行管控：

- 供应商准入：

a) 由采购专员进行调研选型、供应商产品信息、资质收集与审核；

b) 针对供应商服务的功能、性能、兼容性、稳定性等指标开展服务或产品测试评估；

c) 开展信息安全问卷和应用安全评估；

d) 签署合同、保密协议和数据安全条款来约定双方权利及义务。

- 供应商考核：

a) 定期针对供应商的服务质量进行考核评估；

b) 考核结果及时与供应商反馈跟进实现供应商服务的优化改进。

- 供应商清退：

a) 服务到期未续约自动退出；

b) 考核未达标淘汰管理退出。

3 信息安全技术保障

3.1 物理安全 （公有云服务商合规）

法大大采用多云融合架构，合作的公有云服务商均为业界领先的云服务提供商。云服务提供商的机房和数据中心皆符合相关机房规范和数据中心建设要求，具备较强的安全防护能力和容灾应对能力。服务商均取得了 ISO27001 信息安全管理体系认证、ISO27018 公有云用户隐私保护认证、ISO22301 业务连续性管理体系认证、ISO20000 信息技术服务管理体系认证、工信部可信云等国内外权威安全认证，并且通过了公安部信息系统安全等级保护测评（三级）/（四级），为法大大提供了合规安全的电子签章服务奠定了基础和保障。各云服务商的安全说明具体以各服务商对外发布的安全说明文件或安全白皮书为准。

3.2 网络安全

3.2.1 传输安全

数据传输安全：采用 TLS 1.2 及以上协议、权威的 DigiCert SSL 证书，高强度加密套件，实现全站 HTTPS 数据传输，并使用 HSTS（HTTPStrict Transport Security）避免链路劫持降级攻击，确保数据传输过程中的机密性、完整性。

3.2.2 抗 DDoS

法大大数据中心出口网络部署于运营商 BGP 节点，依靠运营商节点的近源压制能力，能够有效的抵御来自其它区域的包括 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood 、

SSDP Flood、DNS Flood、HTTP Flood、CC（ChallengeCollapsar）攻击。

法大大 CC 防御通过智能动态指纹验证模块及多维攻击姿态模型匹配，有效过滤各种类型的 CC 攻击，每秒可过滤百万并发 CC，误伤极低。

法大大 DNS 服务器，74 种解析线路，可有效解决突发的上亿级别的随机 HOST A 记录查询攻击、递归 DNS 穿透攻击、DNS 流量攻击等多种针对域名解析的攻击请求。

3.2.3 边界安全

入侵防御：法大大入侵防御系统已集成威胁情报、基础防御以及虚拟补丁等功能，能够对法大大的互联网边界流量进行实时监控、统计与分析，主动发现外部入侵与恶意外联等未知风险，并提供实时的防护与告警。

ACL IP 白名单：法大大通过设置 ACL IP 白名单对访问关键系统的 IP 进行识别和过滤，从而限定访问关键业务的用户，并定期维护白名单，保证关键系统能够得到安全的访问保护。

安全组：法大大使用安全组在云端划分不同的安全域，通过配置安全规则进行合理的网络隔离，控制各个安全组内不同实例的入流量和出流量。

业务网隔离：法大大的网络依据用途划分为访客，办公，研发，生产等多个安全域，对于不同的安全域之间，使用逻辑控制，物理控制等组合方式实现隔离，除了部分经过安全加固的可信环境外，互相之间无法访问。

3.2.4 内网探测

法大大生产环境使用虚拟化技术，数据传输通过进程交互，不依靠 IP 路由传输，不存在 ARP 与 IP 的映射关系，能够有效抵御 ARP 欺骗攻击。

法大大生产环境使用虚拟化技术，不存在网络统一网关，能够有效抵御 sniffer 嗅探攻击。

法大大生产环境使用蜜罐技术，能够有效捕获 scan 行为，并自适应虚假返回，有效迷惑攻击者。

3.3 主机安全

3.3.1 态势感知

法大大在云主机部署 Agent，实时识别、分析、预警安全威胁的统一态势感知系统，通过安全告警、防勒索、防病毒、防篡改、配置合规检查等安全能力，实现威胁检测、响应、溯源的自动化

安全运营闭环，保护法大大的信息资产安全合规。

3.3.2 入侵威胁检测

法大大在云主机部署 Agent，实现和云端安全中心联动，提供实时的入侵检测的安全能力。主机的入侵检测中主要包括了异常登录检测、网站后门查杀（Webshell）、主机异常行为检测（进程异常行为和异常网络连接检测）、主机系统及应用的关键文件篡改检测和异常账号检测等功能。同时还提供智能学习应用白名单的能力，识别可信和可疑/恶意程序形成应用白名单，防止未经白名单授权的程序悄然运行，可避免主机受到不可信或恶意程序的侵害。

3.3.3 病毒防御

在主机安装 agent，还实现了对主流勒索、挖矿、木马等病毒进行实时拦截。在系统内核层面实现云上文件和进程行为的全局监控和实时分析，有效绕过顽固木马和恶意程序的反查杀能力；agent 能够基于程序行为分析，挖掘出黑名单未能辨识的恶意威胁，实现主动拦截；其云端病毒库也保持实时更新。

3.3.4 基线检查

通过 agent 对主机进行安全配置扫描，包括账号安全、系统配置、数据库风险、合规对标要求等方面，对未符合标准的项目进行提醒。同时，云安全中心也提供云平台配置检查，包括身份认证、网络访问控制、数据安全、日志审计、基础安全防护五个维度的最佳安全配置实践检测。

3.3.5 主机漏洞扫描/补丁升级

通过 agent 定期对所有云主机进行安全漏洞扫描，法大大能够及时发现系统和中间件漏洞，并提供修复建议和修复措施。漏洞扫描及修复引擎，能够实现同时对多个系统和应用进行扫描和修复的安全运维工作，同时还能提供针对网络上突然出现的紧急漏洞的应急检测。

3.3.6 服务最小化

法大大的主机均采用服务最小化安装，执行统一的加固配置，仅运行所需服务，将攻击面降至最小。

3.3.7 生产测试环境隔离

法大大生产环境和测试环境分别使用独立的云账户创建和管理，实现生产环境和测试环境的隔

离，防止因为某一环境产生的问题影响到其他环境系统的运行，保证各个系统平台的独立性。

生产环境的数据只能在生产环境内部处理和存储，不出生产环境；对生产环境的维护，必须通过运维专用 VPN 连接到堡垒机，通过堡垒机的双因素认证后，再根据堡垒机赋予的权限连接到相应系统的管理入口，所有运维操作都通过堡垒机进行维护操作，同时相关的操作将被堡垒机记录并定期审计。

3.3.8 运行权限最小化

针对运行权限的控制，法大大实现了主机账号、数据库账号、存储账号等运行权限最小化配置。法大大对权限管理的四个特性和四个原则：

四个特性：继承性、累加性、优先性、交叉性。

四个原则：拒绝优于允许原则、权限最小化原则、累加原则和权限继承性原则。

3.4 应用安全

3.4.1 WAF

➢ 基于云计算的 Web 防护

法大大引入行业领先的云 WAF--创宇盾，创宇盾是由知道创宇国际安全专家组成的安全研究团队利用大数据及云计算技术实现 Web 安全防护，通过云平台的优势，创宇盾已拥有全球海量的风险样本库，平均每天新增风险样本超过上百条，并持续不断更新；基于云计算的创宇盾云防御平台可以抵御已知的 OWASP Top10 的黑客攻击行为，例如：注入类、跨站脚本(XSS) 、不安全的直接对象引用、使用含有已知漏洞组件等恶意攻击行为等。

➢ 基于大数据的协同防御

传统的防御手段都是各个组织各自为战，攻击数据相互独立，而法大大使用的创宇盾协同防御机制将会针对不同网站的攻击数据进行关联分析，提炼出最新的漏洞信息，包括 0day 漏洞，只要发现一个网站被攻击，创宇盾就会全网封锁该攻击者，实现“一网攻击，全网防护”，利用大数据分析平台，进行联合协同防御，可将防御成功率提升至 99.99%。

➢ 云规则防御/虚拟补丁

法大大使用的创宇盾是基于云模式构建的，可以实时对云防御规则库优化和分发虚拟补丁程序，

节省单台设备人工升级的时间成本，当出现 0day 或者 1day 攻击时，可以及时进行防护，缩短安全空白期，提升法大大 SaaS 的安全能力。

3.4.2 漏洞扫描

全面发现资产关联的子域名、服务器 IP 等，并生成详细的资产指纹信息，如中间件、应用程序、OS、端口、服务等，让安全不留死角。

深度专业漏洞扫描，包含对主机系统、应用服务、中间件等进行专业漏洞扫描，及时发现潜在风险并预警。

3.4.3 APP 加固

- 防逆向

通过 DEX 加密、源码混淆等加固技术对 DEX 和 SO 文件进行保护，防止被 Apktool、IDA 等逆向工具进行分析。

- 页面数据防护

应用防劫持、应用防截屏、虚拟键盘，对输入输出数据进行保护。

- 数据防泄漏

使用加密算法，保护本地数据的安全。

- 传输数据防护

在客户端和服务端对数据进行加密，保证通道中传输的数据为高强度加密后的数据。

3.4.4 统一身份认证和应用级授权

法大大使用统一身份认证和应用级授权，实现统一账户、统一认证、集中授权的管理服务：

- 统一账户

一个账号对接多个子系统，同一用户在各种不同类型应用系统之间的账号相互打通。各子系统的账户关联到主账户中，实现账号体系的统一，方便账号的生命周期管理；

- 统一认证

采集多种认证因子，通过发行加密身份凭证到不同应用的服务端进行认证，实现统一认证和单点登录；

- 集中授权

以 RBAC 模型为基础，构建灵活高效的权限管控系统，集中管理应用系统的业务角色和功能资源，例如菜单、按钮、后台使用资源等，从单个账户、组织单位、组等不同维度与角色进行绑定，同时将角色与权限范围内的功能资源进行绑定，达到从不同粒度集中分配权限的目的，防止越权(未授权)操作。

3.4.5 操作全链路审计

法大大平台在文件签署过程中，所有参与方的多种关键信息（如：文件的指纹（HASH），参与各方网络信息，身份证验证信息等）全程加密存证，能够在后期提供出证报告，确保数据的不可篡改。

3.4.6 密码算法

法大大平台的密码存储采用 SHA2-256 算法加上用户级 salt，经过多轮迭代后保存在数据库。校验时按同样散列算法比对密文，全程无需提供明文密码，极大度提升密码的安全性；敏感信息采用对称加密算法，密钥保存在 HSM 中，能够确保敏感信息的安全性。

法大大全面支持国密系列算法（SM2、SM3、SM4 等），同时法大大产品也已通过国家密码管理局检测中心的产品检测，获得了由该局颁发的《商用密码产品认证证书》。

3.4.7 访问控制

法大大管理系统的账号权限遵循内部统一申请流程，通过正式的授权控制特殊访问权限的分配。通过调岗流程和离职申请流程，控制权限的变更和删除并定期开展用户权限的复查工作。

开发环境、测试环境与生产环境之间实现物理隔离，保证生产环境的独立性，研发人员及普通系统权限管理人员无权限访问生产系统；生产环境由专业的运维人员管理，管理维护接口通过防火墙与外网隔离，且运维人员必须通过运维专用 VPN 连接到堡垒机，通过堡垒机的双因素认证后，再根据堡垒机赋予的权限连接到相应系统的管理入口，所有运维操作都通过堡垒机进行维护操作，同时相关的操作将被堡垒机记录并定期审计。

3.4.8 安全软件开发生命周期

法大大安全软件开发生命周期（Secure Development Lifecycle，简称 SDLC），目标是将安全融入到整个产品开发生命周期中。SDLC 在人员安全技能培训、需求设计审核、安全开发、安全

测试审核、持续运营的各个环节把关，每个节点都有完整的安全审核机制从而有效地提高产品的安全能力并降低安全风险。

3.5 数据安全

法大大建设以数据为核心的动态信息安全防控体系，通过数据治理、安全机制、风险管理和审计溯源等重点识别和控制数据采集获取、传输、存储、使用、共享、销毁等动态过程中的安全风险。并已取得由中国信息通信研究院颁发的数据安全管理能力认证证书。

3.5.1 数据分类分级管理

法大大组织内部实行数据分类分级管理，通过数据治理识别和梳理业务活动中产生的数据类型，对数据进行识别与分类，根据数据的重要性、机密性、影响度等划分不同等级。组织制定了数据安全策略规范，针对不同等级数据的使用、保存、共享和销毁等明确了受控和保护要求。

3.5.2 数据采集获取

法大大保证数据来源的合法合规，定期开展数据合规性审查，明确数据采集的目的、用途、方式、范围、采集源、采集渠道等内容，并对数据来源进行鉴别和记录，确保数据来源的合法合规。

3.5.3 数据传输

法大大提供的服务全站启用 HTTPS 安全传输，使用权威 CA 机构（ DigiCert ）的 OV SSL 证书，在保护数据传输的机密性和完整性的同时，并向用户证明 SaaS 的真实身份；

TLS/SSL 签名算法：SHA256WithRSA，开启 HSTS（Http Strict Transport Security），关闭 SSL3.0、TLS1.0、TLS1.1，仅支持 TLS1.2+，并使用安全的加密套件（cipher suites）。

法大大内部运维人员必须统一通过 VPN 连接至 VPN 网关才能登录到堡垒机进行相关运维操作，与生产系统的通信通过 SSL VPN 加密传输保护。

3.5.4 数据存储

法大大的数据均在中国大陆境内存储，建立了数据存储备份及异地灾备机制并定期开展备份恢复演练；同时法大大对存储介质管理有严格的要求，对于任何移动介质的拷贝敏感数据会受终端上的 DLP 软件阻断拦截。

法大大对个人敏感信息数据如手机号、身份证号码等进行高强度的 AES 算法加密后存入到数据

库；对于非结构化文件，如合同文件等进行高强度的 AES 算法加密后，再存储到高可用的对象存储。

3.5.5 数据使用

法大大严格遵循数据处理最小化、必要原则，明确数据的处理和使用规范，确保员工只能访问职责所需的最少够用的数据。对数据进行操作时，做好去标识化处理，明确数据脱敏的业务场景和统一使用适合的脱敏技术。

3.5.6 数据共享

在对外数据开放共享方面，法大大仅会出于产品或服务需要与第三方共享用户信息，并在隐私政策中告知用户主体共享的目的，取得用户的授权同意，同时严格遵循《网络安全法》、《数据安全法》、《个人信息保护法》要求，以用户隐私信息保护为首要前提，制定对外数据披露细则，明确要求所有对外数据输出必须遵循以下原则：

保护用户隐私：涉及用户隐私数据未经用户的充分授权，不得收集、分析或向任何第三方输出，因法律法规的要求、强制性的行政执法或司法要求所必须提供的信息除外；

必要性和最小化：对外数据输出时，仅共享提供服务所必要的信息，同时必须将数据的数量及知情者控制在最小范围内；

合规性：对外数据合作必须遵循适用于法大大的法律、法规、政策、行业标准等要求，必要时开展个人信息安全影响评估，根据评估结果严格筛选和业务所必须的合作伙伴，并与授权合作伙伴约定严格的数据保护措施。

公开透明：以明确、易懂和合理的方式公开共享用户个人信息的范围、目的，并接受外部监督。

3.5.7 数据提取

法大大内部所有生产数据的提取，都通过审批流程来控制，确保数据的提取符合业务需求，并留存所有的审批记录，保证提取数据的可审计、可追溯。其中制定了生产数据库查询审批流程、数据导出申请流程来控制生产数据的提取和导出。

3.5.8 数据销毁

合同数据销毁：在合同相关各方达成书面协议一致同意销毁合同的情况下，法大大在存储系统

将对应合同文件通过云服务商提供的删除接口进行永久清除，使得相应的合同无法恢复。

存储设备报废处理：目前法大大采用的云服务商已全部通过等保三级测评及 ISO27001、ISO27018、ISO27701、ISO22301 等认证，运营合规可控，对于数据销毁，通过逻辑清零，物理折弯、消磁等方式做到合规可靠的数据消除。

3.5.9 密钥管理

法大大采用云服务商托管硬件安全模块（HSM）的方式，基于国家密码局认证的硬件加密机，提供了云上数据加解密服务，能够对密钥进行安全可靠的管理。使用 HSM 进行密码运算和安全托管等功能，利用硬件机制来保护密钥在生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节不会离开 HSM 的安全边界。

a. 密钥生成

密钥生成由专用密码模块内部产生，不以明文方式出现在密码模块之外；密码模块具备检查和剔除弱密钥的能力。

b. 密钥存储

密钥加密存储，并采取严格的安全防护措施，能够防止密钥被非法获取；密钥加密存储于符合 GM/T 0028 要求的密码模块中。

c. 密钥分发

密钥分发采取身份鉴别、数据完整性、数据机密性等安全措施，能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

d. 密钥导入与导出

密钥的导入与导出采取妥当的安全措施，能够防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

e. 密钥使用

密钥根据使用用途，明确区分密钥；对于公钥密码体制，在使用公钥之前对其进行验证；使用安全措施防止密钥的泄露和替换；密钥泄露时，密钥停止使用，并启动相应的应急处理和响应措施。严格按照密钥管理相关规定进行周期性的密钥更换；采取有效的安全措施，保证密

钥更换时的安全性。

f. 密钥备份与恢复

法大大已制定密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；

g. 密钥归档

法大大采取安全有效的措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；归档密钥进行数据备份，并采用有效的安全措施进行保护。

h. 密钥销毁

法大大的密钥管理措施具有在紧急情况下销毁密钥的功能，包括但不限于拆机密钥自毁、远程控制销毁等措施。

3.5.10 数据安全审计

3.5.10.1 数据库审计

法大大通过数据库审计系统，实时掌握数据业务运行稳定性，为数据库系统的运行管理与监控提供依据；实时监控与审计系统安全风险细粒度管控和合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断；通过对用户访问数据库行为的记录、分析和告警，事故追根溯源，加强数据库访问控制，提升法大大数据资产安全。

3.5.10.2 数据防泄漏

法大大内部终端部署 DLP 数据防泄漏系统，对公司敏感文件的发送、上传、拷贝、打印等进行跟踪记录，防止通过邮件、聊天工具、网盘、U 盘拷贝等途径泄露数据，对用户泄密行为进行审计、阻断。DLP 系统能有效防护敏感数据外泄，同时提高员工对敏感文件的保密意识。

3.5.11 数据库安全运维

法大大通过建立系统运维行为流程化管理，对数据库运维行为提供事前审批、事中控制、事后审计、定期报表等功能。规范数据库运维审批流程，有效实现事中管控、实时运维监控，提供完善管控手段、实现办公流程的深度整合、实现数据库操作管理的政策合规性。

3.5.12 异地灾备

法大大主数据中心位于上海，分布在不同的多个可用区（AZ），主数据中心的结构化数据和对象文件准实时同步至灾备数据中心。

法大大使用的主数据中心（上海）和灾备数据中心（广州）相距 1000 公里以上，可以防止因为自然灾害及不可抗力灾难造成客户数据的丢失。

3.5.13 数据安全责任与意识

数据安全依赖于每一个法大大员工，法大大重视每一位员工的数据安全意识。自员工入职即对员工开展数据安全意识培训，宣贯数据安全的重要性，以及违反相关数据安全法律法规需承担的法律后果。所有员工要求签署《保密协议》和《商业行为准则》，明确数据保密责任。法大大制定了《高压线行为准则》，对于违反数据安全的任何行为列为红线行为并严格追责处理。

3.6 业务安全

3.6.1 验证码安全

随着机器学习与图像识别技术的发展，法大大已深刻感知到第一代、第二代验证码已经失去了安全验证的作用，所以法大大采用了第三代无知识型验证码技术，努力提升整体安全性。

第三代无知识型验证码技术基于人类固有的生物特性及操作环境信息多个维度，来判断操作者是人类还是机器，自适应风险分析引擎通过用户的操作进行风险判断，逐级提升验证码难度。从源头避免强大的图像识别通过训练能够快速识别第一代图片验证码和第二代认证型验证码。

3.6.2 账号安全

法大大账号口令复杂度要求极其严格，密码的传输，计算，存储，找回均采用不可逆方式对密码进行比对和更新，任何人无法对用户的密码进行获取，包括法大大员工。在找回密码环节，法大大使用了先进的技术手段避免因用户的手机丢失导致账号被窃取。在登陆和注册环节，我们使用防注册机和防撞库方案来最大程度保障用户的账号安全。

3.6.3 个人信息/用户隐私

法大大产品在需求设计阶段对用户隐私和敏感数据经过了安全设计，能够确保产品安全合规，在个人信息的展示和日志输出中对用户隐私信息进行掩码显示，存储时使用对称加密算法加密存储，

采集时明示客户（用户隐私协议），在符合相关法律法规的要求下可按客户要求进行个人信息进行销毁，在内部法大大有极其严格的访问控制策略，能够保证用户的个人信息的安全。

法大大已通过 ISO27018 公有云个人信息保护国际认证和 ISO27701 隐私保护体系认证，此认证对法大大的个人信息/用户隐私保护是一种有效的证明。

3.6.4 数据防篡改

数据文件上传至法大大，法大大会将文件的哈希值广播至区块链，利用区块链的原生防篡改技术来保障用户的合同文件全程防篡改。

4 信息安全运行保障

4.1 安全运营

4.1.1 资产管理

法大大通过 DNS 记录、持续的互联网暴露面测绘、端口扫描工具等定期对资产进行扫描，对变动信息进行记录和告警，并利用 agent 对终端进程和账号进行采集实现对资产的统一清点。

4.1.2 内部风险评估

法大大建立了内部风险评估常态化管理机制，定期开展内部风险评估，组织信息安全活动的关键部门和关键岗位人员，通过实地调研和访谈，识别各业务流程和活动中的存在的问题点和风险点，生成风险评估报告，针对报告中的高、中风险问题进行评审和验证，输出风险评估问题清单和整改建议，指定整改责任人和整改期限，定期跟进和验证相关风险问题的整改，形成内部风险评估问题的闭环管理，有效控制和降低内部风险。

4.1.3 日常安全巡检

法大大开展常态化安全巡检与审计，日常巡检包含 DLP 外发记录审计、邮箱异常登录审查、后台系统操作日志审查、WAF、主机安全 agent、安全态势感知巡检、Github 代码泄露监控等，及时发现日常工作中的信息安全问题及风险，生成汇总分析报告，当日内发现的异常问题进行及时跟进和确认。

4.1.4 威胁情报共享

法大大与业界安全应急响应中心、信息安全漏洞共享平台合作，同时在漏洞盒子等平台开设安全应急响应中心，收集威胁漏洞情报；与第三方安全服务机构开展密切合作、积极参与安全社区、安全论坛、安全同行交流工作群，实现威胁情报共通共享，及时开展排查分析采取有效应对和处置措施。

4.1.5 端点检测和响应

法大大采用端点检测和响应技术，通过对端点进行持续检测，发现异常行为并进行实时干预，同时通过应用程序对操作系统调用等异常行为分析，检测和防护未知威胁并实时告警。

4.1.6 自建安全应急响应中心 SRC

法大大参照 ISO/IEC 30111、ISO/IEC 29147 等建立产品安全漏洞处理及漏洞披露流程。

法大大是行业内最早自建安全应急响应中心（https://sec.fadada.com）的电子合同服务提供商。参照业界的最佳实践，法大大结合自身实际建立了一套自有 SRC 的漏洞处理流程，从漏洞的提交、漏洞审核确认、漏洞积分奖励、漏洞修复复核、漏洞的关闭实现全流程的漏洞跟进管理。

法大大 SRC 运营至今收获了许多白帽的大力支持，也取得了一些运营成果，其建立的初衷也是与外部安全爱好者建立一个信息交流平台并利用众测的力量协助和鞭策法大大不断提升和改善自身产品的安全性。我们也在不断完善法大大 SRC 平台的运营规则，积极开展一些运营活动，鼓励和吸引更多的白帽为法大大的安全贡献力量。

4.1.7 合作众测平台

法大大积极与国内外第三方安全众测平台开展深度合作，借助第三方众测平台的资源和能力，为法大大的产品安全提供安全测试，从第三方的视角挖掘自身平台的问题及漏洞，提供修复和改进

建议。众测形式能有效的弥补自身安全能力的不足和薄弱点，减少安全盲区，更全面的帮助内部安全团队全面审视自己的能力和产品安全，为法大大平台安全增加了一道保障。

4.1.8 安全事件响应

法大大对安全事件进行分级响应机制，应急响应专家接到相关安全事件后第一时间进行研判并进行分级分类，并开展调查和取证，根据调查取证结果，按照相关的响应规范进行处理及缓解，事件得到缓解或完结时通知相关部门和同事事件的全部过程。事件关闭后形成相关的分析和总结报告。

4.1.9 漏洞管理

无论是内部测试发现的还是外部接收的漏洞都统一遵循法大大内部漏洞处理流程，统一录入SIEM 评估漏洞对法大大产品和业务的影响，根据评定的漏洞等级采取应急响应和修复处理措施。其中法大大承诺严重、高危漏洞会在三个工作日内修复。所有的漏洞记录在内部漏洞管理平台中，进行跟踪和统计。

4.2 安全运维

4.2.1 授权与访问控制

法大大基于员工的工作岗位和角色，遵循最小权限管理和职责分离的原则授予不同角色有限的资源访问权限。

关键岗位员工录用前都经过背景调查，并签署保密协议、关键岗位责任书、个人信息隐私保护责任书，重要操作实行双人作业，互相监督机制，防止误操及恶意操作时间的发生。

完全隔离开发与生产环境，研发人员及普通系统权限管理人员无权限访问生产系统；对生产环境进行更新、升级及加固等操作严格遵循变更管理流程，提前提交变更申请，逐级通过变更审批，并在测试环境测试通过，才有权对生产环境进行更新、升级及加固等操作，所有的变更申请和记录将会归档保存。

管理人员在平台系统中所做的操作均会被系统管理员日志记录，管理人员无权修改和删除该管理员日志记录，操作完成之后，相关操作记录将会导出保存留证；完成之后需要提交操作报告，有专人核对操作记录，是否与系统记录的操作内容相匹配。

4.2.2 专线与 VPN

法大大平台跨云端服务的通信链路使用专线及 VPN 加密传输，通过传输链路加密通道将跨云端服务安全可靠地连接起来。VPN 账号的申请遵循内部特殊账号权限申请审批流程，确保一人一账号且符合岗位和业务需求。

4.2.3 堡垒机

为保障法大大平台安全稳定的运行，法大大使用堡垒机筑起入口的第一道围墙，隔绝未经授权登录系统的用户。堡垒机登录具备双因素认证，做到三个统一：统一运维入口，统一自然人与主机帐号间的权限关系，统一运维操作审计管控点。

4.2.4 数据库安全运维

为了提升数据库日常运维管理工作的精细度及安全性，法大大部署了数据库安全运维系统对异常操作行为进行管控和敏感数据进行掩码处理，实现敏感数据动态遮蔽，防止内部运维人员泄露敏感数据。数据库安全运维系统可以防范来自内部（如 DBA、运维等）对数据库的威胁，同时也可以阻断来自外部对数据库的注入操作。这些威胁包括账号滥用、权限过大、误操作、缺乏敏感数据访问管控等。

4.2.5 数据库审计

法大大通过部署数据库审计记录数据库所有操作行为，并可通过规则设置，对可能的风险行为及时告警和阻断。当有安全事件发生时，可以追根溯源，查找到相关责任人；同时有效覆盖监管部门对数据库安全方面的合规要求（如网络安全法、数据安全法、个人信息保护法、网络安全等级保护基本要求）。

4.2.6 日志留存

法大大严格按照《中华人民共和国网络安全法》第二十一条（三）“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”的规定，相关系统日志留存至少六个月以上，且历史日志保留存档。

4.2.7 备份管理

根据业务和数据需求，法大大制定了备份策略，实现同城备份、异地灾备等备份方案；对备份

数据进行加密存储，并会定期验证备份有效性。

数据库备份通过对数据库日志的实时增量获取，实现数据的实时备份，通过实时增量备份可以实现秒级 RPO 的备份解决方案。

4.2.8 变更管理

法大大内部制定了操作安全管理程序，严格控制系统变更的各个环节，系统变更人员需遵循变更管理流程，提前提交变更申请，逐级通过变更审批，并在测试环境测试通过，才能对生产环境进行更新、升级及加固等操作，所有的变更申请和记录将会归档保存。

变更完成之后需要提交操作报告，由专人核对操作记录，是否与系统记录的操作内容相匹配。

4.2.9 配置管理

配置管理是保障产品完整性、一致性、可追溯性的重要活动，法大大配置管理分为配置管理规划、配置项识别、配置变更管理、配置状态跟踪、配置活动报告、配置审查、构建管理、发布管理、第三方软件和开源组件管理、版本库管理等。

法大大设置了一系列的流程和技术工具手段来开展配置管理活动，确保交付产品的完整性，包括产品中涉及的第三方软件和开源软件。

4.2.10 账号权限复查

法大大内部会定期/不定期对账号权限进行复查，各个系统的管理员会定期或在任何变更之后（例如调岗、离岗、角色更换），对系统账号的访问权限进行复查。根据复查的结果，各个系统的管理员遵循最小权限原则重新分配用户的访问权限。

4.2.11 MFA 多因素认证

MFA 多因素认证是通过增加至少一个除口令之外的验证因子到身份验证过程，验证因子可以是拥有的东西，如智能卡或令牌；或者你具备的东西，如指纹或其他生物识别信息。MFA 的目的旨在建立一个多层次的安全登录防御系统，将多个身份认证因素结合起来为账号登录和资源访问提供更高的安全保护。

法大大关键系统账号如云账号、堡垒机账号、后台系统账号等都启用了 MFA 多因素认证，相关人员登录系统时除了需要输入账号和口令外，还需要输入移动设备接收的随机验证码，验证账号登

录是授权的实体，保障系统登录安全。

5 安全软件开发生命周期 SDLC

法大大参考 ISO27034 设计了一套符合电子签名行业的安全软件流程和框架，践行安全左移发展方向，将问题遏制在早期和前端，节省大量的后期补救成本。法大大安全软件开发生命周期（SDLC）主要分六个部分。

5.1 安全培训

法大大针对产品、开发、测试人员进行定期的安全能力和意识培训并进行考核，从而帮助相关人员持续加深对软件安全威胁的认知与理解，形成法大大团队的安全文化。

5.2 需求分析

法大大安全人员利用自身丰富的攻防经验，从业务的角度思考安全风险和合规性风险数据安全风险，通过对业务的需求理解，在需求分析阶段引入最合适的安全需求，跟随需求同步开发，使系统具备一定的安全功能提高整体的安全性。

5.3 软件设计

在设计阶段，法大大安全人员会同相关部门进行风险分析、威胁建模，仔细思考系统的安全设计和用户隐私问题，在此阶段确保系统满足机密性、完整性、可用性要求。以最严格的要求自律，在设计阶段从架构、功能设计层面，制定对应的缓解措施。在产品的需求评审阶段，法大大安全人

员会跟产品开发的相关人员确定安全质量要求和隐私要求。

5.4 程序编码

法大大内部制定了严格的安全编码规范，在开发过程中有章可循，同时也会利用 CI/CD 流水线中的代码扫描工具用以快速、准确的查找代码中的缺陷。编码规范包含安全的多个方面，从不同的角度描述了系统开发时应执行的安全操作。通过日常的安全培训，使得开发人员能够熟知例如 OWASP Top 10，CWE/SANS Top 25 等国际主流的标准，更快速开发出安全的代码。

5.5 软件测试

法大大安全测试分为黑盒、灰盒、白盒测试，利用不同的扫描检测引擎，自动化结合手工的方式，分别从代码，第三方组件，配置，应用等层面进行安全测试。同时也会对安全需求进行验证，确保需求安全有效可控。

法大大同时还会定期邀请第三方知名安全公司以及众测平台做渗透测试，通过尽可能多的进行渗透测试，最大限度的减少业务风险以保持安全风险在可控范围内。

5.6 发布/维护阶段

法大大内部严格执行变更、发布、配置管理、维护等方面的流程，能够确保在应用发布到维护及报废阶段的安全有效落地。

6 信息安全资质介绍

6.1 ISO27001 国际信息安全管理体系认证

ISO27001 作为信息安全管理领域的权威标准，是全球业界一致公认的辅助信息安全治理的手段。也是目前国际上最严谨、最被广泛接受和应用的信息安全领域的体系认证标准。法大大作为业内首批获得 ISO27001 国际信息安全管理体系认证的电子合同服务提供商，表明法大大建立了一套完整的、科学有效的信息安全管理体系来保障公司的信息安全。

bsi.

Certificate of Registration

信息安全管理体系 - ISO/IEC 27001:2013

兹证明：

深圳法大大网络科技有限公司
中国
广东省
深圳市深港合作区
南山区南山街道
桂湾五路123号
前海大厦T2栋13层
邮编：518052

Shenzhen Fadada Internet Technology Co., Ltd.
13F, T2 Building, Qianhai Building
No. 123 Gui Wan Fifth Road
Shenzhen-Hong Kong Cooperation Zone
Nanshan Street, Nanshan District
Shenzhen
Guangdong
518052
China

持有证书： **IS 702640**

并运行符合 ISO/IEC 27001:2013 要求的信息安全管理体系，认证范围如下：

提供互联网电子合同平台服务，包括软件开发、运维和客户服务。
这与2023年11月28日版本V1.0的适用性声明相一致。
注册地址：深圳市福田区梅林街道孖岭社区凯丰路10号翠林大厦26层01-5
The provision of electronic contract platform via internet, including software development, operation & maintenance and customer services.
This is in accordance with the Statement of Applicability version 1.0, dated Nov. 28, 2023.
Registration address: 01-5, 26F, Cuilin Building, No. 10 Kaifeng Road, Maling Community, Meilin Street, Futian District, Shenzhen

BSI代表：

Michael Lam - Managing Director Assurance, APAC

首次发证日期： 2016-01-27
最新发证日期： 2023-12-20

生效日期： 2022-01-27
有效期至： 2025-01-26

Page: 1 of 2

...making excellence a habit.™

此证书以电子版本方式发放，所有权属BSI并受合同条款的约束。
可以 在线 查询电子证书的有效性
打印的证书可以通过网站 http://www.bsi-global.com/ClientDirectory或者致电 +86 10 8507 3000 查询。
本证书信息亦可在国家认证认可监督管理委员会官方网站 (www.cnca.gov.cn) 上查询。
关于证书范围及 ISO/IEC 27001:2013 要求的适用性的进一步说明请咨询BSI。
获证组织必须定期接受监督审核并经审核合格此证书方继续有效。
此证书只在提供完整正本时才有效。

信息查询及联系方式：BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. 电话：+44 345 080 9000
BSI保证英国有限公司，注册地英国，注册号码7805321，地址：389 Chiswick High Road, London W4 4AL, UK
英标管理体系认证（北京）有限公司 北京市建国门外大街甲24号东海中心2008室 邮编：100004 电话：+86 10 8507 3000
BSI集团公司成员。

6.2 ISO27018 国际公有云个人信息保护管理体系认证

ISO27018 是关于公有云个人信息保护管理体系认证，它是一个行业内标准，所以又称“云隐私保护认证”。法大大作为第三方的云服务提供商，有责任有义务保障云端用户的数据和隐私安全，而 ISO27018 标准为云端个人信息和隐私保护提供了实施准则和指引，作为 ISO27001 在数据和隐私保护层面的延伸和拓展，不仅顺应了当前国内外个人信息和隐私保护的法律法规要求，也强化了法大大现有信息安全体系，标志着法大大高度重视用户个人信息和隐私保护，提升了法大大整体的

信息安全水平。

bsi.

Certificate of Registration

公有云个人信息保护管理体系 - ISO/IEC 27018:2019

兹证明：

深圳法大大网络科技有限公司
中国
广东省
深圳市深港合作区
南山区南山街道
桂湾五路123号
前海大厦T2栋13层
邮编：518052

Shenzhen Fadada Internet Technology Co., Ltd.
13F, T2 Building, Qianhai Building
No. 123 Gui Wan Fifth Road
Shenzhen-Hong Kong Cooperation Zone
Nanshan Street, Nanshan District
Shenzhen
Guangdong
518052
China

持有证书： **PII 702638**

并运行符合ISO/IEC 27018:2019控制要求的公有云个人信息保护管理体系，认证范围如下：

提供互联网电子合同平台服务，包括软件开发、运维和客户服务。
这与2023年11月28日版本V1.0的适用性声明相一致。
（关联ISO 27001证书编号IS 702640）
注册地址：深圳市福田区梅林街道孖岭社区凯丰路10号翠林大厦26层01-5
The provision of electronic contract platform via internet, including software development, operation & maintenance and customer services.
This is in accordance with the Statement of Applicability version 1.0, dated Nov. 28, 2023.
(ref. ISO 27001:2013 certificate number IS 702640)
Registration address: 01-5, 26F, Cuilin Building, No. 10 Kaifeng Road, Maling Community, Meilin Street, Futian District, Shenzhen

BSI代表：

Michael Lam - Managing Director Assurance, APAC

首次发证日期： 2019-01-27
最新发证日期： 2023-12-20
生效日期： 2022-01-27
有效期至： 2025-01-26

Page: 1 of 1

...making excellence a habit.™

此证书以电子版本方式发放，所有权属BSI并受合同条款的约束。
可以 在线 查询电子证书的有效性
打印的证书可以通过网站 http://www.bsi-global.com/ClientDirectory或者致电 +86 10 8507 3000 查询。
关于证书范围及 ISO/IEC 27018:2019 要求的适用性的进一步说明请咨询BSI。
此证书只在提供完整正本时才有效。

信息查询及联系方式：
和标管理体系认证（北京）有限公司 北京市建国门外大街甲24号华海中心2008室 邮编：100004 电话：+86 10 8507 3000
BSI集团公司成员。

6.3 ISO27701 国际隐私信息管理体系认证

ISO27701 是全球首个隐私信息管理的国际标准，由国际标准化组织(ISO)和国际电工委员会(IEC)于 2019 年 8 月联合发布,旨在帮助组织机构保护和控制所处理的用户个人信息，取得该资质意味着组织在处理用户信息与隐私保护符合全球统一标准要求，目前这一认证也是业内最具权威性的隐私管理体系建设指导标准。ISO27701 标准将隐私保护的原则、理念和方法融入到信息安全管理体系中，为保障用户数据和隐私安全的同时也增强法大大与客户、合作伙伴、投资、监管机构等的

相互信任。

bsi.

Certificate of Registration

隐私信息管理体系 - ISO/IEC 27701:2019

兹证明：

深圳法大大网络科技有限公司
中国
广东省
深圳市深港合作区
南山区南山街道
桂湾五路123号
前海大厦T2栋13层
邮编：518052

Shenzhen Fadada Internet Technology Co., Ltd.
13F, T2 Building, Qianhai Building
No. 123 Gui Wan Fifth Road
Shenzhen-Hong Kong Cooperation Zone
Nanshan Street, Nanshan District
Shenzhen
Guangdong
518052
China

持有证书： PM 729435

并运行符合ISO/IEC 27701:2019要求的隐私信息管理体系，认证范围如下：

请见认证范围页

BSI代表：

Michael Lam - Managing Director Assurance, APAC

首次发证日期： 2020-09-02
最新发证日期： 2023-12-20

生效日期： 2022-01-27
有效期至： 2025-01-26

Page: 1 of 2

...making excellence a habit.™

此证书以电子版本方式发放，所有权属BSI并受合同条款的约束。
可以 在线 查询电子证书的有效性
打印的证书可以通过网站 http://www.bsi-global.com/ClientDirectory或者致电 +86 10 8507 3000 查询。
关于证书范围及 ISO/IEC 27701:2019 要求的适用性的进一步说明请咨询BSI。
此证书只在提供完整正本时才有效。

信息查询及联系方式：BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. 电话 +44 345 080 9000
BSI保证英国有限公司，注册地英国，注册号码7805321，地址：389 Chiswick High Road, London W4 4AL, UK
BSI集团公司成员。

6.4 ISO22301 国际业务连续性管理体系认证

ISO22301 业务连续性管理标准是全球首个业务连续性管理(BCM)的国际标准，是衡量组织业务连续性服务能力和社会责任的唯一标准，旨在通过一系列的业务影响分析和风险评估活动识别出组织的关键业务流程，辨别和分析影响组织关键业务流程的潜在风险和威胁，针对潜在的风险及威胁建立一套预案机制，快速响应及恢复组织关键业务流程，确保组织业务的连续性、可用性。业务连续性管理体系是法大大能够为用户持续提供更成熟和更高质量的产品及服务的最高级保障，也是

法大大承诺客户满足业务可用性的最佳证明。为用户智选可靠、信赖、有韧性的电子签约平台提供了强有力的依据。

bsi.

Certificate of Registration

业务连续性管理体系 - ISO 22301:2019

兹证明：

深圳法大大网络科技有限公司
中国
广东省
深圳市深港合作区
南山区南山街道
桂湾五路123号
前海大厦T2栋13层
邮编：518052

Shenzhen Fadada Internet Technology Co., Ltd.
13F, T2 Building, Qianhai Building
No. 123 Gui Wan Fifth Road
Shenzhen-Hong Kong Cooperation Zone
Nanshan Street, Nanshan District
Shenzhen
Guangdong
518052
China

持有证书： **BCMS 736123**

并运行符合 ISO 22301:2019 要求的业务连续性管理体系，认证范围如下：

提供中国境内地区互联网电子合同平台服务，包括软件开发、运维和客户服务。
注册地址：深圳市福田区梅林街道孖岭社区凯丰路10号翠林大厦26层01-5
The provision of electronic contract platform via internet, including software development, operation & maintenance and customer services in China domestic areas.
Registration address: 01-5, 26F, Cuilin Building, No. 10 Kaifeng Road, Maling Community, Meilin Street, Futian District, Shenzhen

BSI代表：

Michael Lam - Managing Director Assurance, APAC

首次发证日期： 2021-01-19
最新发证日期： 2023-12-18

生效日期： 2024-01-19
有效期至： 2027-01-18

Page: 1 of 1

...making excellence a habit.™

此证书以电子版本方式发放，所有权属BSI并受合同条款的约束。
可以 在线 查询电子证书的有效性
打印的证书可以通过网站 http://www.bsi-global.com/ClientDirectory或者致电 +86 10 8507 3000 查询。
关于证书范围及 ISO 22301:2019 要求的适用性的进一步说明请咨询BSI。
此证书只在提供完整证书时才有效。

信息查询及联系方式：BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. 电话：+44 345 080 9000
BSI保证英国有限公司，注册地英国，注册号码7805321，地址：389 Chiswick High Road, London W4 4AL, UK
BSI集团公司成员。

6.5 网络安全等级保护测评三级

2017 年 6 月国家开始正式实施《网络安全法》，规定国家实行网络安全等级保护制度。为贯彻《网络安全法》的实施随即出台了信息系统备案和等级保护测评。等级保护测评是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，对各机构的信息系统安全等级保护状况进行认可及评定。法大大积极响应国家的法律法规和监管合规要求，早在国家《网络安全

法》发布之前就已备案申请并对标等保三级的标准和条款要求，并从 2016 年起连续多年高分通过信息系统安全等级保护三级测评，三级属于“监管级别”，需每年由拥有测评资质第三方机构开展年度测评，确保法大大平台持续满足等保的三级标准要求。

深圳市网络安全等级保护测评结果通知书

编　号：SZCP202301573

依据《信息安全等级保护管理办法》等有关规定，深圳法大大网络科技有限公司已按规定开展2023年度等级保护测评工作。

特此通知

测评系统信息：

1、法大大电子合同缔约平台系统，三级，良。

深圳市信息安全等级保护工作协调领导小组办公室

2023 年 10 月 20 日

测评机构：深圳市网安计算机安全检测技术有限公司

测评日期：2023.07.18-2023.09.26

6.6 数据安全管理能力认证（DSMC）

数据安全管理能力认证（DSMC）是由中国信息通信研究院联合认证机构面向全行业发起的数据安全领域的国家级权威认证。本项认证依据《数据安全法》、《个人信息保护法》等相关法律法规、政策、标准，从合规角度出发，对数据安全制度落地要求、技术落地要求两大维度共计 15 项指标进行评估。法大大于 2023 年 7 月取得证书，是行业内首家获颁该证书的企业。认证通过充分表明了法大大的数据安全管理能力及技术能力已达到较高水平，实现了数据安全风险的整体可控与合规保障。

注册号：03023DSMC10110ROM

TLC

数据安全管理能力认证证书

Certificate for Data Security Management Capability

兹证明

深圳法大大网络科技有限公司

注册地址：广东省深圳市福田区梅林街道孖岭社区凯丰路10号翠林大厦8层805室

统一社会信用代码：914403003195749464

数据安全管理能力符合

TLC030-2021 《数据安全管理能力技术规范》

本证书覆盖范围

电子合同业务涉及的数据安全管理活动

认证地址：广东省深圳市南山区南山街道桂湾五路123号前海大厦T2栋13层

发证日期：2023年07月11日

证书有效期至：2026年07月10日

（首次颁证日期：2023年07月11日）

（本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）或泰尔认证中心有限公司官方网站（www.tlc.com.cn）上查询；首次颁证日期指TLC030-2021版标准实施后的颁证日期;获证组织必须定期接受监督审核并经审核合格此证书方继续有效）

泰尔认证中心有限公司

TL Certification Centre Co.,Ltd.

签发人：

Signer by

CAICT 中国信通院

卓信大数据计划

扫码关注"泰尔认证"微信公众号，获取更多信息。

中国·北京·西城区新街口外大街28号 100088 http://www.tlc.com.cn/

6.7 可信云企业级 SaaS 评估

可信云企业级 SaaS 认证是中国信息通信研究院（工信部电信研究院）测试评估的面向云计算服务产业的认证，是我国唯一针对云计算信任体系的权威认证，法大大于 2018 年取得“可信云”认证。可信云认证通过官方发布 SLA(服务等级协议）披露法大大的数据存储持久性、数据私密性、故障恢复能力、服务可用性等多方面指标均满足可信云服务认证要求，实现了对用户服务的透明化，为用户选择安全、可信的云服务商提供了重要依据。

TTL泰尔实验室　　CAICT 中国信通院

证书编号：IY2023200093
报告编号：V23Y20093

TRUCS 可信云服务评估

企业级SaaS服务能力检验证书

深圳法大大网络科技有限公司
深圳市福田区梅林街道孖岭社区凯丰路10号翠林大厦8层805室

兹 证 明

深圳法大大网络科技有限公司

法大大电子合同缔约平台

产品版本：V5.0

通过Q/KXY S001—2014《云计算服务客户信任体系能力要求 第4部分：企业级SaaS服务》标准的检验

符合性描述：

"经中国信息通信研究院的检验，贵单位的**法大大电子合同缔约平台V5.0**通过了Q/KXY S001—2014《云计算服务客户信任体系能力要求 第4部分：企业级SaaS服务》标准能力的检验，达到企业级SaaS服务能力评估的要求，特发此证。"

（证书有效性信息及详情可见www.kexinyun.org.cn及可信云服务号。由于该检验是针对2023年7月30日前该产品/服务情况进行披露，用户依然应留意在具体使用过程中可能发生的风险。因云计算软件等技术快速发展、产品/服务不断升级迭代、标准规范随行业发展不断更新等原因，当产品或检验标准发生较大变化时，建议本产品/服务进行重新检验。中国信息通信研究院将在2024年7月组织新一批检验。）

授权签字人：

签发日期：2023年7月30日

云计算开源产业联盟
地址：北京市海淀区花园北路52号
网址：https://www.kexinyun.org.cn/

中国泰尔实验室
中国信息通信研究院
地址：北京市海淀区花园北路52号
网址：http://www.caict.ac.cn/

6.8 商用密码产品认证证书

2019 年法大大通过由国家密码局商用密码组织的产品检测及专家鉴定，获得了由该局颁发的《商用密码产品型号证书》。2020 年法大大根据《国家密码管理局市场监管总局关于调整商用密码产品管理方式的公告》，将《商用密码产品型号证书》换发为《商用密码产品认证证书》。商用密码是指采用密码技术对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的一种密码技术和密码产品。产品认证历经商用密码检测中心的安全测试、现场审核及专家答辩。整个产品检测及鉴定程序比较复杂，对产品的密码算法和相关安全技术规范要求也是非常之严格，能够取得认证，

意味着法大大产品赢得了经国家密码最高管理机构认可，无论是产品技术上、安全性设计上以及密码算法上都符合国家相关的密码技术规范，这不仅仅有利于法大大持续开发有商密资质需要的产品，也为法大大自主研发产品在商用密码的推广及应用提供了强有力的保证。

商用密码产品认证证书

证书编号：GM004419920201437

委托人名称及所在地

深圳法大大网络科技有限公司
深圳市福田区梅林街道孖岭社区凯丰路 10 号翠林大厦 26 层 01-5

生产者（制造商）名称及所在地

深圳法大大网络科技有限公司
深圳市福田区梅林街道孖岭社区凯丰路 10 号翠林大厦 26 层 01-5

生产企业名称及所在地

深圳法大大网络科技有限公司
深圳市南山区南山街道桂湾五路 123 号前海大厦 T2 栋(1201 室、13 层、14 层)

原商用密码产品型号证书批准型号

SFT1914 电子签章系统（原证书编号：SXH2019309 号）

依据商用密码产品型号证书换发。

颁发日期：2023 年 12 月 6 日　　有效期至：2024 年 6 月 19 日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

牛路宏

国家密码管理局商用密码检测中心

中国·北京·万丰路300号　www.scctc.org.cn 证书通过此网站查询

6.9 云安全联盟大中华区会员单位

云安全联盟大中华区（Cloud Security Alliance Greater China Region，缩写“CSA GCR”）是在香港注册的独立、中立、权威的非营利性组织，也是全国首家在公安部注册备案的网络安全类国际 NGO。CSA GCR 立足于中国，专注于下一代数字安全的前沿技术标准研究与产业最佳实践，

作为国际桥梁联接世界，致力于构建国际网络安全的生态体系。法大大于 2022 年 7 月申请加入云安全联盟大中华区 CSA GCR，与 CSA GCR 共同参与标准制定、行业研究、学术交流及人才培养等活动，不仅促进对云计算安全与下一代数字安全的最佳实践的前沿研究，还有利于正确推广云安全和网络信息安全解决方案。