



# 安全白皮书

V1.0



|                    |    |
|--------------------|----|
| 前言 .....           | 01 |
| 安全术语 .....         | 01 |
| 1. 安全文化            |    |
| 1.1 安全理念 .....     | 02 |
| 1.2 社会责任 .....     | 02 |
| 2. 安全防护            |    |
| 2.1 前端安全 .....     | 03 |
| 2.2 数据传输安全 .....   | 03 |
| 2.3 服务端安全          |    |
| 2.3.1 流程安全 .....   | 03 |
| 2.3.2 数据库安全 .....  | 03 |
| 2.3.3 中间件安全 .....  | 04 |
| 2.4 物理安全 .....     | 04 |
| 2.5 数据安全           |    |
| 2.5.1 数据产生 .....   | 04 |
| 2.5.2 数据传输 .....   | 04 |
| 2.5.3 数据使用 .....   | 05 |
| 2.5.4 数据存储 .....   | 05 |
| 2.5.5 数据销毁 .....   | 05 |
| 2.5.6 数据安全审计 ..... | 05 |
| 2.6 安全运营 .....     | 05 |
| 3. 安全合规            |    |
| 3.1 体系建设 .....     | 06 |
| 3.2 审计廉政 .....     | 06 |
| 总结 .....           | 06 |

## 前言

人力家是一个专业的互联网人力资源服务平台，始终坚持技术驱动，为用户提供便捷、安全的HRSaaS服务。自2018年面世以来，经过不断锤炼，已经建立起完整的技术生态体系，累计为数万家企业提供稳定、可靠的服务。

为加强公众对人力家安全的认知，本文重点从安全文化、安全防护、安全合规三大维度，全面阐述人力家的安全技术及实践方法，旨在向全社会披露人力家极力加强安全防范、努力保障客户合法权益的决心。

## 安全术语

**ECS:**是钉钉云提供的云服务器的简称，是一种弹性可伸缩的计算服务。

**RDS:**是钉钉云提供的一种稳定可靠、可弹性伸缩的在线数据库服务。基于飞天分布式系统和全SSD盘高性能存储，支持MySQL、SQL Server、PostgreSQL、PPAS(高度兼容Oracle)和MariaDB引擎，默认部署主备架构且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案。

**DSMM:**阿里巴巴牵头制订的数据安全成熟度模型(Data Security Maturity Model)该标准从组织建设、人员人力、制度流程、技术工具等四个维度对数据安全生命周期提出了明确的安全要求和度量体系。

**HTTPS:**超文本传输安全协议，以安全为目标的HTTP通道，简单理解为安全的HTTP。**AES:**高级加密标准(Advanced Encryption Standard)，在密码学中又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。

## 1. 安全文化

### 1.1 安全理念

人力家始终坚持创新、速度、满意的价值观和聪明、乐观、皮实、自我驱动的人才理念，这些方面首先会体现在员工招聘上，通过电话沟通、现场面试、交叉面试等方式，在进入人力家的第一道程序上就做了严格的筛选。

员工入职时，必须签署劳动合同和保密协议，并进行安全方面的培训。工作过程中，会定期进行安全培训和进行《商业行为准则》考试；

员工离职后，会对其信息资产进行回收，并关闭所有相关的应用权限，保证离职不会带走任何保密数据。同时对于敏感岗位要签署竞业协议并开展离职审计。

对于任何违反安全规范的行为，严格依据员工纪律条款进行处理，必要时追究法律责任。

### 1.2 社会责任

人力家自成立起，已经为数万家企业提供在线服务，未来还会有更多的企业加入进来。我们抱着合作、创新、开放的态度，希望能打造一个高效、透明、有温度、安全的人力资源服务平台，为中国4300万家中小企业提供专业、放心的服务。

## 2. 安全防护

人力家所有产品都建立在钉钉之上，不论钉钉管理后台、钉钉移动端还是钉钉PC端，都依托钉钉强大、稳定的基础设施。在这之上，我们建立起了一套完整独立的安全防护体系，确保用户安全地使用产品。

## ● 2.1 前端安全

人力家产品一方面是基于钉钉容器的H5应用，钉钉APP本身会做各个方面的安全检测，包括:应用完整性、环境可信性、数据机密性、账号安全性。基于这些检测，可天然抵御来自病毒、模拟器、越狱等行为攻击;另一方面是基于普通浏览器的WEB应用，利用钉钉开放平台的免登机制，无需输入钉钉用户名和密码，自动获取当前用户身份，进而登录系统，流程更方便、更安全。

## ● 2.2 数据传输安全

人力家已实现全站部署HTTPS证书，所有前后端数据传输都采用SSL/TLS协议，保证数据不被窃听、篡改。

## ● 2.3 服务端安全

### 2.3.1 流程安全

人力家所有产品迭代都准守《安全开发生命周期》准则。在需求分析阶段，会根据产品功能进行需求安全分析，避免产品本身产生安全漏洞;在技术设计阶段，会有专门的技术委员会一起讨论方案，必要时邀请安全工程师参与讨论，避免在技术架构上出现安全漏洞;在产品开发阶段，会要求所有开发工程师都安装阿里巴巴代码扫描插件，保证代码编写符合《阿里巴巴Java开发规范》。在产品测试阶段，会仔细、严格的进行权限、敏感数据等检测，避免开发过程中产生的安全风险;在产品发布阶段，首先会进行一系列上线前检查，包括代码review，黑白盒测试;在线上运营阶段，会定期通过钉钉云的云盾进行漏洞扫描、渗透测试，发现可疑风险，立即进行分析、处理。

### 2.3.2 数据库安全

人力家使用钉钉云专业数据库RDS，高效、稳定、可靠，可弹性扩展，主备部署。具备自动容灾、备份、恢复、监控、迁移等方面的所有功能。

### 2.3.3 中间件安全

人力家服务端使用全套钉钉云开放中间件，包括分库分表、统一配置、消息队列、缓存等。全部采用分布式架构，稳定、可靠。同时，所有控制台访问都基于钉钉云RAM权限控制体系，高度隔离。

## ● 2.4 物理安全

人力家所有系统都架设在钉钉云之上，而钉钉云则建立在阿里巴巴集团强大的物理设施之上，所以人力家天然具备稳定、可靠的物理设施；同时，人力家所有主机都使用钉钉云ECS，通过建立独立的安全组，实现端口级别的出入网访问控制；人力家使用钉钉云VPC网络，与其他网络隔离，可自定义IP地址范围、网段、路由表和网关等，通过构建内网环境提高了安全水位。

## ● 2.5 数据安全

人力家非常重视客户数据安全，在日常运营过程中严格遵守DSMM规范，在数据的完整生命周期内都严格遵守阿里巴巴集团的安全管控措施，确保用户数据的机密性、完整性。

### 2.5.1 数据产生

人力家制定数据安全规范，按照数据类型、敏感程度、使用价值等方面属性定义数据安全标准，在数据产生时对数据进行打标，在数据流转过程中按照安全等级实行分类管控，分级授权。

### 2.5.2 数据传输

人力家已实现全站部署HTTPS证书，所有前后端数据传输都采用SSL/TLS协议，保证数据不被窃听、篡改。内部应用间调用全部通过内部安全高速通道，大大降低了数据外泄风险。

### 2.5.3 数据使用

客户数据只属于客户，只限客户自己在产品中使用，未经客户授权的敏感数据任何人无法使用。生产环境数据库由专人操作，敏感数据全部加密存储，禁止任何人、以任何形式进行查看、下载。

### 2.5.4 数据存储

客户数据只属于客户，人力家只是在保证产品可用的情况下进行暂存。人力家敏感数据全部使用独立密钥进行加密，使用AES加密算法，密钥严格管理且和数据隔离存储，即使是员工也无法查看客户敏感数据。

### 2.5.5 数据销毁

对于产品层面不再使用的数据，我们会参照DoD5220.22-M、NIST800-88标准及时进行清理，避免数据泄露风险。

### 2.5.6 数据安全审计

人力家不允许将客户敏感数据进行导出及下载，所有系统操作都会记录操作日志并定期审查，发现异常行为立即警告处理。

## ● 2.6 安全运营

人力家使用钉钉云云盾进行安全防护，定期进行漏洞扫描、渗透测试等等，发现风险点及时处理。同时，基于钉钉云云监控构建出完整的一套监控及报警方案，一旦出现问题，立即通过钉钉、短信等方式通知相应负责人。

## 3. 安全合规

### ● 3.1 体系建设

根据《中华人民共和国网络安全法》要求，参考ISO27001、ISO27018以及信息安全等级保护等国内外标准和最佳实践，人力家建立了覆盖产品安全、组织及人员安全、研发安全、运行安全的安全体系。在各个方面做出了明确规定，例如:对外数据披露流程，个人设备使用规范，网络存储使用规范，研发代码规范等等。

### ● 3.2 审计廉政

随着人力家业务不断发展，安全建设工作挑战越来越大。一方面我们会定期进行操作日志、员工敏感 行为审计;另一方面我们不断完善员工制度，定期进行《商业行为准则》、《安全红线》培训及考试认证。发现违规行为严肃处理，轻则警告处分，重则开除永不录用，必要时追究法律责任。

## 总结

随着人力家不断壮大，我们深知肩上的责任重大。我们会不断进行创新、探索前沿技术，加强安全体系建设。同时，我们会不断完善安全规范，加强员工安全意识，以应对日益复杂的互联网环境，人力家会在安全建设的道路上不断努力、不断挑战!