115 产品信息安全白皮书

广东一一五科技股份有限公司

目录

前言

广东一一五科技股份有限公司(简称“115科技”)，是国内率先从事云存储研发的科技企业，旗下云存储系列项目的研发于2008年启动，2011年6月成立公司。通过多年的自主研发创新，先后推出了系列云服务产品(下称“115产品”)，其中包含服务于个人用户的“115”以及服务于社群团体用户的“115管理”，致力于为个人及组织提供高可靠性和高安全性的云服务。

信息安全和用户隐私是115产品最重要的原则。115产品参照CSA云安全指南、信息系统安全等级保护第三级及ISO27001信息安全管理要求，建立了全面、严密的信息安全保障机制，在管理和技术上实施纵深防御体系，采取多重保护措施，保障用户信息安全。

基于十多年安全技术研究积累的成果，115科技力求打造业界一流的安全保障体系，以高效可靠的系统实现机制，为广大用户的信息安全提供全方位的安全保障！

115科技信息安全团队编写本安全白皮书，旨在通过对115产品的安全框架构建和安全技术应用等方面的全面阐述，让用户深入了解115产品的安全能力。

一、组织及人员安全

1.1 安全管理委员会

安全管理委员会成员由安全团队负责人、产品负责人、运维负责人及技术负责人组成，负责监督并决策115产品信息安全体系的建设，对115产品整体安全状况负责。

1.2 信息安全团队

信息安全团队由安全测试、安全运维、安全开发工程师组成，全面负责公司整体安全建设及安全运营工作，是115产品信息安全体系的建设者：

(1)根据信息安全管理制度，完善并制定相关安全流程、安全方案和安全策略，参与业务开发过程的安全规范制定及代码审核；

(2)借助公司的人才资源及技术沉淀，定期对公司所有的网站、系统、主机、网络进行安全评估、安全测试和渗透测试，对发现的问题制定解决方案，在预期时间内完成漏洞修复；

(3)负责接受各单位的紧急信息安全事件报告，组织进行事件调查，分析原因、涉及范围，并评估安全事件的严重程度，提出信息安全事件防范措施；

(4)对互联网领域的重大安全事件进行跟踪、分析，对突发型安全漏洞和安全事件进行7x24小时的应急响应和处理；

(5)保持关注和跟踪业界最新安全技术和安全动态，积累知识库；

(6)建设安全防御体系，完善运维安全体系和业务风控体系；

(7)设计、开发和运营相关安全系统，如漏洞扫描、入侵检测、攻击防护等；

(8)定期组织安全意识培训，普及安全知识，提升公司人员整体安全意识，主导公司信息安全文化的建设。

1.3 安全行为准则

1.3.1 尽职调查

在员工入职前，115科技在国家法律法规允许的情况下，根据岗位的需求对员工进行不同程度的尽职调查，通过一系列背景调查手段来确保每位入职的员工符合公司的行为准则、保密规定、商业道德和信息安全政策。

1.3.2 安全教育与培训

在员工入职后，115科技对员工进行行为准则、保密规定、商业道德和信息安全政策等培训，并

且，所有的员工必须签署保密协议，确认收到并遵守115科技的安全政策和保密要求，尤其关于用户信息和数据的机密性要求将在入职培训过程中被重点强调。

此外，115科技依据员工的工作角色进行额外信息安全培训，针对非技术员工进行安全经验、安全意识及相关安全法律法规的培训，全面加强公司安全管理水平；针对技术员工进行安全技术培训和安全意识培训，如基础安全攻防、Web安全技术、安全开发、安全编码规范、安全测试和安全运维等安全培训。

最后，115科技通过企业价值观考核的方式检验每位员工是否以诚信、敬业的态度来管理每位用户的云端数据，保证其对用户、合作伙伴和竞争对手的尊重。

1.3.3 安全生产

数据是115科技的生命，115产品服务器除了线上运维人员可拥有较高权限外，其他人员的账号会对功能权限进行最大限制。

员工管理的用户数据必须按照安全策略执行，数据运维人员操作或管理数据库前，需要先获得授权，运维人员对数据的所有操作均被审计，对于危险操作将进行告警。

1.4 安全违规问责

115科技已建立严密的网络安全责任体系，要求每位员工对自己的工作和工作成果负责，加强自律，严防网络安全问题发生。

一旦发生网络安全问题，不管是出于何种原因，115科技都会根据公司规章制度及有关法律法规规定，以行为和结果为依据对负责的员工进行问责，严重者追究相应法律责任。

此外，115科技提供机密报告机制以确保员工可以匿名举报任何违反安全政策、商业道德的事件。

二、产品安全

2.1 协议安全

基于SSL/TLS协议为应用程序提供数据保密性和完整性的基础上，115科技构建了一套完整的私有安全通信协议，通过加密用户在网络传输中的信息，以确保信息安全，防范通信过程中信息被侦听、窃取、篡改等，确保数据的机密性和完整性。

2.2 数据备份

115产品数据备份具备自动化、持续在线、实时的特点，让用户数据实现存储的高安全性和访问的高可用性：

首先，115产品数据以数据流方式存储，数据经过安全加密，确保了数据安全和隐私。；

其次，通过多主多从技术，对数据实现多重实时备份；接入阿里云作为基础设施供应商，其供全球部署、多地域多可用区的云数据中心，实现数据的异地备份和多重备份，确保了数据的完整性和可靠性；

最后，为进一步保障数据安全，115产品还实行离线数据备份，避免因恶意损坏等原因造成数据丢失或损毁。

同时，对于可在后台接收数据的人员进行严格管理，所有针对数据的操作均需要获得授权后方可进行，对所有人员均需要签订保密协议，以保障运维安全。

2.3 客户端加密

115产品客户端的数据库进行了整库加密存储，根据用户设备信息通过加密算法生成的唯一密钥，为用户客户端存储的敏感信息、隐私数据提供安全保障。

2.4 用户权限控制

2.4.1 115云盘服务

用户只能下载自己账号内的内容，其他用户无法访问其数据。

即便用户通过抓包工具获得文件的下载源地址，也会有动态校验机制，以确保用户的文件安全，防止被他人获取敏感信息。

2.4.2 115管理服务

115管理采用了高度的成员权限控制机制，成员权限采用加密存储，可分组分级进行管理，针对不同人群设置不同权限。同时组织创建者可以设置对重要分组进行保护，该分组的信息会自动隐

藏，即使是组织的成员，没有相应权限无法访问。对于不同组织的数据，存储空间是相互隔离的，当用户退出该组织后，会被踢出对应的组织，自动删除用户在该组织的权限。

访问权限的控制。用户在事务、日程、消息、圈子、资讯、文件、通讯录等频道可以通过灵活的权限进行信息访问的控制，满足组织沟通时的现实场景，只有拥有权限的信息才可被访问，一方面用户信息安全得以控制，另一方面也保障用户免受繁多的信息干扰。

115管理从业务层面提供溯源能力，如谁编辑过，谁经办过，谁删除过等，均会留下记录。

2.5 文件访问控制

115产品具备独立的访问控制鉴权功能。

115云盘服务对于用户上传的文件，其他账号在非授权情况下将无法访问。

115管理服务对于组织成员上传的文件，非本组织成员或非授权的本组织成员均无法进行访问。比如聊天会话中传输的文件也有相应的权限保证，只有参与该聊天的成员才能够查看对应文件，不在此聊天会话中的成员将无权查看。

115科技通过以上一系列措施保障用户文件访问的安全。

2.6 传输与存储安全

115科技对用户上传的所有数据采用分片以及SSL/TLS协议进行加密传输，数据在云端则采用物理隔离和分片存储双重保护手段，在确保速率的同时保障用户数据传输和存储安全。

115产品所有通信数据均可以通过安全的HTTPS或VPN通道进行传输，在数据被业务用户访问前，均需要完整鉴权信息，例如校验用户是否属于当前组织成员，校验用户是否属于当前会话组正式成员，校验用户是否有对应资源的访问权限等。

2.7 多端登录管理

为保障用户的账号安全，同一个账号只能同时登录同一个设备、同时只能在一个地点进行登录，否则后登陆的端将会将前登陆的端踢出，这种方式可保障用户在其他设备登录时进行预警。

用户可以在账号后台方便地管理自己账号在各类设备上的登录情况，如果存在异常登录情况，用户可以轻易地选择退出，可避免账号可能在其他设备上误登或忘记下线等情况，保障账号安全。具体示例如下图：

115产品提供详尽的用户登录日志，当用户发现账号登录异常时，可以采取如修改密码、加强防护等账号安全保障措施。

2.8 可信设备

115产品会对所有登录的用户进行设备认证，如果该设备没有通过认证则不允许登录，避免账号意外泄露时在其他设备上登录，造成信息泄露风险。用户可进行可信设备管理，可查看自己所有已信任的设备，若发现异常设备，可以在线进行登出处理。

可信设备认证需要经过账号或密码及手机验证码的认证，网站登录也需要手机端扫描二维码等方式进行登录。如果用户使用新的设备，则需要重新进行可信设备认证，以保障用户的账号安全。

2.9 防泄密

115管理支持“信息指纹”水印技术，对敏感信息设置肉眼不可见的隐藏水印，避免泄露后无法追踪溯源的窘境。并且对聊天相关窗口进行安全监控，对于用户触发的截图行为进行提示。

2.10 多因子身份验证

对于用户账号安全，115产品提供手势锁、指纹锁、安全密钥、两步验证等多种身份验证方式为用户账号安全保障提供多维度的选择，避免手机等移动设备借给他人使用时造成信息泄露。

三、数据安全

数据安全的首要任务是保障业务系统和应用程序的基础数据安全。依据数据安全生命周期，115产品从数据创建、存储、使用、共享、归档、清除到销毁，使用了数据分级、数据加密、身份验证和访问控制等措施，保障数据的可用性、保密性、和完整性。

3.1 数据分级

115科技对所有用户存储的数据实施数据等级保护策略，按照数据价值和敏感度对数据进行等级划分，根据数据安全进行分级，并制定对应的保护策略，对用户存储的数据进行全面的安全保护。

3.2 数据安全与加密方案

115产品采用国际高标准加密算法对用户的敏感数据进行加密存储，其中不同用户的数据采用的密钥均不一样，所有数据均有本地备份和异地备份以确保数据的安全性。

3.3 数据访问及用户授权第三方应用访问其敏感信息

115产品为用户数据提供访问控制保障。对涉及用户隐私或机密等敏感数据，115科技将严格控制权限申请，不开放第三方应用访问权限。

3.4 数据安全审计

安全审计覆盖用户所有数据活动的详细跟踪记录，从而实现对用户访问行为的主动控制，生成审计员所需要的信息。所有数据变更记录详细可见，如事务修改、权限变动、日程变更等，做到所有用户操作有踪可寻。

3.5 数据销毁管理

所有存储数据的存储介质(如硬盘等)，如若需要维修必需先进行卸载；需要报废或移出数据中心的网络设备及存储设备，进行清除数据以及物理销毁，进入资产回收处理流程。

四、应用与业务安全

4.1 安全开发流程

115产品在项目开发流程中引入了微软提出的软件安全开发生命周期(Security Development Lifecycle，SDL)，根据企业实际情况，在开发流程中的不同阶段融入安全环节，控制项目整体的安全风险。向上推动安全开发过程继续走到实现层，设计层，向下则是减少企业发布的产品暴露安全事件导致损失的风险。

微软SDL(Security Development Lifecycle)流程，是一种专注于软件开发安全保障的流程，以下为微软SDL流程框架图：

4.1.1 风险评估

在项目确立之前，安全人员需要提前与项目经理进行沟通，确定信息安全方面的具体要求和相关部署。并确认项目计划和里程碑，尽量避免因为安全问题而导致项目延期发布。

在需求分析和设计阶段，安全人员同时进行风险评估和威胁建模。

(1)安全风险评估(SRA)，包括以下信息：

①项目的哪些部分在发布前需要威胁模型；

②项目的哪些部分在发布前需要进行安全设计评析；

③项目的哪些部分需要进行渗透测试；

④是否存在安全顾问认为有必要增加的测试或分析要求已缓解安全风险；

⑤模糊测试要求的具体范围是什么等。

(2)威胁建模，包括以下信息：

①为项目或产品面临的威胁建立模型，明确可能来自的攻击有哪些方面；

②分别有标识资源、创建总体体系结构、分解应用程序、识别威胁、记录威胁和评价威胁等过程。

4.1.2 安全设计

在设计和实施流程中，技术人员使用自主研发的安全框架和模块进行程序开发，有效防止各种漏洞攻击；参考安全开发指导手册进行编码，如弃用不安全函数，禁用不安全的函数和API等；并针对安全问题的编码进行复查指导，如特定API函数的副作用，堆栈溢出错误等等；且较为重要的

业务系统融入安全代码审计的环节。

4.1.3 安全测试

115产品非常注重产品本身安全性，所有产品和业务系统上线前需经过安全团队的安全评估、安全检测和渗透测试，针对网页端和移动APP客户端进行安全把控，通过一系列黑/白盒测试和漏洞扫描，发现和修复潜在的安全漏洞和安全风险。

4.1.4 应急响应

对于线上的产品，有专门的团队负责定期的安全检测和bug跟踪处理，如果发生安全漏洞和安全事件，安全团队负责相关的应急响应工作，包括漏洞分析、事件溯源、安全处理和总结等。

4.2 业务安全

4.2.1 账号安全

在保障用户隐私方面，115产品提供多种安全措施保障用户信息不被窃取、滥用、盗用：

(1)115产品对用户注册、登录进行了多重保护，能够有效防止暴力尝试密码、破解账号、冒用账号等行为；

(2)账号安全体系依托口令策略和访问控制策略，禁用弱口令，监控非法登录尝试；

(3)对非常用设备的登录，需用户进行密码及手机验证码动态口令登录的双因素验证；

(4)除已有的风控体系外，115产品提供了相应的安全辅助功能，如二次验证、图形码验证、双因素认证、手势锁验证、指纹验证等方式，给用户账号安全保障提供更多维度的选择。

4.2.2 暴力破解&撞库

115产品账号基于可信设备判断是否进行二次验证，同时基于后端风控体系，实时监测账号破解、撞库与刷库等攻击行为，告警通知及处置恶意请求；

针对高频异常请求，登录地区变化等不正常行为，进行验证码介入拦截；主动防御系统根据实时日志系统统计分析出需要封禁的ip、uid，在调度之后加入过滤系统，根据分析结果对访问请求进行过滤。

4.2.3 风控体系

115产品使用自主研发业务安全系统对用户账号安全进行全天候监控：

(1)通过账号监测平台，对用户同设备批量尝试登录账号进行监控报警；

(2)对请求频次进行监控，如果多次失败的登录行为将进行访问限制；

(3)对IP信誉度较低或多次仅有登录尝试IP被认定为恶意IP进行封禁。如发现攻击行为，将进行预警，并将该设备ID、IP、账号拉至黑名单。

五、系统及网络安全

5.1 系统安全

5.1.1 系统基础安全配置

线上服务运行在可信安全的操作系统版本上，由运维人员从系统团队维护的可信安装源下载和安装应用软件和系统。

安全团队跟踪业界安全问题和安全漏洞，保持日常的安全渗透工作，评估服务器上的软件是否有安全漏洞，一旦发现存在安全漏洞，通过应急响应流程推动基础软件的漏洞修复。

对于通用的系统软件如nginx，ssh等，制定了对应的安全配置规范和安全加固措施。基础安全配置的主要内容有：

(1)最小权限化，禁用多余或危险的系统后台进程和服务；

(2)文件目录权限：对目录权限控制防止写入后门，如可写不可执行，可执行不可写；

(3)服务加固：对ssh等常用服务进行安全加固；

(4)系统授权和认证：禁止root远程登录；

(5)日志和审计：记录系统的服务、内核进程运行日志等；

(6)账号口令安全：启动登录失败重试次数、密码有效期和复杂度检查等。

5.1.2 人员权限管理

服务器上的账号依据权限大小，分为高中低三个用户组，除了线上运维人员可拥有较高权限的用户组外，普通员工只能申请低权限的用户组，线上服务也以低权限用户运行。对于高度敏感的操作环节，还需要同时取得多个权限组的密钥才可进入，以确保信息安全。

运维人员在开展日常工作时，还必须注意：

(1)对所维护管理的平台或者应用进行安全例行巡检和维护，比如安全加固、口令的定期修改、及时的补丁修补等；

(2)未经授权，不得改变生产环境中设施，设备和系统的用途；

(3)未经许可，不得尝试绕过系统的安全审计措施；

(4)未经许可，不得乱删除、修改和销毁系统日志记录。

(5)不得使用个人存储介质连接服务器；

5.2 网络安全

5.2.1 安全域划分

115产品的网络依据用途划分成办公、测试、生产等多个安全域，对于不同的安全域之间，除了部分经过安全加固的可信中间程序外，相互之间不能互访。

5.2.2 网络访问控制

115产品的各类服务，只有在经过安全团队审核之后，才能发布上线并对公众服务。高危端口和服务禁止对互联网开放。内部后台应用仅对办公网开放。重要后台启用双因子验证登录。

另外，内部的办公网络按部门进行划分和ACL的限制，以防止攻击者就会借助跳板在内网中进行弱口令扫描，发起ARP欺骗等。

5.2.3 HTTPS安全通信

HTTP协议是没有加密的明文传输协议，如果网站或APP采用HTTP传输数据，则会泄露传输内容，可能被中间人劫持，修改传输的内容。

为了防止用户的隐私数据在传输过程中被窃听或者泄露，115产品网站和移动客户端都已经启用https协议来代替http协议。

六、物理与环境安全

6.1 物理及设备安全与基础架构安全

115科技搭建了物理设备安全与基础架构安全，包括机房安全、服务器安全、网络设备安全等。115科技拥有完备的灾难与应急事件响应预案，并定期对预案进行演练、更新。同时，为应对灾难与应急事件，我们通过多项技术提前预防：多机房部署、多网络接入、数据在线备份、数据异地备份、数据离线备份、应用自动部署、应用自主恢复、统一运维管理、日志集中记录并分析等。

机房多活技术：115科技数据中心提供多处机房接入，提高机房可用性；

网络多活技术：115科技数据中心提供多线接入方式，国内、国外均可流畅访问；

数据存储多活：115科技在全国部署多个数据中心节点，在多异地机房备份有在线数据和离线数据，保障数据的可用性；

操作系统OS安全：115科技对于OS安全和网络安全进行实时监控，每日检查，所有OS操作、应用变更操作及DB操作均需要授权，并实时记录并转发至日志中心进行存储，实时展现日志，并对危险动作进行告警提示。

6.2 物理安全控制标准

(1)115科技数据中心所选机房全部采用T3级别机房标准：大楼抗震级别不低于10级；市电与发电机自动切换，UPS不间断电源全部后备负责8小时，保证电力不中断；机房环境控制精度22±2℃，相对湿度40%～50%；消防报警监控，早期烟雾探测报警系统；非接触、读卡式门禁系统，全方位实时图像监控系统。

(2)115科技数据中心所在各地机房全部只允许具备长期授权名单内的内部人员(实时更新)进入数据中心，非长期授权人员需要提前将进入机房人员身份信息传真(或者邮件)发给机房管理人员，进入机房需要经过门卫与网管室双重确认身份，方可进入机房。

(3)数据中心所有属于115科技专属物理设备、设备配件等进出数据中心，需要由115产品内部授权人员发关盖有公司公章的设备进出单传真，数据中心现场核实无误后方可允许将设备、配件等进入。

(4)数据中心拥有专门的115科技操作间，用于放置网络模块、服务器硬盘等备件。

(5)操作间所有备件由专人进行登记记录，任何人申请备件，需要写申请方能领取。

(6)数据中心内部的每个区域，或外部走廊区域，都使用摄像机，网管人员7x24小时分段巡逻，并对所有基础设施进行7x24小时集中视频监控。

(7)所有进入机房人员活动记录纸质保存与电子保存(长期)，所有视频记录保存(3个月)，以备后期审计。

七、业务连续性

115科技依托于十多年云存储处理技术和海量数据处理经验，能够应对线上各类风险，具有自动调整和快速反应的能力，保障115科技业务连续运转。

7.1 应急与灾备技术

115科技建立了本地资源管理系统、监控系统，并配合自动化配置系统来保证整体业务连续性。灾备采用多机房同时服务，业务服务分布式部署，数据库主备库热备，通过自动化运维平台，实时故障检测，切换无需人工干预，保障核心应用不中断，系统恢复方便快捷，可进行自动伸缩扩容，在突发事件及自然灾害时，为115产品基础服务可用性及可持续服务提供保障能力。

7.2 应急与灾难恢复管理

建立了完备的应急响应及灾难恢复流程。应急响应组由安全、业务、技术、运维几个部门专业人员组成，制定了完备的应急响应制度及灾难恢复流程，并定期组织灾备演练。

八、安全合规及荣誉

115科技作为国内最早的云存储服务提供商之一，有着超过十年安全技术研究的积累，以及成熟的分布式集群云架构、高可靠的系统实现机制，并通过不断的努力提高安全性，打造了业界一流的安全保障体系。

信息安全认证和资质是云平台安全性的一项重要考量指标，在这方面，115科技取得累累硕果，以多项国际国内权威安全认证，成为云服务提供商中的信息安全典范，其中115科技所有的个人用户都同等拥有115管理用户的安全应用。

近年来，115科技取得的权威安全认证包括：

(1)2015年12月11日获得ISO/IEC 27001:2013(简称：ISO27001)信息安全管理体系认证；

(2)2016年6月17日，115组织(曾用产品名“115+”)正式获得工业和信息化部软件与集成电路促进中心(CSIP)颁发的“国家中小企业公共服务平台-云管理平台”授权；

(3)2017年1月3日，115科技通过云安全联盟(CSA)C-STAR云安全国际权威认证；

(4)2017年1月，115科技获得国家工信部数据中心联盟测试评估的可信云服务认证；

(5)2019年2月，115科技通过ISO27018云中数据保护准则认证；

(6)2019年3月1日，115云盘及115组织系统获得公安部国家信息系统安全等级保护三级认证。

8.1 ISO27001信息安全管理体系认证

115科技最早于2015年12月11日便获得ISO/IEC27001:2013(简称：ISO27001)信息安全管理体系认证，是国内最早获得该认证的云服务提供商之一。

ISO27001是国际上针对信息安全的权威认证标准，由BSI倡导制定。BSI是国际标准化组织(ISO)、国际电工委员会(IEC)、欧洲标准化委员会(CEN)、欧洲电工标准化委员会(CENELEC)、欧洲电信标准学会(ETSI)创始成员之一，广为人知的ISO9000系列管理标准同样是由BSI所倡导制定。

目前，在信息安全管理方面，英国标准ISO27001:2013(前身为ISO27001:2005)已经成为世界上最权威、应用最广泛与典型的信息安全管理标准，它定义了11个信息安全控制域和133个控制项，旨在帮助企业在安全策略、安全制度、安全操作和管理流程等方面，形成统一的信息安全管理体系。115科技认证范畴覆盖如下：云存储、云社区和机构组织信息化云平台的设计、研发和服务的信息安全管理。

伴随着云计算的高速发展与普及，随之而来的全新网络威胁、数据泄漏和欺诈的风险，在全球

范围内引发了诸多危机。对于云服务商来说，客户的数据信息无疑是企业最重要的资产，一旦发生泄露，对企业的信誉、品牌、客户等多方面都将是毁灭性的打击，将会带来无法估量的损失。

而通过ISO27001信息安全认证，标志着115科技的信息安全管理已进入国际化标准水平，同时，115科技也能凭借标准的力量，打造行业典范，为广大个人用户及组织群体的信息安全提供全方位的安全保障，为建设绿色、文明、安全的网络环境贡献力量。

同时，国际安全体系认证也将提升115科技在业界的声誉地位，增强客户、合作伙伴及投资者的信心和认可度，为115科技云服务业务的发展提供强有力的推助。

信息安全管理体系认证证书

（正本）
兹证明

广东一一五科技股份有限公司

统一社会信用代码：91441900577871548P

注册地址：广东省梅州市世界客商中心五楼

已按照
GB/T 22080-2016 idt ISO/IEC 27001:2013
标准要求建立并实施了信息安全管理体系。
该管理体系适用于

云存储、社区云和机构组织信息化云平台的设计、研发和服务的信息安全管理
（适用性声明版本：V 1.4）
涉及的场所及相关活动：

场所地址	场所邮编	场所主要活动
广东省梅州市世界客商中心五楼	514000	云存储、社区云和机构组织信息化云平台的设计、研发和服务的信息安全管理

注 册 号：01221IS1094R2M
颁证日期：2021.12.14
有效期至：2024.12.10

总经理

Information Security Management System Certificate

(Original)
This is to certify that

GUANGDONG 115 TECHNOLOGY CO., LTD.

Unified Social Credit Identifier: 91441900577871548P

Registration Address: FLOOR 5TH, THE WORLD HAKKA ENTREPRENEURS CENTER, MEIZHOU, GUANGDONG, CHINA

Has implemented and maintains an Information Security Management System in compliance with
GB/T 22080-2016 idt ISO/IEC 27001:2013
The Information Security Management System is applicable to:

INFORMATION SECURITY MANAGEMENT OF DESIGN, R&D AND SERVICING OF CLOUD STORAGE, COMMUNITY CLOUD AND ORGANIZATION INFORMATION CLOUD PLATFORM
This is in accordance with the Statement of Applicability, V 1.4
Involved site (s) and relevant activities

Address	Zip Code	Main Activities
FLOOR 5TH, THE WORLD HAKKA ENTREPRENEURS CENTER, MEIZHOU, GUANGDONG, CHINA	514000	INFORMATION SECURITY MANAGEMENT OF DESIGN, R&D AND SERVICING OF CLOUD STORAGE, COMMUNITY CLOUD AND ORGANIZATION INFORMATION CLOUD PLATFORM

Registration Number：01221IS1094R2M
Issue Date：December 14, 2021
Expiry Date：December 10, 2024

Zhao Guoxiang
General Manager
CEPREI CERTIFICATION BODY

8.2 国家中小企业公共服务平台——云管理平台认证

2016年6月17日，115组织产品获得工业和信息化部软件与集成电路促进中心(CSIP)颁发的“国家中小企业公共服务平台——云管理平台”授权，成为国家产业公共服务平台服务体系的一员。

CSIP是工信部直属单位，全面承担国家软件与集成电路等产业公共服务平台的相关建设和管理工作，为我国企业的发展提供公共、中立、开放的服务。其重点打造的“国家产业公共服务平台”体系，是一个具有国家级技术实力与品牌公信力的产业公共服务平台。

国家中小企业公共服务平台是“国家产业公共服务平台”体系的重要组成部分，旨在为全国中小企业提供平台服务。鉴于115科技多年来雄厚的云计算技术积累及在企业级应用中的强大展现，CSIP与115科技深入合作共同建设、推出了115组织平台服务，并正式授权115组织为“国家中小企业公共服务平台-云管理平台”，旨在为全国千万中小企业提供优质的、高可靠性的信息化服务。

8.3 CSA C-STAR云计算安全评估认证

2017年1月3日，115科技通过云安全联盟(CSA)C-STAR云安全国际权威认证，体现了国际权威机构对115科技信息安全管理体系和能力的认可，也标志着115科技在信息安全管理建设的合规性和高标准方面更进一步。

云安全联盟(CSA)是在2009年的RSA大会上宣布成立的一家非盈利性组织。自成立以来，CSA迅速获得了业界的广泛认可。会员涵盖了几乎所有国际领先的电信运营商、IT和网络设备厂商、网络安全厂商、云计算提供商以及重要的云计算用户。云安全联盟正在成为云计算和云安全产业界最为活跃的安全研究和推动力量之一。

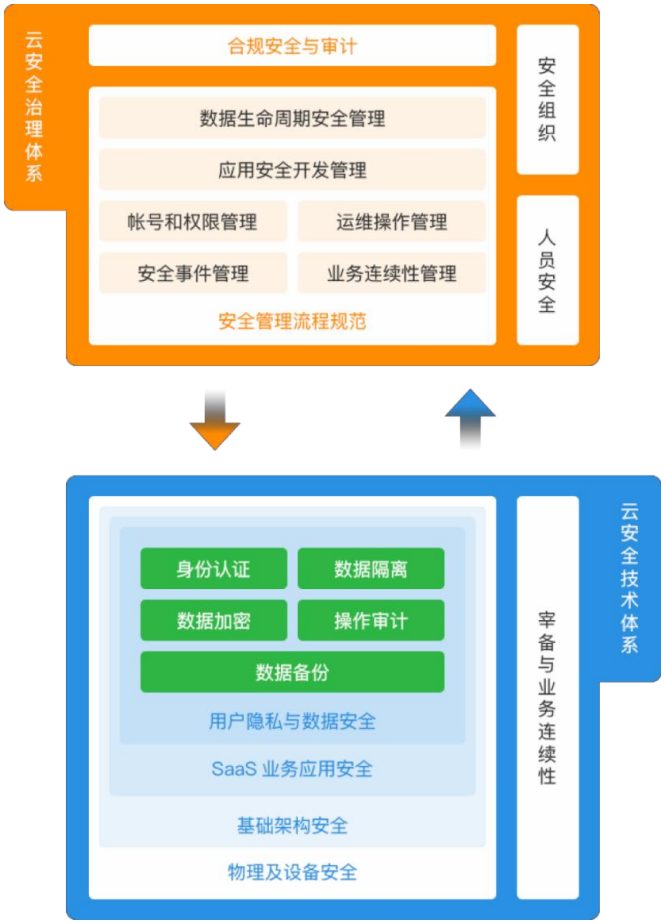
作为国际公认的云服务商安全资质，C-STAR认证是信息安全管理体系ISO/IEC27001的增强版本，结合云控制矩阵(Cloud Control Matrix)、成熟度等级评价模型，以及相关法律法规和标准要求，对云计算服务进行全方位的安全评价。

云时代的到来，给人们生活、商业模式等带来巨大改变。与此同时，安全事件也呈现指数级增长，若干企业遭遇安全危机，损失惨重，这就要求企业具备完善的安全管理体系。

基于此，C-STAR对云厂商提出更高的要求，要求云厂商拥有全面系统的云安全体系。C-STAR云安全评估的管控要求极为严格，评估过程采用国际先进的成熟度等级评价模型，涵盖应用和接口

安全、审计保证与合规性、业务连续性管理和操作弹性、变更控制和配置管理、数据安全和信息生命周期管理、加密和密钥管理、治理和风险管理、身份识别和访问管理、基础设施和虚拟化安全、安全事件管理、供应链管理、威胁和脆弱性管理等16个控制域的全方位安全评估。

企业如若通过C-STAR评估，则可获得CSA颁发的C-STAR云安全证书、获得CSA官网证书注册并受到国际认可、获取云安全管理成熟度报告。企业通过云安全评估，更能促进提高云安全管理水平，减少可能潜在的风险隐患，保障业务持续开展与紧急恢复，更好地满足顾客的云安全要求，并证明云安全水平领先于云服务提供者行列，成为安全领域毋庸置疑的先驱者。



信息安全是企业最关心的问题之一，作为面向群体组织管理协作的SaaS平台，在管理上，115科技根据CSA云安全指南进行建设，并制定了各种信息安全管理规范，对人员、开发、账号管理、运维、事件、审计等多方面进行严格要求，并不断复核、改进；在技术上，115科技严格筛选和监督IaaS供应商的安全，关注SaaS应用安全，对于数据安全，层层把控、严密防御、实时监督并制定各种数据安全策略，来保障数据的可用性、完整性和机密性。

放眼全球，仅有为数不多的公有云企业通过了C-STAR认证。115科技一直努力为用户搭建最全面的安全保障，并积极通过专业资质认证完善安全合规。为用户提供安全、高速、稳定的服务能

力，是115科技最重视、最扎实的内功，也是115科技取得用户信赖的重要途径。

未来，115科技的云安全能力还将不断提升，持续为用户带来更为专业、更为可信、更为安全的云服务。

云计算安全评估证书

（正本）
兹证明

广东一一五科技股份有限公司

统一社会信用代码：91441900577871548P

注册地址：广东省梅州市世界客商中心五楼

已建立并实施了符合 C-STAR 要求的云计算信息安全管理体系。
该管理体系适用于

云存储、社区云和机构组织信息化云平台的设计、研发和服务的信息安全管理
（适用性声明版本：V 1.4）

涉及的场所及相关活动：

场所地址	场所邮编	场所主要活动
广东省梅州市世界客商中心五楼	514000	云存储、社区云和机构组织信息化云平台的设计、研发和服务的信息安全管理

注册号：CPR20CS0003
颁证日期：2020.02.11
有效期至：2023.01.03

总经理签字：

C-STAR (Security, Trust & Assurance Registry) Certificate

(Original)
This is to certify that

GUANGDONG 115 TECHNOLOGY CO., LTD.

Unified Social Credit Identifier: 91441900577871548P

Registration Address: FLOOR 5TH, THE WORLD HAKKA ENTREPRENEURS CENTER, MEIZHOU, GUANGDONG, CHINA

Has implemented and maintains a Cloud Security Management System in compliance with

C-STAR Assessment requirements

The Cloud Security Management System is applicable to:

INFORMATION SECURITY MANAGEMENT OF DESIGN, R&D AND SERVICING OF CLOUD STORAGE, COMMUNITY CLOUD AND ORGANIZATION INFORMATION CLOUD PLATFORM

This is in accordance with the Statement of Applicability, V 1.4

Involved site (s) and relevant activities

Address	Zip Code	Main Activities
FLOOR 5TH, THE WORLD HAKKA ENTREPRENEURS CENTER, MEIZHOU, GUANGDONG, CHINA	514000	INFORMATION SECURITY MANAGEMENT OF DESIGN, R&D AND SERVICING OF CLOUD STORAGE, COMMUNITY CLOUD AND ORGANIZATION INFORMATION CLOUD PLATFORM

Registration Number: CPR20CS0003
Issue Date: February 11, 2020
Expiry Date: January 03, 2023

Zhao Guoxiang
General Manager
CEPREI CERTIFICATION BODY

8.4 可信云服务认证

2017年1月，115科技获得国家工信部数据中心联盟测试评估的可信云服务认证。

可信云服务认证是由数据中心联盟组织，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的评估认证，是我国唯一针对云计算信任体系的权威认证体系。

在工业和信息化部(以下简称“工信部”)的指导下，云计算发展与政策论坛启动了我国首个云服务质量评估体系的可信云服务认证。由云计算发展与政策论坛成立的可信云服务认证工作组负责认证工作，其成员包括工信部电信研究院、电信运营商、主要互联网企业和设备提供商。

可信云认证包括云主机服务、对象存储服务、在线应用服务等11部分、共16项指标的测评，涵盖云服务商需要向用户承诺或告知(基于服务SLA)的90%的问题，已经成为衡量国内云服务厂商能力的关键指标，也成为用户选择云服务厂商的重要依据。

通过率仅为百分之三十多的可信云认证让众多云服务厂商望而却步，而115科技凭借着优质的安全云服务以及众多用户口碑的积累，通过层层检测，终于拿下本次可信云服务认证，这也意味着115

科技提供的云服务的稳定性、可靠性、安全性等指标都达到国内顶级云服务评测系统的认证标准。

可信云服务认证工作从2013年开始，致力于促进我国云计算创新发展，提升服务质量和诚信水平，逐步建立了云计算产业的信任体系，已经被业界广泛接受。115科技作为国内领先的云服务提供商，也一直在致力于推动整个行业向更透明化和健康化发展。而此次可信云服务安全认证的通过，体现了115科技的一贯的可信品质，也是对115科技为客户提供最高等级安全服务的最好肯定和认可。

8.5 ISO27018云中数据保护准则认证

2019年2月，115科技通过了ISO27018云中数据保护准则认证，标志着企业在保护用户数据、知识产权、文档和云端IT系统安全等方面达到了高标准的行业实践。

ISO27018是对ISO/IEC27001和ISO/IEC27002标准的扩展，是首个专注于云中个人数据保护的国际行为准则，是目前国际上最权威、最严格、也是最被广泛接受和应用的信息安全体系认证。

通过ISO/IEC27018国际认证，不仅表明115科技在个人/组织信息处理的准确性、安全性等方面有能力为用户提供可靠保护，更体现了115在数据安全管理方面已经达到国际顶尖水平，成为全球认证合规最完备的云平台之一。

公有云个人信息安全管理体系
认证证书

(正本)
兹证明

广东一一五科技股份有限公司

统一社会信用代码：91441900577871548P

注册地址：广东省梅州市世界客商中心五楼

按照 ISO/IEC27001:2013 标准和基于 ISO/IEC 27018:2019 标准的公有云个人信息安全管理体系认证特殊要求在以下范围实施了个人信息保护：

云存储、社区云和机构组织信息化云平台的设计、研发和服务的信息安全管理
（适用性声明版本：V 1.4）

涉及的场所及相关活动：

场所地址	场所主要活动
广东省梅州市世界客商中心五楼	云存储、社区云和机构组织信息化云平台的设计、研发和服务的信息安全管理

本认证基于以下 ISO/IEC 27001:2013 认证
注册号：012211S1094R2M
ISMS 适用性声明版本：V 1.4

注 册 号：CPR22ISP001R1M
颁证日期：2022.01.10
有效期至：2025.01.09

总经理：

Public Clouds Personal Information Security Management System Certificate

(Original)
This is to certify that

GUANGDONG 115 TECHNOLOGY CO., LTD.

Unified Social Credit Identifier: 91441900577871548P

Registration Address: 5/F, THE WORLD HAKKA ENTREPRENEURS CENTER, MEIZHOU CITY, GUANGDONG PROVINCE, CHINA

Implements PII protection by following ISO/IEC 27001:2013 and certification special requirements of personal information security in public clouds based on ISO/IEC 27018:2019 for the following scope:

INFORMATION SECURITY MANAGEMENT OF DESIGN, R&D AND SERVICING OF CLOUD STORAGE, COMMUNITY CLOUD AND ORGANIZATION INFORMATION CLOUD PLATFORM

This is in accordance with the Statement of Applicability, V 1.4

Involved site (s) and relevant activities

Address	Main Activities
5/F, THE WORLD HAKKA ENTREPRENEURS CENTER, MEIZHOU CITY, GUANGDONG PROVINCE, CHINA	INFORMATION SECURITY MANAGEMENT OF DESIGN, R&D AND SERVICING OF CLOUD STORAGE, COMMUNITY CLOUD AND ORGANIZATION INFORMATION CLOUD PLATFORM

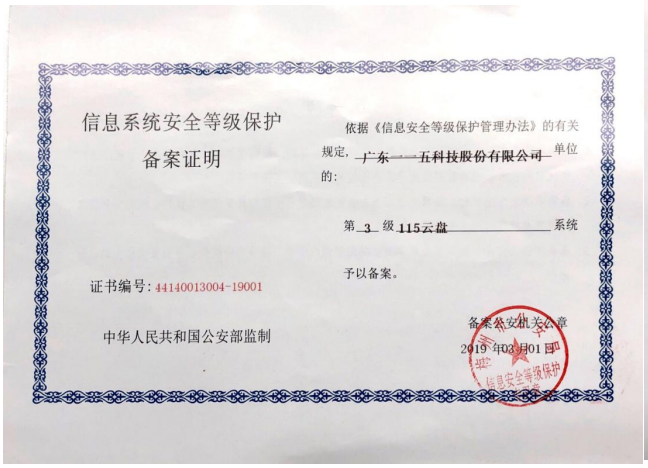
This certify is based on the following ISO/IEC 27001：2013 certificate
Registration number: 01221IS1094R2M
The ISMS is in accordance with the Statement of Applicability, V 1.4

Registration Number：CPR22ISP001R1M
Issue Date：January 10, 2022
Expiry Date：January 09, 2025

Zhao Guoxiang
General Manager
CEPREI CERTIFICATION BODY

8.6 公安部国家信息系统安全等级保护三级认证

2019年3月，115产品均通过国家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，广东一一五科技股份有限公司 单位的：

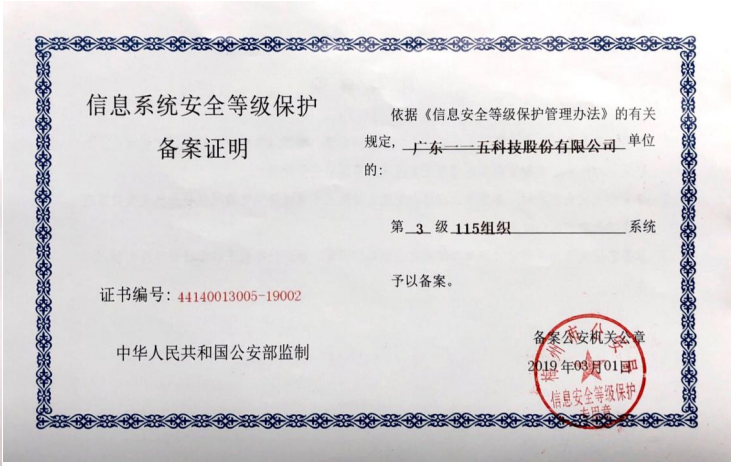
第 3 级 115云盘 系统

予以备案。

证书编号：44140013004-19001

中华人民共和国公安部监制

备案公安机关公章
2019 年03月01日



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，广东一一五科技股份有限公司 单位的：

第 3 级 115组织 系统

予以备案。

证书编号：44140013005-19002

中华人民共和国公安部监制

备案公安机关公章
2019 年03月01日

国家信息等级保护认证是中国最权威的信息产品安全等级资格认证，由公安机关基于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。

信息安全保护等级共分为5级，等级越高，意味着计算机信息安全保护能力越强。其中三级是国

家对非银行机构的最高级认证，属于“监管级别”，由国家信息安全监管部门进行监督、检查，认证要求十分严格，国有四大行的省级和市级分行即是三级备案认证。

此次115产品凭借强大的安全技术能力，顺利通过测评，获得公安部“国家信息系统安全等级保护”三级认证，代表115科技在信息规范化管理方面得到了国家权威机构的监管和认可。