IMOU 乐橙

乐橙云安全及隐私保护白皮书

版权声明

- ©杭州华橙网络科技有限公司 版权所有。
- 在未经杭州华橙网络科技有限公司（下称"华橙网络""我们"或"公司"）事先书面许可的情况下，任何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，可能包含华橙网络及可能存在的第三人享有版权的软件。除非获得相关权利人的许可，否则，任何人不能以任何形式对前述软件进行复制、分发、修改、摘录、反编译、反汇编、解密、逆向工程、出租、转让、分许可等侵犯软件版权的行为。

商标声明

- imou 、imou 乐橙，华橙是杭州华橙网络科技有限公司的商标和/或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，华橙网络都不对任何人因本文档中相关内容及描述的产品而产生的任何特殊的、附随的、间接的、继发性的损害或任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均"按照现状"提供，仅作为使用指导，除非适用法律要求，华橙网络对文档中的所有内容不提供任何明示或暗示的保证。

出口管制合规声明

华橙网络遵守适用的出口管制法律法规，并且贯彻执行与硬件、软件、技术的出口、再出口及转让相关的要求。就本文档所描述的产品，请您全面理解并严格遵守国内外适用的出口管制法律法规。

关于本文档

- 您购买的产品、服务或特性等应受具体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之内。
- 如不按照本文档中的指导进行操作，因此而造成的任何损失由使用方自己承担。
- 如获取到的文档无法打开，请将阅读工具升级到最新版本或使用其他主流阅读工具。
- 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，恕不另行通知。
- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以华橙网络最终解释为准。

名词解释

名词	说明
API	Application Programming Interface，即应用程序编程接口，是一些预先定义的函数，或指软件系统不同组成部分衔接的约定。
BIA	Business Impact Assessment，业务影响评估。
DevOps	Development 和 Operations 的组合词，是一组过程、方法与系统的统称，用于促进开发（应用程序/软件工程）、技术运营和质量保障（QA）部门之间的沟通、协作与整合。
双 PbD	Privacy by Design：隐私设计原则，是一种在系统和流程设计初期就将隐私和数据保护融入其中的方法。 **Protect by Default**：默认保护原则，意味着在系统或产品的设计和配置中，安全保护措施应该是默认启用的，而不是需要用户手动设置。
RASP	Runtime application self-protection，运行时应用自我保护。
SDLC	Secure Software Development Lifecycle，即安全软件开发生命周期。
STRIDE	Spoofing（假冒）、Tampering（篡改）、Repudiation（否认）、Information Disclosure（信息泄漏）、Denial of Service（拒绝服务）和 Elevation of Privilege（提升权限），是一种威胁建模方法。
P2P	Peer-to-Peer，也叫对等互联或点对点技术。P2P 不是一种新的协议，而是利用现有的网络协议实现网络数据或资源信息共享的技术，它使用的可能是 TCP、UDP 或其他协议。
PIA	Privacy Impact Assessment，隐私影响评估。
PII	Personally Identifiable Information，个人可识别信息。
TSL	Thing Specification Language，物模型是一个 JSON 格式的文件，它是物理空间中的实体在云端的数字化表示。
VPC	Virtual Private Cloud，是公有云上私有网络，通俗讲就是用户可自定义的网络。
WAF	Web Application Firewall，Web 应用防火墙。

目录

01

引言

1.1 乐橙介绍

乐橙，是杭州华橙网络科技有限公司于 2015 年创立的面向全球民用智慧物联网市场消费端的智能家居品牌，致力于为消费者提供更智能、更便捷、更舒适的生活体验。华橙网络构建了乐橙安防、乐橙互联、乐橙机器人、乐橙 IoT 四大产品体系，依托于乐橙 AI 能力以及乐橙云平台的支撑，为消费者提供全场景的家庭安全智能解决方案。通过前沿科技和智能产品，乐橙为每个用户竭力打造更加简单、安全、智能的生活。同时，华橙网络利用乐橙云开放平台，与第三方视频应用开发者分享云平台服务能力，帮助其开拓更多的场景化应用服务，并共同建设智慧物联网云生态。

网络安全及隐私保护始终是华橙网络最高纲领和核心发展战略之一。华橙网络坚守"合规、开放、透明"的理念，秉持为用户提供高效、安全、可信视频云服务的初心，积极面对不断出现的安全与合规挑战。为了应对这些挑战，华橙网络基于纵深防御的安全理念，结合"默认保护"和"隐私设计"的双 PbD 原则，不断完善云安全保障措施，联动全领域安全能力，持续构建乐橙云安全及隐私保护框架，以确保用户的数据和隐私得到充分保护。

图：云安全及隐私保护框架

1.2 安全责任和角色

乐橙云依托基础云服务提供商的"基础设施即服务 IaaS"能力，构建了以视频为核心的 AIoT 云平台能力，并基于此为用户提供乐橙 APP、乐橙含光、开放平台、电商平台、IoT 平台等服务。下图为基础云服务提供商、乐橙云以及用户，三方的云安全责任共担模型：

图：责任共担模型

1.2.1 乐橙云责任

乐橙云通过选择全球知名的云服务提供商，依托全球一流的云计算平台，确保提供安全的管理和运营基础设施、物理设备、虚拟化服务。另外再通过签署服务协议，约束云服务提供商的安全管理；通过核查服务报告和开展尽职调查，检验云服务提供商的安全水平。

乐橙云提供云平台和服务的规划、设计开发、运维及运营安全，以保障用户数据和隐私安全。包括但不限于：

平台安全：使用安全标准化后的网络、主机、中间件、基础能力，构建安全的乐橙云平台；

应用安全：基于乐橙云平台提供的乐橙 APP、乐橙含光、开放平台、商城平台、IoT 平台等服务的安全与合规。

数据安全：业务数据在云服务环境中的全生命周期管理和隐私保护，包括数据分类分级、安全隔离、访问控制、传输及存储加密、隐私脱敏展示等。

访问控制安全：对资源和数据的访问权限管理，包括用户管理、权限管理、身份验证等。

1.2.2 用户责任

用户在使用乐橙云解决方案的时候，需要关注云服务使用安全，通过加强身份凭证和终端设备安全管理，以更好地保护个人数据安全。

用户基于乐橙开放平台（包括使用 SDK）自行开发终端应用时，乐橙云仅对开放平台自身和保存到云端数据的安全负责，并提供技术支持。需要用户自行保障终端应用及数据的安全合规。

用户以物模型方式接入乐橙云时，需要严格按照乐橙云的安全配置和接入要求执行，以确保产品本身的安全性。

02

网络安全

2.1 基于 NIST CSF 框架的网络安全体系

NIST CSF（National Institute of Standards and Technology Cybersecurity Framework）是由美国国家标准与技术研究所制定的网络安全框架，该框架于 2014 年发布，以帮助各类组织建立、改进和管理网络安全策略，以加强网络安全防御和响应能力。NIST 于 2024 年 2 月发布了 CSF2.0 版本。

NIST CSF 框架包含框架核心（Core）、配置文件（Profile）、实施层级（Tier）三部分。其中框架核心由六个核心功能组成，实现了网络安全"事前、事中、事后"全过程覆盖。

- 治理（Govern）：建立并监督组织的网络管理策略，期望及政策。
- 识别（Identify）：帮助确定组织当前面临的网络安全风险。
- 保护（Protect）：使用安全措施来避免或减少网络安全风险。
- 检测（Detect）：发现和分析可能的网络安全攻击和漏洞。
- 响应（Respond）：针对检测到的网络安全事件采取行动。
- 恢复（Recover）：恢复受网络安全事件影响的功能或服务。

华橙网络基于 NIST CSF 框架来构建、提升华橙网络的网络安全防御能力与风险管理能力，并在运营过程中遵循 PDCA 循环模型持续改进，为用户提供更加安全、可靠、稳定的服务。

2.2 网络安全策略和控制措施概述

治理

- 华橙网络成立了公司级的合规管理委员会，并设立网安与数据保护合规组、产品合规组等专业合规组织，全面落实网络安全、数据保护等方面的合规义务。自上而下推进合规规范管理，以增强全员合规意识，提高风险控制与防范能力。
- 华橙网络已建立专门的安全团队，针对不同的安全领域，管理、指导、执行、监督、验证网络安全与数据保护工作的推进。
- 华橙网络制定了一系列风险管理计划，并按计划逐步推进各部门严格落实风险管理措施。
- 华橙网络面向不同的对象与资产分别发布信息安全管理制度与流程、数据安全管理制度与流程、隐私保护管理制度与流程，以确保各个领域得到管控。

识别

- 华橙网络建立资产清单，并对资产进行全生命周期的管理，使所有为用户提供服务的资产得到有效管控。

- 华橙网络基于数据资产的类型、对象、用途和重要程度，结合相关法律法规和行业标准，对数据进行分类分级并建立数据资产目录，使用数据系统对数据进行全生命周期的管理。
- 华橙网络通过持续的漏洞扫描工具、定期内部渗透测试、华橙网络 SRC 接受公众提交漏洞等方式或途径识别存在的安全风险与隐患。
- 华橙网络通过将软件成分分析 SCA 融入到 CICD 流程中，每一次发版都进行软件成分分析以识别供应链风险。
- 华橙网络定期组织内部合规团队开展 ISO27001、ISO27701、ISO27018 等面向组织体系的内审，识别组织体系存在的安全风险。
- 华橙网络定期组织内部合规团队开展隐私影响评估、APP 隐私合规、安全基线等面向产品、服务或系统的内审，以识别产品、服务、系统存在的安全风险。

检测

- 华橙网络将行业标准、法律法规、客户要求、威胁建模等相关要求整合成《云服务安全基线》，将安全基线融入到业务需求及 DevSecOps 流程中，产品及服务在上线前按照对应的安全基线或需求验收点执行检查，确保安全基线得到落实。
- 华橙网络部署数据防泄漏 DLP、主机型入侵检测系统、WEB 应用防火墙、软件成分分析 SCA、安全日志统一分析平台等网络安全事件检测与分析工具。
- 华橙网络对系统、应用、主机、网络等进行常态化全天候的漏洞扫描，定期组织内部安全团队开展渗透测试。

保护

- 华橙网络员工账号遵从员工账号管理规定。华橙网络云平台及华橙网络用户账号遵从华橙网络云账号权限管理要求和国家相关法律法规要求。
- 华橙网络通过安全组策略、ELB 策略等实现网络分割与攻击面最小化，并严格落实业务与租户隔离策略。
- 华橙网络制定《云服务安全基线》、《客户端安全基线》等产品与服务安全基线，并通过开展 SDLC 将安全需求落实到服务与产品的生命周期中。
- 华橙网络提供了高可用基础设施，多节点冗余备份能力，备份依次轮换更新；制定业务连续性计划，并定期开展演练测试。
- 华橙网络对数据进行分类分级管理，提供多种安全保护措施与能力，为用户的数据安全与隐私保护进行保驾护航。在数据采集时进行采集源认证、敏感数据采集时源端加密；数据传输时采用安全加密信道（如 https）；数据存储时加密存储；数据展示时脱敏展示等。使用数字签名和时间戳等机制，防止数据被篡改、重放等。对应用服务间的调用、操作进行日志留存与审计。对接口间调用进行身份认证鉴权、访问控制与传输保护等。
- 华橙网络部署 HIDS 主机型入侵检测系统、WEB 应用防火墙、防病毒软件、软件成分分析 SCA 等安全工具，保护云服务、产品及系统的安全性。
- 华橙网络部署数据防泄漏 DLP、防病毒软件、安全准入系统、堡垒机等，确保员工的操作安全与行为规范符合要求。

响应

- 华橙网络制定了包括网络安全事件应急响应在内的网络安全事件管理流程，并持续优化。
- 华橙网络制定应急响应演练计划，并定期开展应急演练，确保过程得到验证，能力得到提升。
- 华橙网络已建立安全团队负责网络安全事件的监控、分析、取证等响应过程，确保网络安全事件得到专业人员的管理与评估。
- 华橙网络在内部事件管理系统中记录并跟踪所有的网络安全事件，确保安全事件得到端到端的跟踪闭环。
- 华橙网络制定了公众沟通与上报机制，与行业机构、监管部门保持联系，及时告知客户关于影响客户业务的服务通知与相关事件，提升客户服务感知。
- 华橙网络部署 HIDS 主机型入侵检测系统、WEB 应用防火墙、防病毒软件、安全组策略、ELB 策略等，并通过调整安全策略防止事件扩散，减轻事件影响。

恢复

- 华橙网络制定了网络安全事件管理流程，并持续优化。
- 华橙网络云异地跨区域多副本备份，实现高可用。
- 定期以快照形式进行全量备份，快照备份依次循环更新，以确保数据可以及时恢复。

定期计划并实施应急恢复演练，以检验一旦发生网络安全事件可以按程序快速恢复业务和数据的能力。

03

数据安全及隐私保护

3.1 数据隐私保护理念与设计

华橙网络践行数据隐私保护功能化、场景化，秉承隐私保护"合法性、公正透明、目的限制、数据最小化、准确性、存储限制、适度安全"原则，尊重用户"知情权、访问权、修改权、遗忘权、限制处理权、可携权 、拒绝权、自动化决策与数据画像有关的权利"，采用业界认可的 Privacy by Design，Privacy by Default 理念作为指导，结合在数据隐私保护领域多年的经验沉淀，形成《产品隐私保护设计指引》。华橙网络已应用该指引开展隐私需求设计和隐私功能管理，同时，通过开展隐私保护影响评估（PIA），识别隐私风险并采取处置措施消除或降低风险。

目前，华橙网络已支持隐私模式、华橙网络云解码、第三方视频加密、账号信息导出等隐私保护功能。通过《隐私政策》以及客户反馈通道，帮助用户了解华橙网络隐私保护能力。

3.2 数据生命周期安全管理

图：数据生命周期

华橙网络云通过对数据全生命周期（采集、传输、使用、存储、提供、销毁）的安全管控，提升数据的保密性、完整性、可用性、隐私合规，保障云平台安全稳定运营。

- **采集**：

1. 华橙网络应用及设备，包括 IoT 设备（华橙网络摄像头、智能门锁、无线探测感应器等）、APP 应用程序、PC 客户端、小程序等，遵守法律法规要求，评估业务功能逻辑，严格控制数据采集的范围、频率和精度。
2. 对数据采集来源进行身份鉴别和记录，防止非法数据源，避免采集到错误和失真数据。
3. 通过隐私政策告知用户，并获得同意和授权。

- **传输**：

1. 传输通道使用 TLS 加密传输协议，并对传输通道的主体进行身份认证。
2. 数据面与业务面分离，控制信令与数据传输分离，避免数据过失性泄露。
3. 提供口令、音频、视频、图片等敏感数据在传输过程中内容加密的增强能力。
4. 慎重处理数据跨境的情况，通过调研对应区域及国家的法律法规，开展隐私影响评估，签署数据处理协议等方式确保合规遵从。

- **使用**：

1. 实施细粒度的访问控制策略，仅授权人员鉴权成功后可访问数据。
2. 处理过程中，遵循收集时所声称的目的或合理关联的范围。
3. 展示个人敏感信息时采取脱敏处理，避免数据被非法访问或使用。

- **存储：**

1. 用户个人数据存储期限遵循最小化原则，处理目的完成后及时删除。
2. 媒体数据存储依托云服务提供商的落盘加密存储能力，个人可识别信息（PII）实现 AES256 加密后存储（口令采用 HASH 加盐后存储），加密密钥（因子）可由用户设置。
3. 普通数据和敏感数据分表存储，数据访问权限控制在表级别，以实现数据的逻辑隔离。

- **提供：**

1. 使用 APP 的安全导出功能或联系官网客服，通过身份校验后可导出用户注册时提供的个人数据。
2. 提供用户使用自定义密码功能对导出数据进行加密。
3. 支持对发起导出数据的请求进行用户行为审计。

- **销毁：**

1. 提供易于操作的注销账户功能，用户还可以联系官网客服清除云上个人数据。
2. 在使用乐橙摄像头等终端设备时，用户通过恢复出厂设置功能可以删除存储在设备中的个人数据，增加数据删除处理的透明性。
3. 在用户注销账户或者数据到期时，及时删除用户的个人数据或匿名化处理。

3.3 数据备份安全

图：数据存储中心

3.3.1 多数据中心

乐橙云采用高可用策略，基于分布式架构，部署了中国（国内）、美洲（海外）、欧洲（海外）、亚太（海外）四大可用数据中心，乐橙云灵活地将数据和系统部署于不同数据中心或不同区域，根据用户所在地区提供相应的数据服务，以保证业务的容灾性。

3.3.2 多副本冗余

用户的音视频和图片数据采用多副本模式存储在云存储中，基于云服务提供商的 SLA 进行服务保障。结构化数据存储于加固后的数据库中，采用多副本模式（至少保证两个副本）每日自动增量备份，每周全量备份，通过定期的应急演练检验备份的完整性和可用性。

3.4 数据隐私保护安全实践

3.4.1 媒体数据安全实践

媒体数据安全是数据安全的核心，也是用户最关心的部分。当用户购买乐橙云存储服务，乐橙设备产生的报警录像将被存储在乐橙云上，供用户随时随地查看。华橙网络对媒体数据进

行端到端加密，对上云的录像从录像上传、存储、下载、访问采取全生命周期安全防护，避免了媒体未授权访问、数据泄露等风险发生：

- 录像上传：对媒体流进行源端内容加密，并具备支持基于 HTTPS 协议的传输加密能力。
- 录像存储：源端加密后的录像数据在落盘时进一步加密存储于云存储中。
- 录像下载与访问：客户端必须经过鉴权后才能下载、访问录像，且录像在下载过程中依旧内容加密，到客户端再进行解密，确保媒体数据端到端安全。

3.4.2 企业数据安全实践

乐橙云对归属于不同企业客户之间的数据逻辑上禁止互相访问以实现安全隔离，并在符合法律法规的基础上按照客户书面指示、合同约定来处理客户数据，针对不同的业务场景提供不同的数据存储服务，对敏感数据采用 AES256 等加密算法进行加密存储，同时对加密密钥采用统一的安全管理和分发机制。

04

合规与审计

4.1 合规管理体系

为有效防范、识别、应对可能发生的合规风险，适应全球化业务发展，华橙网络基于ISO37301 合规管理体系要求建立了合规管理体系，以促进业务经营活动的合规规范，增强公司全员合规意识，以帮助公司在全球范围内更好的符合包括网络安全与数据保护等在内的合规要求，确保公司在全球规范开展业务经营活动。

华橙网络成立了合规管理委员会，每季度审议合规管理工作的周期性计划及执行情况，对合规管理重大问题进行决策。

在合规管理委员会的框架下，分别设立了由专业团队组成的网安与数据保护合规组、产品合规组等专业模块的合规执行组织，各专业模块合规组每月召开例会，管理各模块合规工作的周期性计划及执行情况，并汇总上报至合规管理委员会进行审议决策。

图 乐橙合规管理组织架构

4.2 内部合规审计

华橙网络通过开展内部合规治理，落实内部审计工作，验证管理活动、技术措施、安全策略以及相关结果是否符合网络安全、数据安全、隐私保护等方面的法律法规、客户与相关方、体系标准文件的要求，确保产品、服务、管理的符合性、适宜性和有效性。目前，已开展包括但不限于以下方面的工作：

面向管理体系：

ISO 27001 信息安全管理体系内部审计。
ISO 27017 管理体系内部审计
ISO 27018 管理体系内部审计
ISO 27701 管理体系内部审计

面向产品与服务：

云服务安全基线内部审计
运维安全基线内部审计
客户端安全基线内部审计

面向隐私保护：

APP 个人信息安全规范内部审计

4.3 合规认证

在隐私保护合规领域，华橙网络遵循GDPR法案，落实隐私与数据治理实践标准，已通过 IoT 服务隐私保护认证和 ISO27701 隐私保护管理体系认证、ISO27018 云隐私保护认证、移动互联网应用程序（App）安全认证。

在云安全控制领域，华橙网络践行 CCM 云控制矩阵和 NIST SP 800-53 标准，已通过 CSA STAR 云安全国际认证和 ISO27017 云计算信息安全管理体系认证。

在信息安全管理领域，华橙网络遵循国际权威认证体系，已通过 ISO27001 信息安全管理体系认证。

在网络安全及运营服务领域，乐橙符合网络安全等级保护要求和 GB/T36326-2018《信息技术云计算云服务运营通用要求》，已通过了网络安全等级保护三级认证和 ITSS 云计算服务能力评估三级认证。

05

云平台安全

5.1 基础设施安全

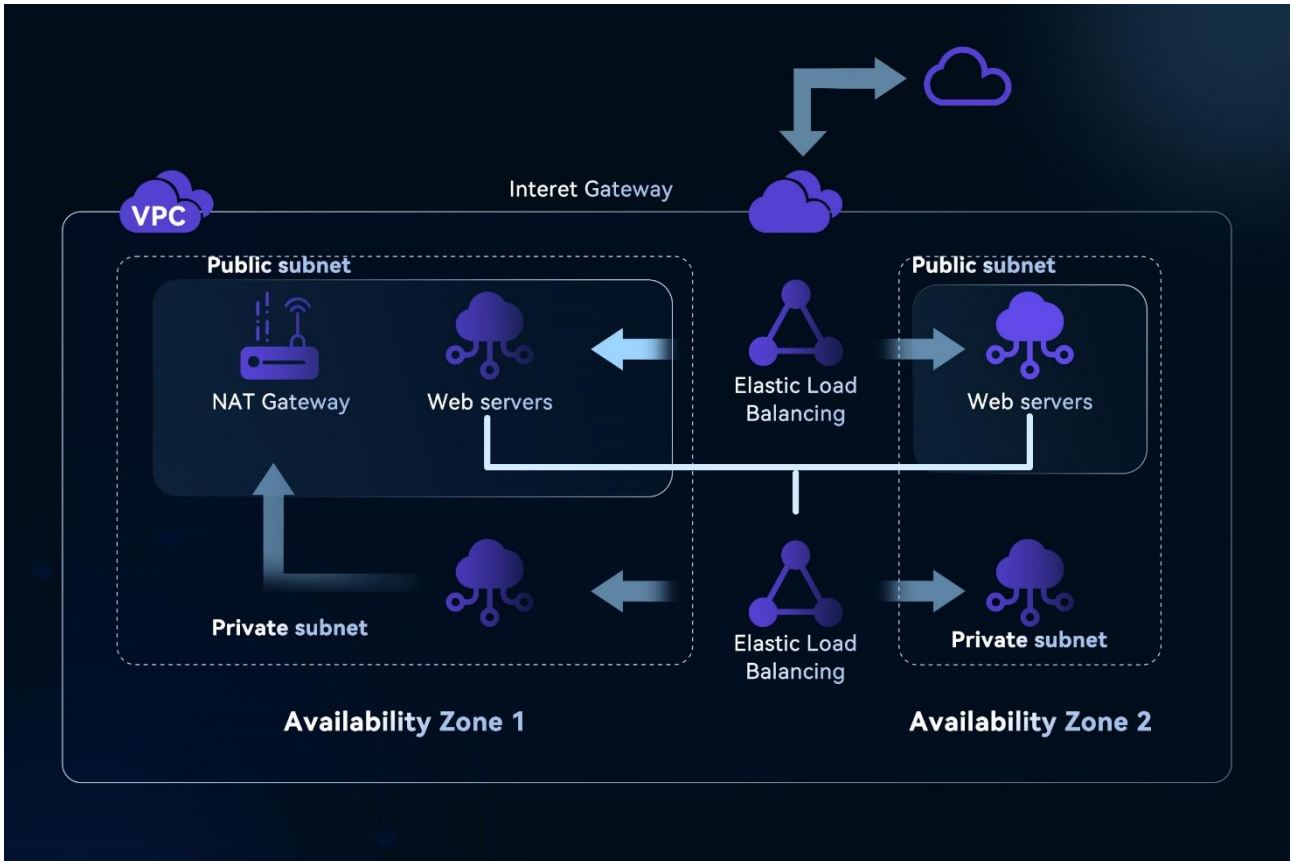
乐橙云依托亚马逊云 AWS、Oracle Cloud、阿里云等全球知名云服务提供商的基础服务，构建了乐橙云全球服务节点，通过管理和技术手段提高基础服务的稳定性。

- 供应链安全管控：设定云服务提供商安全能力与资质门槛，严格把控准入条件，不定期开展尽职调查，检验各云服务提供商安全报告，确保基础设施的安全性与可靠性。制定应急计划以应对潜在的供应链中断，包括在关键时刻采取替代措施和补救措施。
- 高可用架构：采用多云厂商互备的策略，校验云厂商之间的可移植和互操作性，以快速应对部分云服务提供商不可用的情况。乐橙云灵活地将数据和系统部署于不同数据中心或不同区域，以保证业务的容灾性要求。

5.2 网络安全

乐橙云整合防火墙、安全组、云 WAF 等多重防护机制，采用 VPC 网络部署方式构建网络安全架构。VPC 对等连接功能保障了多个区域节点之间的数据传输安全，利用 VPC 的 ACL、安全组功能，按需配置安全与访问规则，乐橙云可实现细粒度的网络隔离需要。

- 访问控制：通过安全组强制默认拒绝规则，开启 IP 白名单，限制到具体 IP 和端口，只允许可信的请求通过可信网络访问。
- 网络隔离：乐橙制定了严格的内部网络隔离规则。通过物理和逻辑隔离方式实现内部的办公网络、开发网络、测试网络、生产网络等访问控制和边界保护。。内部管理系统使用堡垒机统一管理，服务器 SSH 端口及业务管理后台只对堡垒机开放，业务网络无法访问管理网络。
- DDoS 防护：乐橙云使用云服务提供商的 DDoS 防护功能，自动检测、调度和清洗，确保云平台网络稳定。结合防火墙和云 WAF 对恶意攻击流量进行阻断。
- 网络冗余：乐橙云数据服务云主机通过在全球多个区域建立云主机，实现了跨地域的网络灾备能力，有效降低了非人为因素导致的网络故障对业务的影响。同时，采用冗余的网络建设方式，以及多物理机房部署，实现了网络的便捷性和流量承载的工程调度，确保网络服务不会因单点故障而中断，实现了同城和跨城容灾。



图：VPC 网络划分

5.3 主机安全

严格限制云主机的访问权限。在操作系统层面，构建了加固、检测、修复能力。

- 安全镜像：采用云服务提供商官方安全镜像，定期更新系统补丁、主机密钥。
- 系统加固：统一采用密钥登录，加固系统与服务配置，限制开放端口、安装服务最小化。
- 恶意程序检测：重要业务主机部署了防病毒软件，实时监控主机安全状态，定期对主机采取全盘病毒和木马扫描，并对恶意程序进行查杀。
- 关键文件变更检测：实时监控系统关键文件（如：开机加载、网络配置、crontab 任务、passwd、sudoers 配置等），一旦文件被修改即触发告警。
- 资源监控：实时监控主机资源容量情况，若超出事先设定的阈值，即触发告警。

5.4 中间件安全

为保障应用程序的运行效果和用户体验，使用了多种开发框架、中间件、数据库等。乐橙云

从如下几个方面兼顾安全与性能的平衡。

- 安全选型：在选型时遵循软件准入原则开展安全评估，评估覆盖业务必要性、替代方案、维护更新情况、安全能力和合规水平。开源软件遵守开源管控要求。
- 安全加固：及时升级至较新版本，修复安全漏洞，开启安全功能、删除默认页面和禁用不使用的组件等。
- 凭证安全：删除或修改中间件默认账号及口令。设置账号不能为常用用户名如 root、admin 等。设置口令必须 8 位以上数字、字母、特殊字符组合。登录凭证最小化权限处理，且要求不同项目使用不同的登录凭证。
- 访问控制限制：基于角色的访问控制策略，不同角色分配不同的访问权限。

5.5 安全及隐私设计

图：安全及隐私设计

乐橙云安全及隐私设计覆盖规划、设计开发、运维和运营服务全过程，贯穿内部和外部多层

防护，保障云服务核心业务和数据安全。内部防护机制，安全基线和专项加固以互补形式重点提升服务自身基础安全能力；外部防护机制，防护引擎可直接集成部署用于提升服务安全和动态防御能力。

结合 CIS 标准和业界优秀实践，乐橙云已具备 Springboot、Docker、Nginx、RabbitMQ、ActiveMQ、MySQL、WEB 安全加固能力。并采取统一标准化进行要求。安全加固以标准安全理念为指导，降低组件攻击面，增强防御能力。

目前已正式发布《云安全基线》、《运维安全基线》、《客户端安全基线》，并持续迭代升级。配套发布《隐私保护规范》和《密码算法使用规范》，统一规范数据敏感等级及对应安全管控要求，加密算法和强度使用规则。

云安全基线：

乐橙云实施“安全基线”计划多年，坚持以“Security by Design”和“Security by Default”为核心原则，深耕云安全技术，为用户提供充足的安全保障。

安全基线立足并践行安全与隐私设计原则，构建“AAA+CIA+P”的安全要素布局，形成覆盖系统安全、应用安全、数据安全、网络安全和隐私保护的系统化保护框架。

“AAA+CIA+P”安全要素布局具体为：

- AAA：认证（Authentication）、授权（Authorization）、安全审计（Audit）
- CIA：保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）
- P：隐私保护（Privacy Protection）

图：云安全基线

安全基线作为华橙的重要企业标准之一，是安全开发生命周期的重要组成部分，已融合到研发质量保障体系中，帮助乐橙云遵循安全管控要求、落地技术措施。

06

应用与业务安全

乐橙云在应用架构设计中充分评估安全风险，并在应用部署中实施安全增强措施，乐橙云应用在开发、测试、上线过程中遵守企业安全标准，以保障数据安全为目标，安全合规为基础，充分考虑用户体验，提供个性化的应用服务。

6.1 账号安全

乐橙云针对账号注册、账号登陆、密码找回、账号注销等账号生命周期环节进行了全面的威胁建模与风险分析，对风险场景制定了相应的管控策略和技术方案，并严格落实安全策略与技术措施，确保用户的账号安全。

- 默认使用强口令策略，包括对口令长度、复杂度以及集成弱口令库等限制。
- 基于 Digest 认证，Digest 认证技术是一种挑战式的认证方法，基于对密码和随机数（一次有效）的 HASH 运算，确保认证过程的机密性和不可重放性。
- 传输过程使用标准 HTTPS 加密通道。
- 集成第三方验证码，自动识别用户账户攻击行为，通过拖动滑块等方式，防止机器批量注册，批量撞库登录等风险。通过 AI 等技术手段，识别非用户行为，定点锁定用户账户。
- 通过二次短信校验帮助用户找回密码。
- 注销后及时删除用户个人数据及关联数据。

6.2 API 安全

乐橙云整体采用微服务架构设计，提供标准的 RESTFul API 接口。考虑到 API 对云服务承载的重要功能和其在应用层面临的安全威胁，乐橙云采用多重机制和安全措施对 API 进行重点保护，包括：

- 认证鉴权：乐橙云的 API 请求都会通过与后端的 IAM 服务进行身份验证，仅允许经过鉴权的用户访问相关信息。用户通过 API 接口来管理账号下的 IoT 设备，所以乐橙云对不同 API 或者 API 中包含的执行命令进行二级权限管理。当用户调用 API 管理设备时，不仅需要通过 IAM 的认证鉴权，还需要对命令的执行权限进行校验。当前的认证

方式支持 Token 认证和 AK/SK。

1) Token认证：认证请求会包含一个认证的Token，该Token值由用户通过使用用户名及密码调用IAM接口获取。在Token获取之前，乐橙云需通过集成了第三方防人机、防暴力破解工具的检测。为防止Token被滥用、盗取，设置了合理的Token失效时间。

2) AK/SK：请求会包含AK/SK鉴权信息，用于游客模式的用户请求处理，并定期对AK/SK进行更新。

- 签名摘要：乐橙云采用金融级加密方案对每个 API 请求进行加密。并且在签名摘要的计算过程中融入了防重放攻击、防暴力破解，提升接口调用的安全性。
- 传输保护：API 调用时使用 TLS 加密以保证传输链路的机密性。并且支持 IoT 设备和乐橙客户端对乐橙云平台进行证书校验，确保 IoT 设备、客户端与乐橙云平台连接的安全性。
- 流量观测：乐橙云采用了云 WAF、API 频率检测、流量染色等技术提高用户访问乐橙云的高可用性和稳定性。

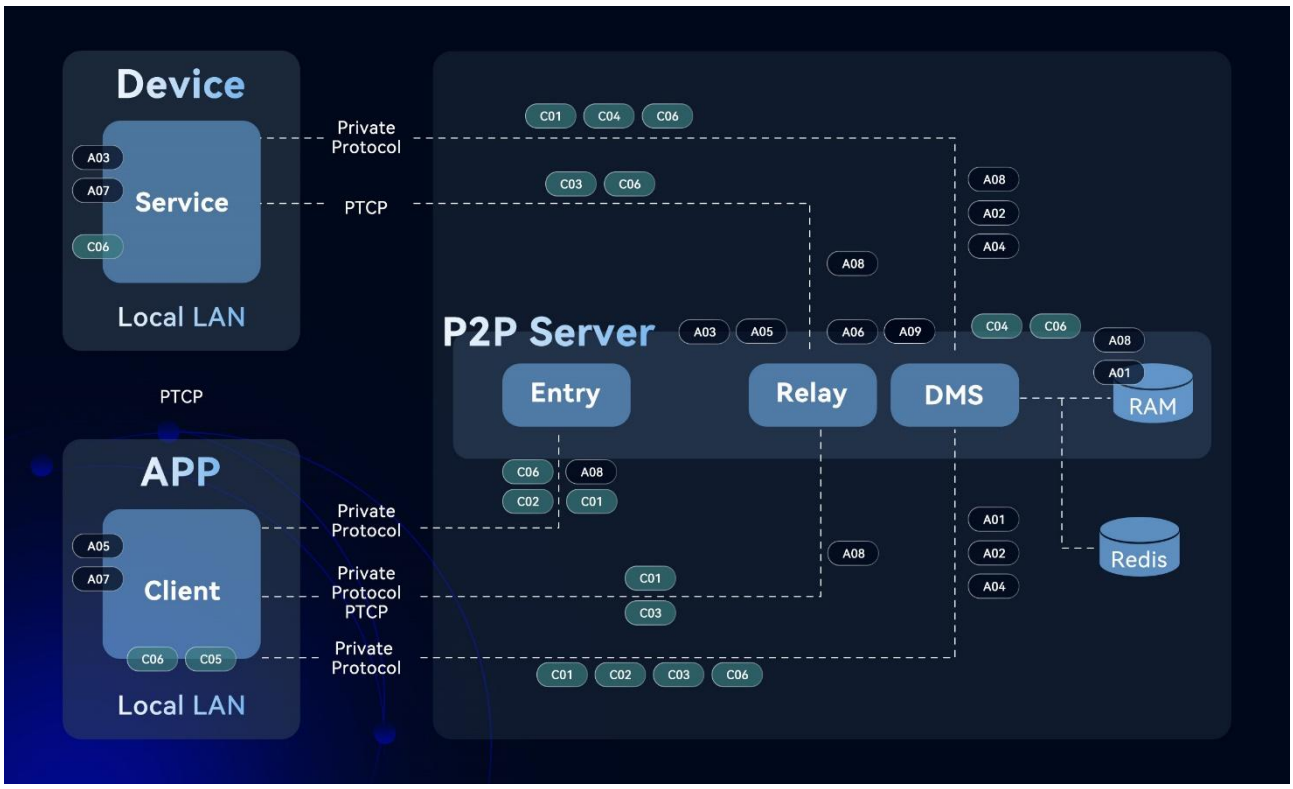
3) API频率检测：为用户的API接口制定次数配额和调用频率阈值。一旦用户的请求次数/频率发生异常，会立即产生报警消息并通知相关人员进行处理。

4) 流量染色：支持API请求灰度上线，对将流入的API请求进行分类，指向指定的后端灰度服务。

6.3 P2P 安全

乐橙云支持 P2P 技术，P2P 技术提供了用户通过公网远程安全地访问部署在局域网内的设备，实现设备点对点服务，提高资源利用率和访问效率，降低云服务运营成本，推动 IoT 互联互通能力。然而，利用 P2P 技术提升用户体验，推动物联网节点互联的特性时，对保障 P2P 服务架构体系的自身安全性也带来了极大的挑战。以下结合资产识别和安全控制来

阐述 P2P 安全防御体系。



图：安全策略

- 资产识别

- 设备信息（A01）：设备信息是建立 P2P 业务通道所必须的与设备相关的信息，其中包括设备唯一标识，设备公网地址和设备业务服务端口。
- 设备公网地址（A02）：在客户端请求与设备建立 P2P 通道的触发下，设备动态建立外出公网地址，该地址代表了穿越 NAT 访问设备的一个通道，以供客户端与设备建立点对点访问通道。
- 设备准入凭证（A03）：P2P 云服务器为了防止恶意使用者滥用服务资源，出厂时为合法设备植入了准入凭证，只有拥有该凭证的设备，才能注册到 P2P 云服务端，确保接入设备的身份可信。
- APP 公网地址（A04）：在用户期望通过 P2P 访问设备时，APP 主动建立外出公网地址，该地址代表了穿越 NAT 访问 APP 的一个通道，用于和设备建立点对点访问通道。
- APP 准入凭证（A05）：P2P 云服务器为了防止恶意使用者滥用服务资源，APP 发布程序中携带了 APP 准入凭证，只有拥有该凭证的 APP 才能接入 P2P 云服务并使用云服务资源，保证接入 APP 的身份可信。
- 传输加密服务器私钥（A06）：该私钥属于服务器专有，用于和设备及 APP 建立加密通信通道使用，即在建立加密通道时协商对称加密密钥，该私钥是加密通道的信任根。

- 传输加密客户端私钥（A07）：该私钥属于设备端或 APP 专有，用于和设备及 APP 建立加密通信通道使用，即在建立加密通道时协商对称加密密钥对称加密密钥，该密钥在系统中是有设备端或 APP 动态生成，而非固定长久保存。
- 转发节点绑定凭证（A08）：当 P2P 打洞失败的情况下，为了保证两端通道依旧能够建立成功，P2P 服务实现了转发业务，每一个通道都拥有一个专属节点，代表了双方通信的专属通道，而转发节点绑定凭证是用于保护通道使用权，不被恶意攻击者利用转发节点访问私网中的设备或 APP。
- 服务资源（A09）：P2P 服务资源是指云端的服务计算能力、内存等用于服务所必须的基础能力，该资源支撑了相应体量的 P2P 服务能力，也是云服务提供商的基础运营成本。

- 安全控制

- 准入控制机制(C02)：P2P 云服务扩展了 WSSE 认证机制对设备和 APP 进行准入控制，WSSE 利用了时间戳、准入凭证、随机数等的 HASH 计算，实现身份认证的同时，保证消息的不可重放性和保密性。
- Relay 点对点凭证校验（C03）：由于网络环境限制，会存在一些场景打洞失败的情况，无法实现点对点交互，P2P 服务云提供了交互中转能力，为了避免恶意攻击者利用该转发节点，穿透目标设备或 APP 所在 NAT，Relay 节点设计了身份凭证校验机制，保证 P2P 转发通道合法用户才能实现数据转发。
- Dos 告警通知（C04）：P2P 服务云内部将会实时监控服务运行状态，当发现以下（不限于）异常状态时，将会通知运维人员，以保证及时处理服务异常：内存异常、CPU 异常、存储异常、服务异常、流量异常。
- 代码模糊化（C05）：为了保护 APP 程序的一些保护逻辑机制不被恶意攻击者研究，我们对 APP 的固件进行了代码模糊化处理，提高逆向攻击成本。
- 数据校验（C06）：APP/设备/P2P 服务云的数据交互，都有严格的数据校验，避免恶意攻击利用非法参数对程序或服务进行攻击，实现内存溢出、代码注入等攻击模式。

6.4 客户端安全

基于国内外法律法规、业界标准、监管要求、威胁建模、技术分析，并结合乐橙的业务情况整合成客户端安全基线，并强制将安全基线纳入需求列表，确保客户端满足安全合规要求、保护用户数据、增强系统防御能力。乐橙的客户端分别从技术与合规的以下方面落实了安全防护和隐私保护措施。

- 身份认证安全：包括登录认证要求、密码重置、登录防爆破机制、客户端密码设置、密码组成规范等。
- 数据传输安全：包括加密传输、证书校验、配套设备安全。
- 数据存储安全：包括存储位置要求、存储加密要求、日志上传合规、日志内容脱敏、密码算法要求等。
- 数据展示安全：数据脱敏展示等。
- 客户端静态安全：升级包完整性校验、安装包签名、代码保护、禁止密钥硬编码、多余功能/接口移除等。
- 安全策略：APP 组件安全设置、AndroidManifest.xml 安全配置、Webview 安全配置、so 编译栈保护、地址空间随机化技术、防触摸劫持、敏感界面防录屏/截屏、TargetSdkVersion 配置等。
- 运行时安全：root 检测、模拟器检测、动态调试检测、服务端口开放限制、输入参数校验、内容安全管控等。隐私保护：包括隐私政策文本及集成要求、个人信息收集合法透明及最小化要求、权限申请明确告知及最小化要求、针对第三方 SDK 的合规审查、对用户权利的保障、隐私友好设置、法律合规遵从、应用准入资质等。

6.5 业务安全

账户安全管理

具备识别登录终端设备变化、地理位置变化、频繁登陆等异常行为的能力，提示用户确认操作的真实性并记录登陆日志，以避免用户账户被盗用，滥用等风险。

内容安全管理

使用业务文件类型识别和病毒扫描、木马扫描引擎，识别上传文件的安全风险。通过集成第三方内容过滤机制，识别色情、暴恐、涉政、广告、辱骂等违法违规字样，并且能够结合行为策略管控灌水、刷屏等恶意行为。

07

安全组织和人员

为了不断提升员工的信息安全与网络安全意识，保障业务的合规运营，华橙网络将相关安全要求贯穿至员工招聘、入职培训、上岗培训、持续培训、岗位变动和离职等各个环节，将安全工作落实到每一位员工的日常工作中。

7.1 安全组织架构

华橙网络通过自上而下的安全组织机构，保证安全目标、安全策略和安全战略规划的一致，为有效落实云安全战略，推动公司安全与合规建设提供所需的资源。

在组织管理层面，成立了公司级的合规管理委员会，直接决策和批准网络安全战略，负责全面领导、管理并监督网络安全有效实行。

在隐私合规层面，聘请有丰富安全实践经验的数据保护负责人，负责数据安全和隐私保护事务。同时，成立了网络安全与数据保护合规小组，包括法务代表、网络安全代表、信息安全代表、市场代表、交付代表、产品线代表，持续对标业界领先法案和标准，以主动合规和持续内部审计的策略来提高产品的合规性和安全能力。

在安全技术层面，设立专门的安全团队，指导和评价公司安全设计、安全方案、关键安全技术、安全开发生命周期管理、安全风险管理和安全运维工作，以及支撑安全事件的应急处置。

图：华橙网安与数据保护合规组织架构

7.2 安全教育培训

华橙网络从意识教育普及、安全能力培训、宣传活动开展、安全能力考核四个方面开展员工安全教育培训：

- 意识教育普及：定期开展全员信息安全意识培训及针对关键岗位人员的网络安全和隐私合规培训，要求员工了解公司的政策和制度，知晓个人需要负担的责任和义务，并承诺按要求执行。
- 安全能力培训：定期针对公司安全骨干进行集中安全技能培训，持续提升安全骨干的安全能力，并赋能各自团队，最终提升所有员工的安全能力。
- 宣传活动开展：开展形式多样的安全宣传活动，包括信息安全专项行动，安全与合规典型案例宣传等。
- 安全能力考核：通过员工学习平台，每半年度开展例行信息安全考试，传递公司在信息安全及隐私保护领域的要求，以此提升员工安全意识和能力水平。

7.3 人员安全管理

员工在入职时需签署员工保密协议、参加并通过信息安全考试。机要岗位人员需额外签署机要岗位保密协议。

公司安全流程制度充分考虑落地执行，对过程的活动、角色、职责进行了明确的定义。遵循最小权限和职责分离原则，通过审批流程授予员工资源访问权限。在员工转岗或离职时，通过加签工单审核节点，确保权限及时回收。保存完整的过程记录，供安全团队定期审计。

08

安全工程能力

乐橙在 SDLC 安全开发生命周期管理实践过程中积累了安全工程能力和安全管理经验，结合持续集成，持续交付，持续部署模式，积极推行快速迭代的 DevOps 流程，并引导 DevOps 逐步向 DevSecOps 演进。

图：安全工程

8.1 需求分析

- 根据业务场景、数据流图进行威胁建模。当识别出威胁后，安全团队会根据消减库制定消减措施，并完成安全方案设计。威胁消减措施最终将转换为安全需求、安全功能。
- 采用主流工具为项目提供需求管理、任务管理等功能，准确把控每个迭代进度。

8.2 安全设计

- 系统对接 LDAP 域账号，统一认证入口。
- 系统根据组织的具体需求、合规性要求和安全威胁进行数据分类分级，并采取适当的安全措施来保护数据的机密性、完整性和可用性。

8.3 安全编码

- 研发代码遵循对内发布的安全编码规范。使用静态代码扫描工具，其结果数据通过质量

门限进行控制。云产品、云服务在发布前，均需完成静态代码扫描的严重告警清零。

- 引入 SCA 软件成分分析工具遵循开源管控要求，完成开源协议合规、开源漏洞扫描，高危风险及时清零。

8.4 安全测试

- 测试、研发人员可协同参与测试用例的编写，确保测试需求的实时同步。
- 服务发布前经过多轮内部安全测试、渗透测试，安全团队通过漏洞管理系统跟踪漏洞修复。

8.5 部署/发布

- APP 加固对 APP 进行加密和保护，增强 APP 的安全性，防止恶意攻击和盗取敏感信息。
- 建立乐橙安全应急响应中心，邀请外部白帽黑客持续对乐橙产品及服务进行软硬件的渗透测试，并对提交的漏洞及时排期修复。

建设 SIEM 系统实时监测和检测各类安全事件，快速响应并及时处理安全威胁。

09

安全运维&运营

面向资产的安全风险管理是乐橙云核心安全管理体系框架之一。

- 考虑到云上资产数量庞大、变化频率快的特征，乐橙建立了自动化资产管理系统，定期更新云上资产。
- 依据 NIST SP 800-37、ENISA 云安全风险评估、ISO 31000、GB/T 20984 等国际国内标准，制定网络安全风险评估标准，并通过识别、分析、处置、监控环节持续治理风险项。

乐橙云运维团队负责业务的部署、扩容、变更、监控等操作，运维过程需遵守安全运维规范和安全运维基线。

9.1 特权账号管理

日常业务活动不允许使用特权账号，运维人员使用运维账号接入乐橙云管理平面，根据人员职责进行权限分配。

- 特权账号仅在密码和 MFA 验证码均验证成功后启用，密码和 MFA 由不同人员保管。
- 通过 VPN 隧道连接至内网，完成 AD 域认证后，方可进入管理平面。
- 运维账号与员工 ID 一一绑定，使用双因子认证。
- 通过独立的安全团队定期审计，检验账号的必要性和权限的合理性。
- 定期更新特权账户口令密码，并且要求口令使用强密码降低被破解的风险。

9.2 操作安全管理

运维通过堡垒机统一管理云主机、登陆密钥，避免密码、密钥泄露。堡垒机登录强制开启双因子认证。人员操作都有录屏，便于事后审计。

9.2.1 容量管理

在对容量进行监控、预测与规划时，考虑如下几个方面：

- 根据 SLA、业务备份和恢复要求以及容量监控、业务预测结果，制定资源服务对象的监测范围和指标，以及监测周期、阀值、方法和技术等。

- 根据容量监测数据，进行容量分析，分析现有容量与服务级别协议之间的差距，并提出改进建议。
- 对信息系统进行持续的容量监控，一旦发现异常会及时预警，并实现动态调整和管理。

9.2.2 变更管理

变更操作遵循统一流程化管理要求，通过变更前测试保证变更过程不影响业务的稳定性和连续性。变更流程负责人定期分析变更质量，并对失败变更进行分析评估，定期对流程进行回顾、优化，回顾内容包括关键衡量指标、流程执行效率和流程支持工具的有效性等内容，确保对变更管理流程的持续改进。

9.2.3 威胁防御

安全扫描：

- 定期执行安全扫描，包括 WEB 站点漏洞扫描、应用和服务漏洞扫描、主机漏洞扫描、软件成分分析等。
- 漏洞管理：通过内部安全活动和外部安全研究者反馈，及时发现网站或业务系统的漏洞，并统一管理安全漏洞。
- 安全专员全程跟进漏洞的识别、分析、分配、跟踪、验证直至漏洞关闭。
- 漏洞管理遵守应急响应 SLA 要求。

补丁管理：运维人员遵循《系统补丁管理制度》，规范化补丁更新周期、时间点、测试、操作、备份及回滚，确保补丁的及时、有效升级。

9.3 安全日志及事件管理

9.3.1 日志分析与告警

乐橙云使用 ELK 技术构建了 SIEM 系统，对业务日志、系统日志、安全日志进行收集、关联、分析，制定安全规则自动识别异常事件（包括内部管理系统特权账号的启用，账号创

建、修改、删除，账户异地、异常时间段登陆，爆破攻击、网络攻击等)，以告警方式通知责任人和安全团队，通过自动创建电子流程单跟踪问题闭环。乐橙云服务中的安全日志至少保存 180 天，可用于实时查询、审计和事后回溯。

9.3.2 事件管理

乐橙云遵循公司制定的事件管理流程，对事件实施分级评估。将事件分为特别重大、重大、较大和一般四个等级。采用保护、检测、响应和恢复的方法论提供技术保障能力，事件处理遵守应急响应 SLA 要求。

9.4 业务连续性

为消除关键经营活动出现中断的风险，避免遭受重大故障或灾难，乐橙云通过运维平台对云平台的主机、应用、服务、网络等实施实时监控，结合业务故障的自动化报警流程，通过多服务热切换保障服务不中断。除此之外还组织开展业务连续性计划演练和业务影响分析（BIA)，持续改进业务连续性策略和 SLA 指标。

9.4.1 灾难恢复

采用主从数据实时热备份、冗余存储和多地备份的方式，保障业务数据安全可靠，持续可用。并对备份情况进行监控和验证。

同时针对业务系统，多链路备用系统，以实现快速应急切换。

9.4.2 应急预案

内部建立对各类型资产、安全及隐私合规风险的应急方案措施，以《业务连续性管理程

序》为依据执行，通过有序、高效地应急处理，确保业务的快速恢复。应急方案包括了事前的预案流程、监控和故障应对手段。事中通过系统监控审查记录，提供足够资料用于事件分析。事后优化处理流程方法和应急预案，提升问题处理、分析和回溯能力。

9.4.3 应急演练

根据重要程度和业务实际情况各业务部门定期开展数据库异常恢复、云厂商切换、用户数据泄露处置等安全及合规应急演练，为应急响应工作提供技术、能力和经验储备。

9.4.4 应急值守

乐橙云运维人员会在各节假日排班进行人员值守，确保节假日期间乐橙各线上系统正常运行，如出现异常情况将及时处理并恢复。

9.5 运维安全管理

乐橙云定期开展运维安全审计，输出运维安全审计报告，并在规定期限内完成整改。乐橙运维安全审计依据《运维安全基线》开展，审计主题包括：资产统计与变更、网络安全、服务器安全、内部系统管理、账户和权限管理、配置管理、安全部署、漏洞管理、云厂商控制台安全配置、补丁管理、安全监控、备份与恢复、应急事件处置和运维操作权限等。

10

未来展望

10.1 新兴技术对网络安全和隐私的影响

随着技术的迅猛发展，新兴技术对网络安全和隐私产生了深远的影响。特别是在 AIoT（人工智能物联网）领域，新技术不仅推动了行业的快速发展，同时也带来了新的安全挑战和隐私问题。下文会讲述几项关键新兴技术对网络安全和隐私的影响。

10.1.1 人工智能（AI）

人工智能技术在 AIoT 系统中的应用具有双重效应。一方面，AI 可以增强网络安全性，通过机器学习算法分析海量数据，识别网络威胁和异常行为，从而实现自动化安全监控和事件响应。另一方面，AI 也可能被恶意攻击者利用，开发更复杂的攻击手段，如深度伪造（deepfake）和自动化攻击工具。这种双刃剑效应要求我们在使用 AI 技术增强安全性的同时，必须防范其可能被滥用的风险。

10.1.2 物联网（IoT）

物联网设备在 AIoT 系统中起着关键作用，但它们往往面临着安全性问题。大量低成本 IoT 设备缺乏足够的安全防护措施，容易成为网络攻击的目标。一旦这些设备被攻破，不仅会导致数据泄露，还可能被用来发起大规模的分布式拒绝服务（DDoS）攻击。此外，IoT 设备采集的海量数据中包含大量用户隐私信息，如何有效保护这些数据成为一项重大挑战。

10.1.3 区块链

区块链技术因其去中心化和不可篡改的特性，被广泛应用于 AIoT 系统的数据管理和交易记录。然而，区块链技术也面临智能合约漏洞、51%攻击和私钥管理等安全问题。尽管

区块链可以提高数据的透明度和可追溯性，但公开的交易记录可能会泄露用户行为模式，威胁隐私安全。因此，在 AIoT 系统中应用区块链技术时，需要综合考虑其安全性和隐私保护。

10.1.4 通信 6G 网络

第六代移动通信（6G）技术的发展也为网络安全和隐私保护带来了新的挑战。6G 通信网络将实现全球无缝覆盖和高速度、低延迟的通信，但也面临着更多的安全威胁和攻击方式，如黑客攻击、网络钓鱼等。

10.1.5 边缘计算

边缘计算将数据处理能力从中心云端下沉到网络边缘，极大地提高了 AIoT 系统的实时响应能力。然而，这也带来了新的安全和隐私问题。边缘设备通常具有较低的安全防护能力，容易成为攻击目标。此外，边缘计算中的数据处理和存储也面临数据泄露和未经授权访问的风险。因此，需要采用强大的加密和访问控制措施，保护边缘计算中的数据安全和隐私。

10.2 面向未来

华橙网络作为以视频服务为核心的智能物联网服务商和解决方案提供商，始终秉承客户第一的原则，非常重视用户的个人信息安全和隐私保护，并采取一切合理可行的措施保护个人信息安全，力求为客户提供一个更安全健康的乐橙云环境。

我们将持续重视网络安全和隐私保护，为此持续投入专项资金，全面提升安全意识与能力，为产品提供充分的安全保障。公司通过内部建立的专业的安全团队，为产品的设计、开发、测试、生产、销售与维护持续提供了全生命周期的安全赋能与管控。我们的产品在坚持

数据最小化、服务最小化、严禁后门植入、去除非必要不安全服务的同时，将不断引入创新的安全技术，努力提升与完善产品的安全保障能力，更好地满足用户不同场景的安全需求。

公司将利用已成立的网络安全响应中心 ISRC（Imou Security Response Center），持续解决网络安全问题，为全球客户提供可靠、安全的解决方案，包括提供安全通告和预警、漏洞上报和响应流程，分享安全建议和研究成果等。

我们将持续关注新兴技术的发展，加强与行业伙伴的合作，共同推动云安全和隐私保护技术的发展，为用户提供更安全、更可靠的云服务和解决方案。