萤石云安全白皮书 v1.0

目录

1. 萤石介绍

萤石，安全智能生活主流品牌，利用智能硬件、互联网云服务、人工智能（AI）和机器人等技术，努力为用户打造一个智能化的工作、生活和学习环境，让人们在智能技术营造的安全、便捷和绿色的居住环境里，享受科技带来的轻松、舒适和愉悦的生活。

萤石构建“1+4+N”以安全为核心的智能家居生态，以萤石云为中心，搭载包括智能安防、智能入户、智能控制、智能机器人在内的四大自研硬件，开放对接环境控制，智能晾晒，智能影音，智能门禁，智能会议等子系统生态，实现住宅、办公室、商铺、学校、酒店等场所的全屋智能。同时利用互联互通的萤石云开放平台，与合作伙伴分享智能视频的云平台服务能力，共同打造物联网云生态。

2. 安全责任

2.1. 萤石云的安全责任

萤石云通过选择全球知名的云主机服务商亚马逊、阿里云等全球一流云计算平台，确保安全管理和运营的基础设施，物理设备的安全。

萤石云安全覆盖数据安全和云服务安全。萤石承诺利用其安全团队以及全球范围内知名的安全服务厂商的专业攻击防护技术经验，提供云平台的安全运维和运营服务，切实保护萤石云的安全运营，以及保障客户、用户隐私和数据的安全。主要覆盖但不限于如下：

- 数据安全：指客户在云计算环境中的业务数据自身的安全管理，包括收集与识别、分类与分级、权限与加密以及隐私合规等方面；
- 访问控制管理：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；
- 云服务安全：指在云计算环境下的业务相关应用系统的安全管理，包括应用和服务接口的设计、开发、发布、配置和使用等方面。

2.2. 客户的安全责任

客户在使用萤石云的解决方案的时候，需要严格按照萤石的安全配置和接入要求执行。同时客户需要保证自己的云端、客户端或者硬件产品本身的安全性。基于萤石 SDK 开发的 APP， 萤石仅提供技术支持，但是无法提供任何安全保障。对于基于萤石 OEM(公版)APP(无任何定制场景)的数据安全合规、隐私政策等相关信息，萤石会提供模板供客户参考，具体

上线的隐私政策声明以及法律合规性由客户自己负责，必要时候，萤石安全团队愿意提供安全解决方案的帮助和咨询服务。

3. 合规性

萤石遵守国际权威的安全标准及行业要求，并整合到内部控制框架中，在云平台、APP、硬件产品等需求实现过程中严格执行。同时，萤石还与独立第三方安全服务、咨询和审计机构进行合作，验证和保障了萤石云平台的合规性和安全性。

目前，萤石已经通过全球多个咨询和审计机构的信息安全和隐私合规的认证，是一家拥有多个认证的 IoT 解决方案提供商。萤石承诺，将持续地进行多个信息安全和隐私安全相关的认证和合规证明，为客户的数据和隐私安全保驾护航。

目前，我们的认证和合规凭证如下所示：

3.1. ISO 27001

ISO 27001 是信息安全管理体系（ISMS）国际标准，为各类组织建立并运行信息安全管理体系提供了最佳实践指导。按照标准要求：

- 基于业务风险的方法，建立、实施、运行、监控、评审、维护和改进信息安全；
- 为了确保信息的机密性、完整性和可用性，设立了相应的组织架构，建立了体系化的安全管理制度，并提供资源保障；
- 遵循 PDCA 方法，持续改进信息安全管理。

3.2. ISO 29151

ISO 29151 作为国际通用的《个人身份信息保护实践指南》，基于 ISO27002 的准则，增加了为保护 PII 量身定制的隐私保护准则，准则分类如下：

同意和选择

目的、合法性和规范

数据最小化

使用、保留和披露限制

准确性和质量

公开、透明和注意

个人参与和访问

问责制

信息安全

隐私合规性

萤石获得了由 DNV GL 颁发的 ISO 29151 隐私安全认证，建立了满足与保护个人可识别信息安全有关的风险和影响评估的控制目标，控制措施和实施措施，进一步印证了萤石在国际隐私权和数据保护标准方面的承诺。

3.3. CSA-STAR

CSA STAR 认证是一项全新而有针对性的国际专业认证项目，旨在应对与云安全相关的特定问题。以 ISO/IEC 27001 认证为基础，结合云端安全控制矩阵 CCM 的要求，运用成熟度模型和评估方法，为提供和使用云计算的任何组织，从沟通和利益相关者的参与；策略、计划、流程和系统性方法；技术和能力；所有权、领导力和管理；监督和测量等 5 个维度，来综合体现萤石云的安全管理和技术能力。

3.4. ISO 20000

ISO 20000 是面向机构的 IT 服务管理标准，目的是提供建立、实施、运作、监控、评审、维护和改进 IT 服务管理体系(ITSM)的模型。

萤石获得了由 DNV GL 颁发的 ISO 20000 认证，意味着萤石建立了标准的服务流程并严格执行，将云平台服务规范化，从而提高服务的可用性、可靠性和安全性，为业务用户提供高质量的服务，持续优化服务流程来提升服务水平和业务满意度。

3.5. 服务组织控制（SOC）审计

萤石云获得四大会计师事务所之一安永出具的 SOC1 Type2 报告，是通过独立的第三方审计师对萤石云提供的云服务进行检查验证而出具的独立审计报告。SOC 审计作为一项相当严苛的内控审计，尤其是在用于保护云存储和处理信息的保密性和隐私性上，可以较为充分证明萤石内部控制设计合理性和实施有效性。

4. 数据安全

4.1. 萤石云数据安全体系

萤石云数据安全体系从数据安全生命周期角度出发，采取管理和技术两方面的手段，进行全面、系统的建设。通过对数据生命周期（数据收集、存储、加工、传输、共享、删除）各环节进行数据安全管理管控，实现数据安全目标。

在数据安全生命周期的每一个阶段，都有相应的安全管理制度以及安全技术保障。

4.2. 数据所有权

萤石为客户定制的服务中，客户是数据控制者，客户需要保证数据使用的合规性，萤石是数据处理者，萤石将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个人数据，所有数据处理行为对客户透明。因此，在符合法律法规、《隐私政策》的基础上，萤石可帮助客户和用户保障数据的保密性、完整性、安全性。

4.3. 多副本冗余存储

采用分布式架构，所有业务服务器同时部署于同城不同区域的三个机房，数据库等数据存储服务采用多副本模式（最少保证二个实时副本），并实时进行数据备份。从物理层面保障了数据和服务的高可靠性和高可用性。

4.4. 用户设备数据安全

在设备与云端交互方面：

- 数据加密：使用 AES128 加密数据内容。
- 身份识别：萤石自有算法保障设备连接认证，请求授权，指令下发等多重交互认证、访问控制和有效授权的保障。
- 动态密钥：一机双码，包括动态密钥和动态口令，保障设备安全。
- 通道加密：使用 TLS1.2 加密传输协议。
- 安全芯片：部分芯片支持选择使用带安全芯片版本，用来安全存储硬件授权信息和加密 key 等。

在设备局域网内交互方面：

- 数据加密：使用 AES128 加密数据内容，在局域网内传输。
- 动态密钥：配网时算法动态分配。

4.5. 企业数据安全

萤石云会对企业数据进行隔离，保障客户数据的安全性。同时萤石云针对不同的业务场景提供不同的数据存储服务对客户或用户的敏感数据使用 AES128 进行加密存储，部分敏感数据会进行必要的脱敏处理，同时密钥通过密钥管理中心进行统一的安全管理和分发。

4.6. 残留数据保护

曾经存储过客户数据的内存和磁盘，一旦释放和回收，其所有信息将被自动进行零值覆盖。同时，任何更换和淘汰的存储设备，都将由云服务器基础设施提供方统一执行消磁处理并物理销毁之后，才能运出数据中心。

4.7. 隐私保护

萤石云平台践行“一切以用户价值为依归”的经营理念，尤其重视与客户建立长久持续的信任关系。萤石以坚实的技术基础和完备的运营管理机制，确保用户和客户数据得到全面的保障。萤石云将严格执行萤石公开发布的《隐私政策》，切实保护用户隐私。

法律和规范赋予用户个人信息相关的权利（来自于《中华人民共和国网络安全法》,《信息安全技术-个人信息安全规范》（GB/T 35273:2017），GDPR）：

1. 知情权：用户有权了解数据处理的目的、依据、来源、处理过程、所享有的权利等信息。
2. 访问权：用户有权获取和确认与其相关的个人信息。
3. 纠正权：用户有权纠正和完善与其相关的个人信息。
4. 删除权（被遗忘权）：用户有权要求删除与其相关的个人信息。
5. 限制处理权：用户有权限制对其相关的个人信息进行的处理活动。
6. 可移植权（可携性）：用户有权以结构化、通用和机器可读的格式接受与其相关的所有个人信息。
7. 拒绝权：用户有权拒绝基于直接营销目的对其相关的个人信息进行的处理活动。
8. 自主决定权：用户有权不受基于自动处理的决定的约束。

确保用户的合法权利与产品功能一一对应：

N	权利	产品上的体现
1	知情权	在获取用户数据的时候需要告知用户所采集的数据以及获得用户明确的授权（注册的时候的服务协议，隐私政策，权限说明的强提醒用户阅读和授权，以及我方协议有所变化之后的强提醒用户再次的阅读和授权，增值服务需求获取额外数据时的强提醒用户采集的数据情况和获得授权）
2	访问权	用户可以查询到自己相关的数据，无论时通过产品还是通过售后的方式。
3	纠正权	用户可以修改包括手机号码，邮箱在内的所有用户自己相

		关的数据。(包括但不限于，身份信息，地址，头像，昵称)
4	删除权（被遗忘权）	一定要实现“注销账号”并且删除用数据的功能
5	限制处理权	用户可以选择自己的个人数据的使用场景
6	可移植权（可携性）	提供用户获取平台上所有自己相关的数据，无论是通过APP自助获取，还是通过客服和技术支持的方式。
7	拒绝权	非提供用户服务的必要信息，用户有权拒绝提供和拒绝授权使用，如基于个人信息的推广的个性化的广告。
8	自主决定权	所有需要用户确认授权的位置，不能默认打勾确认，必须是用户主动确认的。

数据分类：区分个人数据和平台信息数据，针对个人数据，使用敏感程度和密级进行分类。

4.8. 数据存储区域

五大数据中心：中国机房、北美机房、南美机房、和欧洲机房、新加坡机房（各数据中心之间物理隔离不互通）。根据用户所在地区提供相应的数据服务。

中国：数据保存在中国杭州电信 IDC 机房，由萤石提供基础云计算支持。

北美：数据保存在美国弗吉尼亚北部，由 Amazon AWS 提供基础云计算支持。

欧盟国家：数据保存在爱尔兰机房，由 Amazon AWS 提供基础云计算支持。

新加坡：数据保存在新加坡机房，由 Aliyun 提供基础云计算支持。

其它国家：根据就近原则选择机房存储，后续会逐步开放更多区域机房，目前多个地区的机房在建设中。

5. 安全组织和人员

为了让所有员工不断提升安全意识，更好的保护客户（租户）数据，尤其是用户的隐私数据，更好地保障客户利益和产品与服务信誉，萤石在公司内部建立了**“信息安全、全员参与；关键数据，严谨管控；积极预防，持续改进；客户信赖，稳定运营。”**的管理方针，提高全员的信息安全意识，将信息安全文化融入到企业文化中，将信息安全的工作落实到每一个人；

5.1. 安全与隐私保护团队和人员

在安全技术层面，萤石有专业的安全技术团队来支持萤石云的安全架构、安全设计、安全评估和安全运维工作。在隐私合规层面，萤石设立了隐私保护官 PPO(Privacy Protection Officer)，负责隐私影响评估、隐私需求设计的规则制定并推动隐私保护管理工作的执行，

同时，萤石内部成立了信息安全管理与合规小组，内容覆盖信息安全和隐私保护，小组成员分为决策层、管理层和执行层，分别对应信息安全领导小组、信息安全工作小组及萤石各团队成员。通过自上而下的安全组织机构，保证了安全目标、安全策略和萤石的业务战略规划的一致，为萤石（包括运营和业务利益相关方）提供风险和合规性所需的资源。

5.2. 人力资源管理

萤石的人力资源安全管理框架和公司的整体人力资源管理框架一致，对员工、关键岗位和第三方人员提出了安全的要求，包括入职管理、在职管理、离职管理和人员安全考核管理四个方面，通过主动防范来有效防患或减少因人为原因引起的信息安全事件。

5.3. 安全意识教育

为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，萤石内部发布了《员工信息安全手册》，并以此为基准定期开展网络安全意识教育学习，要求员工持续学习网络安全知识，了解手册上面的的政策和制度。知道哪些行为是可以接受，哪些是不能接受的，意识到即使主观上没有恶意，也要对自己的行为负责，并承诺按要求执行。

5.4. 安全管理体系相关培训

为了让公司全员能够准确理解公司信息安全管理政策，并且有效推动和落实安全策略，萤石安全团队定期对业务人员进行隐私保护合规和数据保护相关的培训。

5.5. 信息安全能力提升

萤石内部会定期的举行安全开发培训和信息安全交流，旨在提升员工的安全技能，确保员工有能力交付安全、合规的产品、解决方案和服务。

6. 云平台安全保障

6.1. 物理安全

萤石作为物联网云计算服务提供商，萤石云平台着力为每一个客户提供安全、稳定、持续、可靠的物理设施基础。萤石云依据数据中心相关的国际标准和监管要求，建立了一套全方位的安全管理体系，从制度策略，到流程管理，并配合严格的监察审计，通过持续改进来保证云平台数据中心的物理和环境安全。

6.1.1. 高可用的基础设施

萤石云平台整合全球最知名的云主机服务商 AWS、Azure 和阿里云等，构建全球服务节点。为客户提供安全、稳定、持续、可靠的物理设施基础。萤石云根据中国企业内外销区域结合海底光缆分布和全球各城市的实测结果,部署覆盖中国、欧洲、北美、南美和新加坡五

个可用区。包含但不限于美国的弗吉尼亚机房；南美的圣保罗机房；欧洲爱尔兰机房；阿里云新加坡机房；

萤石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。

6.1.2. 安全检查和审计

安全事件管理：萤石和 IDC 机房及云服务器供应平台达成物理安全应急预案，并定期组织数据中心工作人员进行安全演练。一旦发生物理安全事件，该预案将能够立即生效并指导相关人员以最大可能保护客户资产。

6.2. 网络安全

6.2.1. 安全架构

萤石云拥有成熟的网络安全架构，包含防火墙、WEB 应用防火墙、入侵检测、RASP、主机防护系统等多重防护机制，以应对来自互联网的各种威胁。

6.2.2. 网络通信安全

萤石云平台上的通信均采用 TLS1.2 安全协议，且实施强制的证书认证的加密保护，包括设备和 APP 与云端的通讯，并且提供的 API 接口也具有完善的 TLS 等安全能力，能够对客户提供端口级别的安全保障。同时，通讯的内容额外使用 AES128 加密。双层加密保护通讯过程的安全。

6.2.3. 网络隔离和访问控制

萤石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、生产网络等的访问控制和边界防护。萤石云确保非授权人员禁止访问任何内部网络资源。所有员工如需从公司网络前往生产网络开展日常运维时，都必须经过堡垒机的严格审批和权限控制，才能使用受限的权限登录生产系统，并且使用全程有审计。

6.2.4. 网络冗余

萤石云数据服务云主机遍布全球多个区域，构建了网络跨地域的灾备能力，能够最大化的减小非人为因素导致的网络故障的业务影响。同时，采用冗余的网络建设方式，同时同城也采用多物理机房部署，能够实现网络的便捷性和流量附和的工程调度，确保网络服务不会因为单点故障而中断，实现同城和跨城容灾。

6.2.5. DDOS 防护

萤石使用自研 WAF 和第三方安全工具对 DDOS 攻击进行检测、阻断和处理，并针对 DDOS

的攻击规模制定了不同的完善措施，保证云平台网络稳定。对于 CC 攻击，内部通过防火墙和 WAF 进行阻断。同时内部通过对所有请求日志的分析，进行异常的 IP 进行检测，动态屏蔽可疑的源地址。

6.2.6. 入侵防护

入侵防护：通过防火墙和 WAF 等设备进行入侵阻断。

主机入侵检测系统：萤石通过使用自研的 HIDS 和第三方的 HIDS 结合的方式来抵御众多外部的攻击，功能包括 WebShell 检测模块，服务器部署了 WebShell 实时检测引擎，能够实时检测、删除和上报 WebShell。主机异常登录检测模块，能够识别机器被非堡垒机登录。不安全基线配置检测模块，能够识别机器是否按照安全基线配置上线。暴力破解检测模块，能够识别到服务器是否被远程爆破，主机漏洞检测模块，能够识别主机的应用漏洞和系统漏洞等。

数据库审计：对数据库的权限进行严格的统一管理和限制，并且对所有数据库的增删改查都进行完备的日志审计。

7. 安全开发周期管理

严格按照安全开发生命周期方法开发云平台及云产品，目标是将信息安全融入到整个软件开发生命周期中。

萤石的开发生命安全周期，全面涵盖了系统开发生命周期的各个阶段。通过安全管理平台进行统一的项目 SDL 实施监控和管理，基本实现全自动化的流程跟踪和自动化安全评级。

7.1. 安全培训

萤石安全团队为开发人员建立常态化的安全培训管理机制，根据测试、发布以及漏洞运营阶段发现的安全漏洞，持续完善安全培训课程。

7.2. 安全需求与评审

需求分析阶段：

产品经理会根据安全团队制定的基线要求作为标准，包括密码安全、认证、加密解密、服务与端口安全、文件上传、配置安全、隐私保护等方面，收集需要满足的安全需求，需要时，安全团队会协助制定安全需求，新应用、旧应用、系统、产品的创立或有变更需求时，若涉及隐私风险，产品经理会按照“隐私设计管理要求”执行，确保将隐私保护措施设计渗透到项目方案中。

需求评审阶段：

需求评审遵循萤石整体的信息安全要求，包括但不限于如下内容：

a) 数据安全：数据收集、传输、使用、存储、清除需要遵循《萤石数据保护管理规范》的要求，保证应用相关数据的生命周期安全；此外应对应用程序接口、跨越多个系统的接口、数据库的数据输入和输出进行常规的完整性校验；

b) 密钥安全：密钥生成、传输、存储、更新、销毁、审计需要遵循《萤石密钥安全管理控制程序》的要求，保证应用相关密钥的生命周期安全；

c) 网络安全：因业务需求而需要开通的服务协议、端口、IP 等应进行安全评审。

d) 权限安全：基于角色的访问控制（RBAC）进行授权，在主题和对象之间实现最小权限策略，确保访问控制列表涵盖所有可能的方案。

e) 业务安全：对应用上线后涉及到的业务规则、流程，产品功能安全进行评估，需要符合国家相关法律法规、网站相关规则等具体要求。产品应当规划采取必要手段或者措施加强对安全风险的管控，如对接安全产品、过滤安全风险名单，采取必要的防控手段等。

f) 技术安全：技术安全评审对应用技术框架、代码漏洞、系统安全等进行评估，需要符合产品安全相关具体要求。产品应当规划采取必要手段或者措施加强对安全风险的管控，如使用安全组件、自觉进行安全代码扫描等，并在出现安全风险及漏洞时，及时响应和防范风险。

7.3. 安全设计

在设计阶段会充分考虑与安全需求相匹配的安全管理和技术手段，基于需求分析和评审的结果，在新开发系统或现有系统版本迭代时，开发团队会在安全团队的协助下进行安全架构设计和威胁建模，充分考虑业务系统保密性、完整性、真实性、可靠性、可用性、不可抵赖性，识别假冒、篡改、否认、权限提升、拒绝服务、信息泄露以及与业务安全、合规相关的风险。

7.4. 安全开发

7.4.1. 代码规范

在整个开发周期中，应用开发/测试活动与生产环境信息资源相隔离，保证线上环境的高可用性。制定安全开发规范和指南，使用安全的方法进行开发工作。

7.4.2. 代码审计

萤石自主开发的代码审计，绑定了萤石的项目发布系统，项目到提测阶段前，自动化进行代码审计测试。自动化化实时跟踪主流漏洞情报，自动更新不安全的第三方组件库，能够第一时间生成规则进行漏洞告警。

7.4.3. 移动扫描

萤石 APP 打包平台，在完成新 APP 打包后，会自动发送 APP 包到移动扫描平台进行扫描，支持安卓和 IOS 的 APP。

7.5. 安全测试和修复验证

萤石安全团队参考 OWASP Top10、第三方漏洞平台、行业安全实践不断完善产品和规则，制定《萤石安全测试用例》，以供测试人员测试。只有通过安全测试并且通过安全发布评审后，系统才能发布到生产环境，能够有效防止产品携带安全漏洞在生产环境运行，测试过程中，禁止使用未授权或未脱敏生产环境的敏感数据。发布过程严格按照安全上线规范对系统进行整体加固。

8. 安全运维和运营

通过萤石的安全运维平台进行统一的管理，采取严格的访问控制、监控审计来确保运维安全。

8.1. 访问控制

8.1.1. 原则

萤石访问控制遵循以下原则：

- 隔离运行：对于不同重要等级、不同用途的网络和信息系统，应采取特定的隔离措施(逻辑隔离或物理隔离措施)，确保各类系统独立运行。
- 最小权限：用户应只拥有完成某项工作所需的最小访问权限，用户权限应与工作职责紧密关联并及时更新。

- 按需审批：系统责任人在授予用户访问权限时，应按需授权避免用户访问权限过大的情况。
- 职责分离：一个用户不能同时承担多个职责冲突的角色，以防止获得过大权限。重要访问动作的请求方、授权方、管理方应实现职责分离。
- 默认拒绝：未经明确授权的用户应默认拒绝访问。

8.1.2. 账号管理和身份认证

萤石使用域账户对员工进行统一身份认证和账号管理，员工在职期间，域帐号唯一且不可变更，使用户与其行为结合，并对其行为负责，确保可问责性。集中下发密码策略，强制密码强度，并要求定期修改密码，对核心系统开启了双因素认证，获取动态验证码进行二次校验。

8.1.3. 特殊访问权限管理

限制并严格控制特殊访问权限的分配和使用，日常业务活动不允许使用特权账号。特殊访问权限按照“按需使用”、“一事一议”的原则分配给用户，即仅当需要时，才为其职能角色分配最低要求；定义特殊访问权限的有效期限，到期则立即回收特殊权限。定期对特殊访问权限授权情况与用户账号进行审核，并保留记录，以确保不存在未授权的特殊权限。

8.2. 操作安全管理

8.2.1. 操作程序

萤石为信息处理设施相关操作活动建立适当的操作职责和标准作业程序（SOP），制定安全策略，以确保员工正确、安全地操作信息处理设施。同时建立有效的访问控制策略，禁止未授权的访问和披露。

8.2.2. 变更管理

所有的变更操作遵循《萤石云变更管理程序》的要求，保证变更过程不影响业务的稳定性和连续性，变更流程负责人每月出具变更管理报表，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。

8.2.3. 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，分析现有容量与当前服务级别协议和预计要求之间

的差距，并提出改进建议；

- 应对信息系统进行持续有效的容量监控，一旦发现异常应及时预警，并实现动态调整和管理。

当出现新的服务级别协议启动时，影响系统容量的变更实施后或新技术、业务、法律和业务流程及其它外部变更影响系统容量时，会重新进行容量规划的管理

8.2.4. 备份管理

在数据备份活动中，按照 RPO 要求，制定数据备份策略，定期对数据进行备份；同时对备份数据设置了严格的权限控制，禁止未授权的访问和使用；定期进行恢复测试和演练，保证数据的机密性、完整性和可用性。

8.2.5. 日志管理

员工对生产系统的所有运维操作必须且只能通过堡垒机进行。所有操作过程完整记录和录制下来，并部署日志服务器统一集中保存。定期进行日志检查审计，针对特权使用、非授权访问的试图、系统故障和异常等内容进行检查审计。对所有可疑或经确认的非法访问行为和企图，及时汇报至信息安全工作小组并采取相应的措施。

8.2.6. 安全基线管理

对信息系统涉及的网络、系统、中间件、数据库等组件设置标准的基线规范；并根据实际情况不断更新和维护，在系统上线前以及运行过程中，通过自动化的方式检测和监控信息系统的基线配置情况，并进行预警、跟踪和管理。

8.2.7. 测试管理

萤石制定严格的环境隔离措施，线上环境与测试环境相分离，禁止使用包含个人信息或其他敏感数据的线上数据用于测试，严禁在线上环境进行压力测试。

8.2.8. 安全威胁防范

安全扫描：每周执行全网安全扫描，包括 WEB 站点漏洞扫描、应用和服务漏洞扫描、主机漏洞扫描等。

安全众测：萤石通过发布奖励的方式激励全社会的安全专家来测试和发现企业自身网站或业务系统的漏洞，及时发现线上存在的高危漏洞，保证安全风险可以快速进行响应和修复，防止造成更大的安全损失。

病毒防范：

1） 萤石的办公终端统一安装防恶意程序的软件，严禁未安装防恶意程序的终端接入公司网络，同时开启自动更新功能。

2） 萤石的服务器端部署防恶意程序软件，并确保防恶意程序软件各相关组件能够正常运行，实时扫描和组件自动更新等功能正常开启。

9. 业务安全与风控

9.1. 账号安全

萤石云服务设计上非常重视用户的账号安全，所以针对账号的注册、登录、密码找回等都进行了严格的安全管控和日志审计，采用验证码，保障人机识别的能力，避免账号暴力破解等攻击行为，使用短信验证码绑定用户常用设备，通过二次短信校验保证用户账号的安全。用户账号等隐私数据的存储都进行了高等级的加密保护。针对撞库、API 滥用等常见账号攻击都有实时的检测和报警机制进行安全响应。

10. 终端安全

10.1. 硬件和固件安全

10.1.1. 通信安全

根据不同硬件芯片的性能，萤石提供不同等级的加密机制，来最大化芯片的安全能力，不论哪种加密机制均保证数据的通信安全。目前萤石模组主要的通讯协议是 MQTT over TLS 和 HTTPS，采用 TLS1.2 和 AES 加密算法保障通信安全，同时针对交互过程中的数据和控制指令进行额外的 AES 加密保护。TLS 启用基于标准 X509 证书强制校验功能，AES 加密密钥使用动态生成的基于设备的，具有唯一性的随机密钥。

同时，萤石关键通讯数据都会使用数据防重放校验、真实性和完整性校验、设备身份校验、访问控制和权限校验等多种数据保护机制。

10.1.2. 固件保护

萤石针对固件进行多重保护：

1.固件防伪校验，萤石固件都会通过萤石的证书进行签名，萤石设备升级前会通过证书校验固件的合法性。

10.1.3. OTA 安全

萤石针对固件升级过程采取了多重保护手段进行保护：

1.在生成固件包时，打包工具会生成一个固件完整性校验信息，该信息由多个变量组成。

2.客户端请求固件时，服务端会下发一个固件下载信息和固件校验信息。该固件校验信息采用安全的 RSA + SHA256 签名算法，并且加入设备唯一的身份密钥信息作为因子，保证传输过程固件无法被篡改。

3.设备端获取固件后，需要计算固件校验信息，并和服务端提供的固件校验信息进行对比，同时解压缩的时候还需要校验打包工具在固件内计算的完整性校验信息。只有完成固件双重校验后，才允许写入固件。

4.固件如果写入失败，或写入后无法正常使用，会自动恢复到原有的固件。

10.1.4. 数据保护

萤石智能门锁产品使用安全芯片来存放智能门锁的授权信息和加密 key。授权信息用以保证对萤石模块和云端进行通讯的安全性和合法性，能够有效防止授权数据和加密 key 被非法人员盗取或篡改。安全芯片内部有安全数据区，在使用过程中，萤石模块会将加密的敏感信息读取到 RAM 中，掉电丢失。同时，模块和安全芯片通讯的时候，都会有临时密钥的加密保护。

非安全芯片版本，为了保障核心数据的安全，本地存储的重要信息，会进行 AES 加密后，存放。

10.1.5. 配网安全

配网前的设备发现，APP 和硬件发出的广播信息，经过 AES 加密的传输。

配网过程中，设备开启由 WPA2 保护的 WIFI 热点，配网信息由 WPA2 加密后传输至设备端，保障了用户网络的安全，减小配网过程的风险。

11. 业务可持续性

11.1. 业务连续性

为消除关键的生产经营活动出现中断，避免其遭受重大故障或灾难的影响，萤石制定业务连续性管理策略、文件化业务连续性计划、组织开展业务连续性计划的演练，以及业务连续性策略和计划的持续改进。通过运维平台对云平台所有的主机、应用、服务、网络等的实时监控，并且有一套完整的业务故障的自动化流程体系和保障，通过多服务热切换保障服务不中断。

11.2. 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。并对对备份情况进行实时的监控和验证。

同时针对业务系统，多链路备用系统，保证能够快速应急切换。

11.3. 应急预案

内部建立对各类型资产和安全风险的应急方案措施，以《萤石业务连续性控制程序》为依据执行，能够保障事后能够正确、有序、高效地进行应急处理，保障工作的正常运转。应急方案包括了事前的预案流程、监控和一系列故障应对手段。事中通过详细的系统监控审查记录，为事后提供足够资料能够快速了解和分析，以及对应的接口人员。事后有一套完善的处理流程方法和应急预案，保障能够快速处理问题，分析问题和责任追责。

11.4. 应急演练

定期实施大型的硬件故障、网络 DDoS、安全事件等内部技术应急演练测试和实战。