纷享销客安全白皮书

北京易动纷享科技有限责任公司

2018 年 11 月

纷享销客
移动销售管理专家

目录

前言

“纷享销客”是一款自主研发的，提供一站式移动销售管理 SaaS 解决方案的产品。通过云计算、移动互联网、大数据、微服务等全新的技术，为企业提供一体化的移动 CRM 解决方案，全面提升营销团队的销售产能和成单赢率，助力企业核心业务的发展升级，保障企业进入安全的移动 SaaS 时代，为企业的安全生产保驾护航！

1 安全战略

纷享销客是企业级服务提供商，对安全的要求，从公司整体战略上就有所规划。为此专门组建信息安全委员会来保障安全政策的推广，加强全司上下的安全意识，完善信息安全体系的建设，每年都会指定专项专款用于保障安全，确保应对各类故障时的服务恢复时间最短，全面保障企业在纷享销客平台上的业务连续性。

2 组织及人员安全

2.1 信息安全委员会

信息安全委员会由 CTO 直接领导，由应用安全、系统&网络安全、安全开发等专家团队组成，并加入各业务线的安全负责人来对接并贯彻安全措施，通过定期沟通、检查、完善安全方面的工作，来高效协作来加强安全管理，应对各种安全威胁，为广大用户提供稳定、健康、安全的工作环境，在安全策略、安全开发流程设计、落实及执行中扮演重要的角色。

2.2 信息安全保障团队

2.2.1 安全专家团队

由应用安全、系统&网络安全、安全开发等专家团队组成的安全专家团队，关注从设计到最终产品实施的整个开发、运营、维护过程，通过开发工具、优化流程、强化意识、安全培训等，保障安全生产。主要职责包括：

1. 联合专业安全厂商，设计、开发和运营入侵检测、攻击防护产品，提供 7*24 小时安全监控，做漏洞扫描与检测等；

2. 依据数据类别及安全等级，设计访问控制策略,通过技术手段制定隔离措施和访问控制管理流程；
3. 依据业务系统访问逻辑，审核访问请求，自动化监控可疑活动（例如：数据的非授权访问及操作）并实时审计，定期复查其执行情况；
4. 通过安全解决方案流程，在产品设计阶段，对功能需求进行安全评审，在产品发布前，进行安全测试以及产品发布后，进行安全回归测试，以保障纷享业务的安全运营；
5. 借助公司内的技术沉淀和外部专业安全机构，定期对纷享销客内部和外部应用进行漏洞检测与扫描，及时发现安全漏洞，并在预期时间内完成漏洞修复；
6. 遵循信息安全事件管理标准,依据数据安全性的危害程度定义安全事件类别和响应流程,提供全天候人工和系统的监控识别、分析和处理信息安全事件的能力;
7. 定期进行演练，评估安全策略可靠性和控制措施的适用性;
8. 定期为纷享员工提供安全意识培训,包括个人准则、信息保护、数据安全认证和安全开发等领域；
9. 积极参与安全论坛与会议，吸取业界前沿的安全技术并保持与外部安全专家、白帽子黑客的交流沟通；

2.2.2 安全审计小组

安全审计小组主要对纷享销客系统化的监测、控制、处理、独立审查，以验证是否满足信息安全体系及标准，通过审计以满足合规性要求，如 GB/T 22080-2008/ISO/IEC 27001:2003、《信息系统安全等级保护基本要求》等。

2.2.3 物理安全小组

物理安全小组主要根据机房安全相关的国家标准，保障数据中心基础设施的高安全性：

GB/T2887 - 2000《计算机场地通用规范》

GB 50174 - 93《电子计算机机房设计规范》

GB 9361 - 88《计算站场地安全要求》

2.3 人员安全

员工在入职前，在国家法律法规允许的情况下，通过一系列背景调查手段来确保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，背景调查手段涉及刑事、职业履历和信息安全等方面，背景调查的程度取决于岗位要求。

3 生产过程安全

3.1 安全政策要求

ISO 27001，推动信息安全体系(ISMS)建立与实施，采用以风险管理为核心的方法管理公司和用户信息，保障信息的保密性、完整性及可用性；安全审计团队依据该安全标准，审核纷享技术方案与技术框架内部信息安全管理，同信息安全最佳实践接轨。

等级保护基本要求：根据国家下发的《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》开展信息安全等级保护工作，主要是指对国家、法人和其他组织及公民的专有信息、公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应与处置。

纷享销客根据国家信息安全相关法律、法规要求，设置与信息安全监控机构之间的联络员，制定实施程序，以确保提供的纷享产品符合国家关于知识产权相关法律和法规要求。

3.2 保密要求

纷享同合作企业及开发者签署保密协议，并通过定期检查识别、记录、评审保密协议中数据安全的相关控制要求（如访问控制、防泄露及完整性要求），防止不正当披露、篡改和破坏数据。

在纷享员工入职后，所有的员工必须签署保密协议，确认收到并遵守纷享安全政策和保密要求，尤其是关于客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，依据员工的工作角色进行额外信息安全培训，确保员工管理的用户数据必须按照安全策略执行。

3.3 软件开发周期安全

1. 人员培训环节：安全工程师给开发人员进行安全开发规范、安全意识培训等，提高其安全意识；
2. 安全需求环节：根据功能需求文档进行安全需求分析，针对业务内容、业务流程、技术框架进行沟通，形成《安全需求分析建议》；
3. 安全开发环节：根据不同的开发框架，开发安全包、提供安全编码规范及安全框架配置规范，避免开发人员写出不安全的代码；主要包括 web 框架安全、html5 前端安全、移动端框架安全、服务端数据访问组件安全等。
4. 安全测试环节：通过代码扫描工具进行静态代码扫描，从白盒/黑盒测试发现程序漏洞，并结合人工二次审核，来更全面地发现代码漏洞；
5. 产品发布环节：安全部门依据上述环节评价结果决定是否发布； 在该环节中融入安全扫描与监控；
6. 安全运营与应急响应：安全工程师根据权威网站发布的安全漏洞，针对进行安全运营及事件应急响应；

4 物理与环境安全

纷享销客的所有硬件托管在专业的数据中心，这些数据中心通过严格的准入制度来授权访问；同时电力、制冷等基础设施均提供相应级别的冗余以加强 IDC 环境的安全性。承载业务的操作系统平台均采用当前广泛使用的稳定版本，采用镜像的方式统一部署，并对镜像执行定期更新确保修复各种安全漏洞；对于已上线的系统，涉及环境变更时执行严格的审批策略后，由专门的运维人员从内部经过验证和测试的可信源上执行下载和安全。

纷享销客的所有硬件设备托管在下列数据中心：

1. 北京亚太中立数据中心（UptimeInstitute Tier 3）（典型客户：阿里，华为）
2. 北京铁通 T3 数据中心（典型客户：京东）
3. 中国移动南方基地（广州）（五星级，典型客户：腾讯，网易，新浪）

4.1 物理安全

1. 电信 5 星级机房：电信级机房比普通的企业机房具备更高的可用性和抗灾能

力。

2. 机房进出安全制度：IDC 机房对进出人员进行严格管理，配备了门禁系统，严格验证进入人员身份，保证机房空间安全性。一旦发生遗失情况立即申请电子卡管理系统进行权限注销。所有设备及设施所处的机房部署了严格的访问控制和白名单机制，严格审核人员出入来防范可能出现的破坏物理设备等事件。
3. 机房安保措施：数据中心配备专业的保安员 7*24 小时在岗，随时巡视。机房进行 24 小时安全监控，机房内部的所有活动均有摄像记录。
4. 机房监控全面：目前部署在跨省市的多个数据中心，每个数据中心内部的每个区域 ,或外部走廊区域 ,或仓库门口区域 ,都使用了摄像机 ,物业保安 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；采用全方位电子摄像机对数据中心的基础设施内外部区域进行视频监控，对设施区域中 的其他系统进行检测和监控跟踪访问人员情况；所有人员活动记录电子保存（长期），所有视频记录被保存（3 个月），以备后期审计， 同时提供额外的安全控制措施，如:特定区域采用隔离或生物识别技术认证；
5. 机房设备安全 :数据中心所有纷享销客专属物理设备、设备配件、网络耗材，以及设备厂商的维修设备、配件、耗材等进出数据中心，必须由纷享销客内部人员进行授权，数据中心现场核实无误后方可允许设备、配件、耗材等的进出；

4.2 环境控制

数据中心采用一系列措施来保障运行环境：

1. 电力：为保障数据业务 7*24 持续运行，数据中心采用冗余的电力系统（交流和高压直流）,主电源和备用电源具备相同的供电能力 ,且主电源发生故障后（如电压不足、断电、过压、或电压抖动），会由备用发电机和带有冗余机制的电池组对设备进行供电，保障数据中心在一段时间的持续运行能力。
2. 气候和温度：均采用空调（新风系统冷却或水冷系统冷却）保障服务器或其他设备在恒温的环境下运行，并对数据中心的温湿度进行精密电子监控，一旦发生告警立即采取对应措施。 并且 ,设备冷风区域进行了冷风通道密闭，充分提高制冷效率，绿色节能。空调机组均采用 N+1 的热备冗余模式（部分数据中心采用 N+2 的冷、热双重冗余模式），空调配电柜采用不同的双

路电源模式，以应对其中一路电源发生故障后空调能正常接收供电。且在双路电源发生故障后， 由柴油发电系统提供紧急电源，减少了服务中断的可能。

3. 火灾检测及消防：自动火灾检测和灭火设备防止破坏计算机硬件。火灾探测系统的传感器位于数据中心的天花板和底板下面，利用热、烟雾和水传感器实现。在火灾或烟雾事件触发时，在着火区提供声光报警。在整个数据中心，也安装手动灭火器。数据中心接受火灾预防及灭火演练培训，包括如何使用灭火器。

5 系统安全

5.1 系统软件安全

线上服务运行在可信的操作系统版本上，安装软件，必须由运维人员从指定的可信安装源下载和安装。对于通用的系统软件，例如 tomcat，nginx、ssh 等，制定了对应的安全配置规范，通过基线系统实时采集服务器上运行的软件版本和配置信息，并进行相应的维护。安全团队也会跟踪业界安全问题，评估服务器上的软件是否有安全漏洞，一旦有安全漏洞产生，会通过应急响应流程推动基础软件的漏洞修复。

5.2 系统登录授权访问

对于所有线上操作人员的管控，遵循最小权限原则，基于角色的访问控制应用在从网络设备到主机到数据库等各种系统，对关键设备的访问，采用了业界成熟的多因子身份验证。

员工登录服务器时使用个人帐号体系，登录服务器的密码强制定期修改。员工登录服务器做任何操作前，需要先提交审批，在通过审批后，员工才能获得对应服务器的登录权限。员工离职/岗位发生变动/申请的权限到期时，都会在对应的服务器上删除对应的帐号。

对于生产服务器，员工需要首先登录堡垒机，才能登录其他生产服务器。堡垒机经过了特别的加固，只对办公网开放，启用了双因子验证，并部署有操作日志记录和审计系统，堡垒机上的操作会被实时传送到远端进行存储和审计。

5.3 系统安全检测防御

纷享销客的服务器上统一部署了主机入侵防御系统，并依托大数据处理平台，对出入站流量进行分析，实现对入侵等安全事件的检测。

6 网络安全

生产网络与办公网络完全隔离，并通过严格的审核机制以及上线流程来保证受信程序或端口的安全访问 ;同时安全专员会定期执行网络安全扫描测试以主动发现可能存在的网络隐患。已实现全站https的访问以防止各种网络窃听行为和流量劫持的发生。并与第三方安全厂商合作实现DDOS的攻击防护，确保第一时间发现攻击并进行流量清洗，保障企业的安全访问。

纷享销客采用GlobalSign颁发的企业级SSL证书对传输信息进行加密处理。除了加密功能，该国际证书也是对纷享销客网站安全性的认可。

6.1 安全域划分

纷享销客通过不同的安全域或物理隔离的网络来实现不同级别的网络隔离。所有的用户接入请求均通过严格配置的NAT策略实现 ,所有的维护请求均通过独立网络经由DMZ完成。对网络的出口处通过端口镜像的方式来甄别各种网络威胁。而内部网络根据不同的用途实现物理隔离，如公共网络，存储网络，心跳网络以及管理网络。

6.2 网络访问控制

网络依据用途划分成办公、测试、生产、公有云等多个安全域，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。各类服务，只有在经过安全保障团队审核之后，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。

另外，安全保障团队会通过检测系统，定时地依据逐步完善的安全规则，进行白盒审计，依据端口扫描进行黑盒审计，用于主动及时发现访问控制中存在的安全问题。

6.3 DDoS 安全防御

与第三方专业防 DDoS 机构合作，对所有的入站流量实现准实时分析，对异常流量实现及时阻断。

并于第三方安全机构一起，建立流量清洗中心，抵御各类基于网络层、传输层的 DDoS 攻击（包括 SYN Flood、UDP Flood、UDP DNS Query Flood、(M)Stream Flood、ICMP Flood 等所有 DDoS 攻击方式），并通过安全运营后台实时掌握网络攻击趋势及防御状态。当攻击发生时，通过自动化的运维机制，被攻击节点将自动停止服务，并通过第三方专业防 DDoS 机构执行流量清洗后回源到纷享销客的备用节点，保障服务持续运行。

6.4 流量劫持

针对 http 协议在网络传输过程中，可能会被篡改/窃听/截取，为了防止用户的隐私数据在传输过程中被窃听或者泄露，纷享销客的所有业务都已经启用 https 协议来代替 http 协议。

对于 DNS 劫持，纷享销客通过采用 HTTPDNS 机制，避免了流量劫持。

7 数据安全

信息安全主要目标之一是保护业务系统和应用程序的基础数据安全，所以数据安全是企业的生命线。依据数据安全生命周期，纷享销客从数据创建、存储、使用、共享、归档至销毁，使用了数据分级、数据加密等措施，保障数据的保密性、完整性、可用性、真实性、授权、认证和不可抵赖性。

7.1 数据分级与加密

纷享销客对所有用户和企业数据提供存储安全保护；根据存储与使用的数据，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，根据数据安全分级，有对应的保护策略和要求，对用户和企业数据进行安全存储与保护。

凭借以数据为中心的安全愿景，通过数据分类分级、数据加密和密钥管理为敏感数据提供可持续的信息保护;借助密钥管理中心和加解密产品实现数据安全保护和控制，将安全技术嵌入至整个数据安全生命周期中，以保障数据安全。

加密算法采用业内先进的非对称 AES 加密算法， 使用 CBC 模式，

PKCS5Padding 补码方式，采用安全散列算法较高位数的 SHA-256，来充分保障密钥的不可破解性。它的设计与管理满足行业合规性及审计要求。

7.2 数据使用授权

纷享销客为用户和企业数据提供访问控制保障。根据数据等级，对数据的使用和应用展示均进行了严格的控制，禁止展示机密信息及未脱敏信息，同时对于需要展示信息的场景，对于任何数据请求，均需要授权使用，阻断对敏感信息的爬取。

对于涉及用户隐私或机密数据的使用，包括第三方应用的访问，均严格控制权限申请，实施权限多次校验及加密存储的策略，同时必需经过企业或用户可感知的授权。对于所依赖的第三方服务当存在数据访问合作时，均签订了安全生产、保密协议。

7.3 数据安全审计

安全审计覆盖所有数据活动的详细跟踪记录，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。生成的审计结果报表使所有数据活动详细可见，如登录失败、权限升级、计划变更、非法访问、敏感数据访问等，以便于判断这些行为是否合规，并能够一览无余的做到所有用户操作有迹可循。主要的审计包括：

1. 企业系统管理员操作日志

各企业系统管理员在 web 端管理后台可以查看系统管理日志，任何涉及系统管理行为都会记录，所有日志要求至少保留三个月。

系统管理员具有查询日志的权限。业务模块内根据场景也会提供不同的业务操作日志，如遇到未提供的情况，可联系纷享客服人员进行单独沟通。

2. 纷享平台操作管理日志

纷享平台的运维人员操作系统配置、数据时，均记录操作日志。所有审计日志均不可人为修改、删除。所有审计日志要求至少保留三个月。

7.4 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，依据相关安全标准进行清除数据、

磁盘消磁以及物理销毁。

8 应用安全

8.1 帐号安全

8.1.1 登录安全

所有用户登录密码要求为 6-20 位英文、数字、字符、大小写至少 2 种的组合。

帐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。对非常用设备的登录，需用户进行密码+动态口令登录的双因素验证。
同时，通过帐号监测平台，对用户同设备 批量尝试登录账号进行监控报警，发现攻击行为，可将该设备拉至黑名单。

除已有的风控体系外，也会提供相应的安全辅助功能，如二次验证、双因素认证、扫码验证等方式，给用户帐号的安全保障提供更多维度的选择。
每一次用户登录行为，都会记录安全日志，并发送企信通知给该用户帐号知晓。包括登录的机型、登录的时间等。若发现异常，可以及时的发现。

8.1.2 密码安全

密码存储为加密存放，采用的是不可逆的多重哈希混淆算法加密。当用户需要找回密码时，只能通过重置或者管理员赋予新密码来更改密码。

8.1.3 暴力破解

每一个用户帐号的登录，均基于可信设备判断是否已授权可登录的验证，同时基于后端风控体系，实时监测帐号破解、撞库与刷库等攻击行为，告警通知及处置恶意请求；帐号依据信息安全风险库检测帐号是否存在风险，发现存在风险的帐号及时告知用户，进行帐号密码的升级。

同时，针对短时间内多次帐号密码错误，采用图片验证码进行防范机器行为的暴力破解。

8.1.4 设备安全

纷享销客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。

1. 对于 Web 设备的验证，除帐号+密码+验证码的方式认证外，还需要使用已授权可信的移动端设备进行扫码授权；
2. 对于移动端可信设备的认证，需要经过帐号+密码+短信验证码的认证；
3. 对于非可信设备登录用户帐号，需要经过用户有感知的授权，授权方式有两种：

1）向绑定用户纷享销客帐号的手机号发送短信验证码，登录者输入验证码来进行授权验证；

2）向对用户帐号已授权认证过的可信设备，发送纷享销客系统消息，请用户人工进行授权操作；

3）以上授权设备均可以随时被用户取消授权。

8.2 应用数据安全

8.2.1 通讯协议安全

基于 HTTPS（TLS）协议为应用程序提供数据保密性和完整性的基础上，构建了一套完整的私有安全通信协议，以 AES 加密传输为主，并通过独立技术保护 AES 密钥的安全性，来保护用户在网络传输中的信息，防止窃听，以确保信息在网络中传输安全。

8.2.2 终端设备安全

客户端的数据库进行了整库加密存储，采用业内成熟的 256-bit AES 加密算法，保护用户客户端存储的敏感信息不被攻击者非法获取，保障用户的隐私数据不被泄露。

8.2.3 企业通讯录安全

企业通讯录采用加密存储，可分级管理通讯录，针对不同人群设置不同权限；对于不同公司的信息，存储空间是相互隔离的，当员工离职后，会被踢出对应的

企业群，自动剥离员工在该企业的权限。企业可以设置对员工的手机号进行隐私保护，在对外展示员工信息时隐藏手机号码，防止信息泄露。

8.2.4 企业网盘安全

纷享销客企业网盘具备独立的访问控制鉴权功能，来保障企业文件存储、传输和访问的安全。

对于在纷享销客平台上，以任何方式上传的文件，访问控制的粒度会细化到个人，其他人在非授权情况下无法访问或下载文件。

1. 保存到网盘的企业文件具有企业权限保证，企业与企业之间的网盘文件是绝对隔离的。
2. 聊天会话中传输的文件也有相应的权限保证，只有参与该聊天的人能够查看对应文件，不在此聊天会话中的人无法看到该文件，更无权查看。
3. 对于分享、日志、日程等传输的文件，一样具备鉴权能力，只有被作者选定的人或部门范围内有权限，未被选定的即便是拿到文件链接，也一样无权访问。

企业网盘为保障用户数据安全，会对所有上传数据进行分片以及采用 SSL/TLS 加密传输，并且在云端应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数据存储安全。

9 灾备与业务连续性

企业的业务连续性是对企业是至关重要的一个环节。纷享销客平台所提供的服务，能够应对线上多数风险，具有快速反应的能力，来保障企业在纷享销客平台的业务连续运转。

9.1 应急与灾备技术

建立了本地应急及容灾技术体系，服务于生产系统，全面保证纷享销客整体的业务连续性。

核心业务及数据服务均实现冗余或主备部署，部署在多机房，分布在不同地域，相互间通过多家运营商实现多链路链接；数据库采用热备、冷备相结合，实时同步到不同物理机，保障业务连续性；以准实时的方式同步到异地机房；通过自动化运维平台，实时故障检测，保障核心应用不中断，系统恢复方便快捷，可

进行分钟级伸缩扩容，在突发事件及自然灾害时，为基础服务的可用性及可持续性提供保障能力。

关于数据的恢复演练及容灾备份策略，我们针对 DDoS 防御执行每季度演练，利用数据库相关的复制技术生成多个副本来实现容灾，针对文件类型的数据，利用其自身的复制技术，采取生成多个副本，并定期转储至异地机房，实现容灾。针对其余相关的涉及可用性的演练（如数据库主从切换、机房链路切换、防火墙主从切换等）不定期执行。

同时，通过已制定的灾难恢复流程及应急方案进行定期灾备演练，保证当事故发生时的应急处理效率。

9.2 灾难恢复管理

建立了完备的应急响应及灾难恢复流程。应急响应组由安全专家、业务专家、技术专家组成，制定了完备的应急响应制度及灾难恢复流程，并定期组织灾备演习和维护。

10 安全认证

10.1 ISO 27001 认证

2016 年 10 月通过了 ISO27001:2013 版信息安全管理认证。并且在之后的每年都会接受一次安全审查，来确保各项安全策略都实施到位。

ISO27001 是信息安全领域的管理体系标准。当企业通过了 ISO27001 的认证，就表示企业的信息安全管理已建立了一套科学有效的管理体系作为保障。


信息安全管理体系
认证证书

注册号：016ZB16I20281R0S
统一社会信用代码：91110102674290067J

兹 证 明

北京易动纷享科技有限责任公司

信息安全管理体系符合
ISO/IEC 27001:2013标准，适用于

仅供“纷享销客”客户
作为资质证明使用

与纷享销客产品研发维护相关的信息安全管理；
适用性声明：FXXK-ISMS-1002 版本：V1.1

注册地址：北京市西城区北纬路九号205C室
经营地址：北京市海淀区知春路甲63号卫星大厦607、703和708（机房）

初次发证日期：2016年10月27日
证书有效期至：2019年10月26日

北京新世纪检验认证股份有限公司
总裁：

BCC地址：北京市西城区国英园1号楼11层1101室
本证书在国家规定的各行政许可、资质许可有效期内使用有效
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。
证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询
本证书信息可在国家认监委网站www.cnca.gov.cn查询

BCC

CNAS 中国认可 管理体系 MANAGEMENT SYSTEM CNAS C016-M

北京新世纪检验认证股份有限公司 1101020176645

10.2 信息系统安全等级保护定级（DJCP）

纷享销客系统于 2018 年 10 月通过了公安部信息系统安全等级保护三级定级，并且获得了备案证明。之后的每年都会接受一次安全审查，来确保各项安全策略都实施到位。

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，北京易动纷享科技有限责任公司单位的：

仅供“纷享销客”客户
作为资质证明使用

第 3 级纷享销客系统系统

予以备案。

证书编号：11010813772-00001

中华人民共和国公安部监制

备案公安机关公章

2018 年 10 月 16日