明道云产品行业合规白皮书

明道云产品行业合规白皮书

参照 FDA CFR Part 11 电子记录和电子签名

国家药监局《药品记录与数据管理要求》

上海万企明道软件有限公司

2023 年 4 月

1. 简介

在特定行业和关键业务环节，对信息系统本身的合规性是一个重要的 IT 管理主题。企业的业务活动在接受政府监管或者第三方审计时，提供的电子数据记录需要能够证明它的真实、有效、完整和可追溯性。

为了说明明道云 APaaS 在构建此类应用时能够达成相关的合规规定，我们通过典型的被监管行业——医药行业的相关法规和具体技术规范来说明明道云产品是如何响应和满足相关标准的。为实用目的起见，我们采用国家药监局 2020 年 12 月开始施行的《药品记录和数据管理要求》和美国 FDA 发布的 *21 CFR Part 11 行业指南（2003）（以下简称 Part 11）* 作为狭义标准进行合规和偏差分析。

本白皮书仅作为技术参考文件，提供给客户群体，方便了解明道云产品的技术原理，不作为对客户和公众的法律承诺。

2. 合规要点

无论是中国的《药品记录和数据管理要求》，还是 Part 11，对电子记录和电子签名环节相关的合规要求可以总结为以下要点：

（1）访问控制

（2）数据一致性和安全

（3）可追溯性

（4）电子签名的效应

（5）记录有效性

3. 细则解析

因为只有 Part 11 提供了细化的合规要求，且完全覆盖了中国《药品记录和数据管理要求》的原则性规范，我们的解析将基于 Part 11 的每一个细则进行。

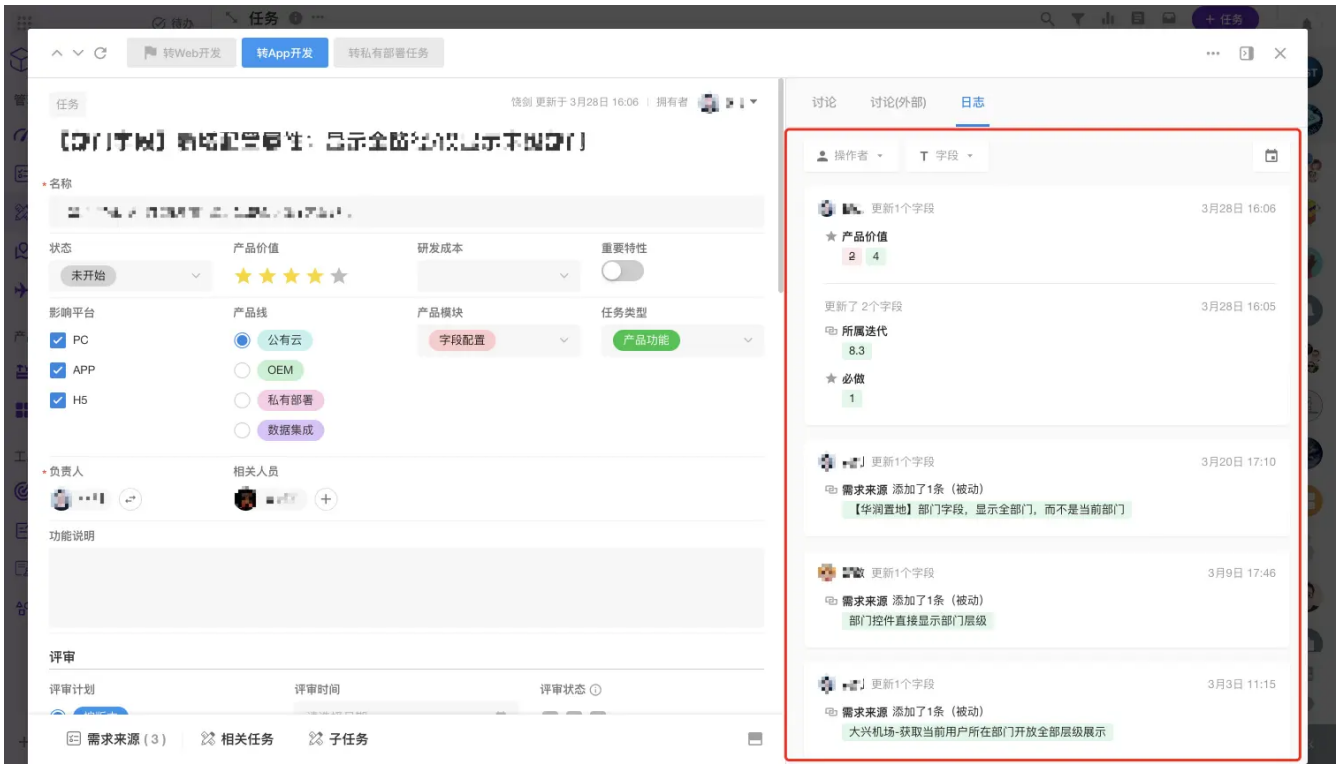
要求：§11.10(a)

合规要点：

系统的整体有效性，以确保准确性、可靠性、预期的一致性以及能够发现无效或被篡改的记录的能力。

系统能力说明：

- 标准的系统设计方法（即系统适用性测试）存储在系统中。
- 记录日志内部存储，在软件中可以被恰当权限的用户查看。



要求：§11.10(b)

合规要点：

能够生成准确完整的纸质和电子记录副本，供检查、审查、复制。

系统能力说明：

- 可以根据需要打印出结果报告、操作程序、范围和审计跟踪报告。

要求：§11.10(c)

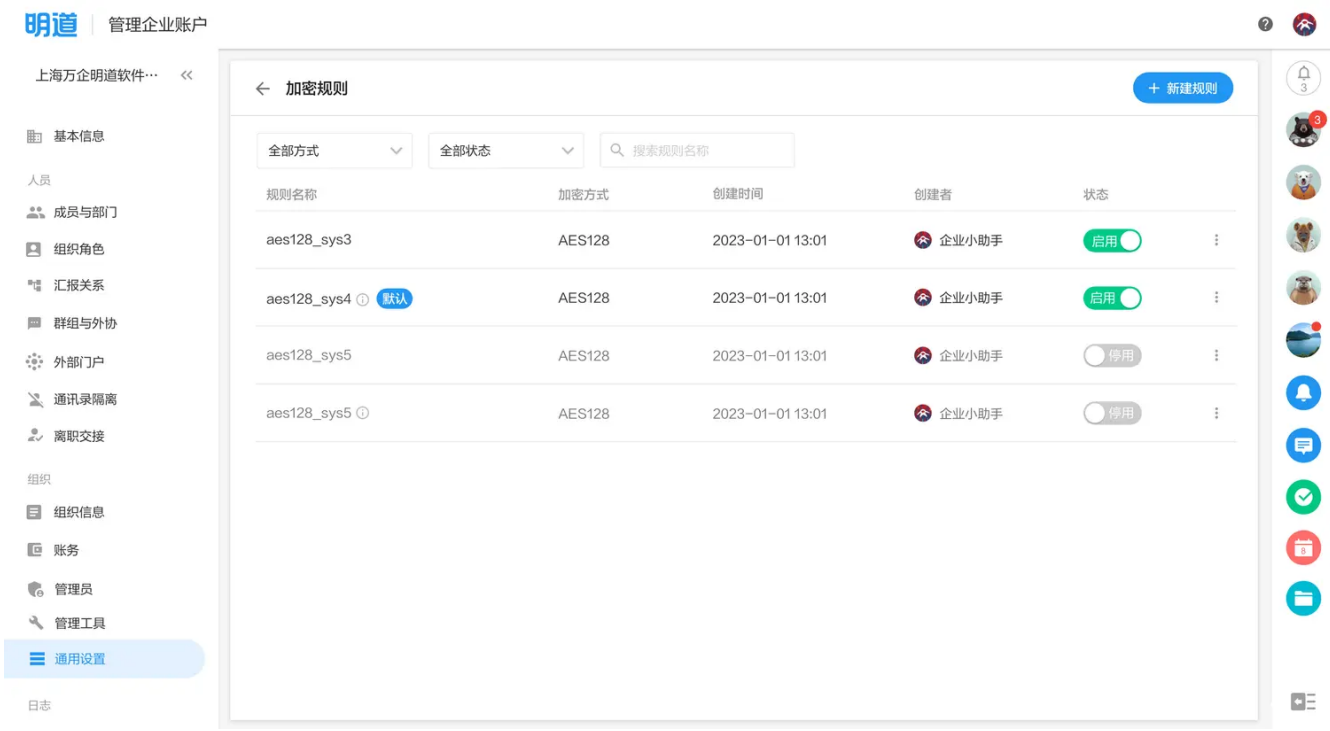
合规要点：

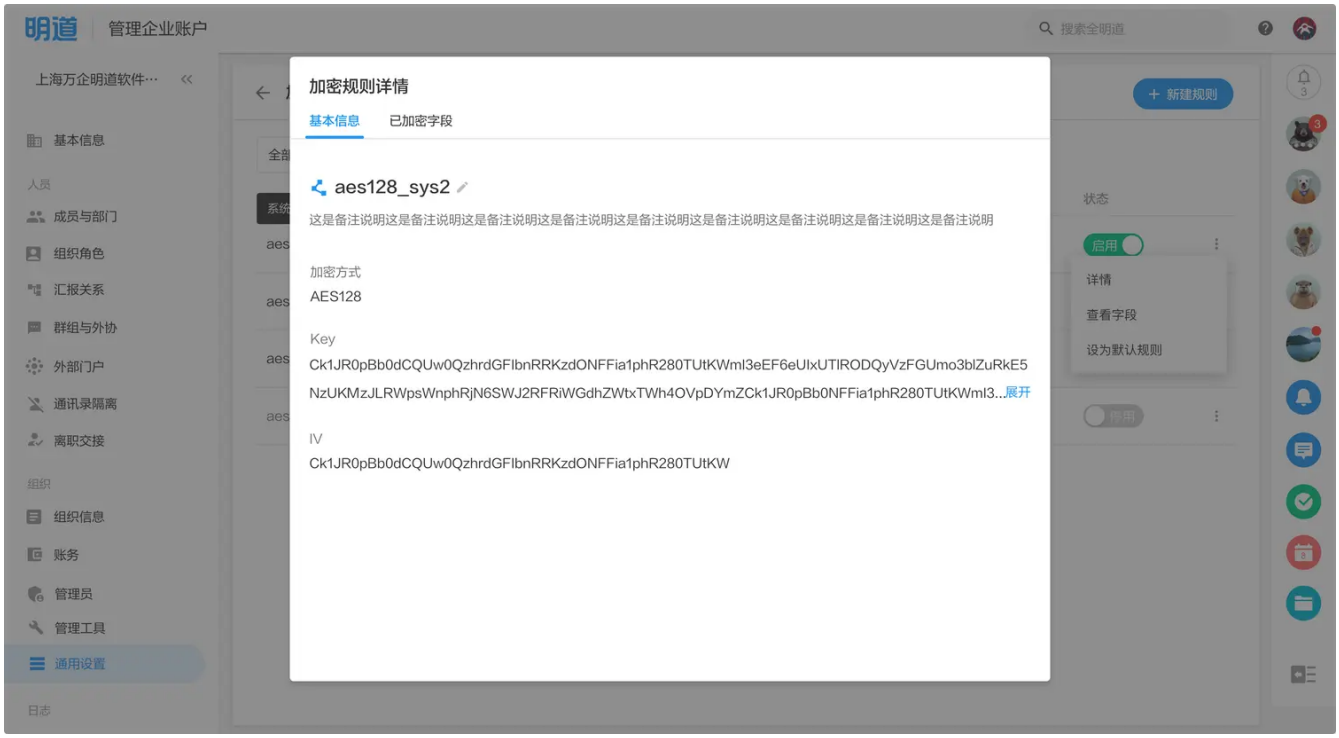
保护记录，确保其在记录留存期内能够准确、方便地获取。

系统能力说明：

- 系统将数据持久存储在业界标准数据库中。可以使用系统备份功能或通过纸张、正常打印获取副本。
- 存储设备上的数据可经过加密并附有校验码，系统能够识别对数据进行的修改。

1. 设置加密规则


明道
管理企业账户
上海万企明道软件…
基本信息
人员
成员与部门
组织角色
汇报关系
群组与外协
外部门户
通讯录隔离
离职交接
组织
组织信息
账务
管理员
管理工具
通用设置
日志
加密规则
新建规则
全部方式
全部状态
搜索规则名称
规则名称
加密方式
创建时间
创建者
状态
aes128_sys3
AES128
2023-01-01 13:01
企业小助手
启用
aes128_sys4
默认
AES128
2023-01-01 13:01
企业小助手
启用
aes128_sys5
AES128
2023-01-01 13:01
企业小助手
停用
aes128_sys5
AES128
2023-01-01 13:01
企业小助手
停用


明道
管理企业账户
搜索全明道
上海万企明道软件…
加密规则详情
基本信息
已加密字段
aes128_sys2
这是备注说明这是备注说明这是备注说明这是备注说明这是备注说明这是备注说明这是备注说明这是备注说明这是备注说明
加密方式
AES128
Key
Ck1JR0pBb0dCQUw0QzhrdGFIbnRRKzdONFFia1phR280TUtKWml3eEF6eUIxUTlRODQyVzFGUmo3blZuRkE5
NzUKMzJLRWpsWnphRjN6SWJ2RFRiWGdhZWtxTWh4OVpDYmZCk1JR0pBb0NFFia1phR280TUtKWml3...展开
IV
Ck1JR0pBb0dCQUw0QzhrdGFIbnRRKzdONFFia1phR280TUtKW
新建规则
状态
启用
详情
查看字段
设为默认规则
停用

2. 字段加密

要求：§11.10(d)

合规要点：

限制系统仅允许授权个人访问。

系统能力说明：

- 系统提供了具有自定义内部访问权限（比如：管理员、实验室管理员、仪器用户）的登录体系，管理员只能对其授权的人员授予访问权限。

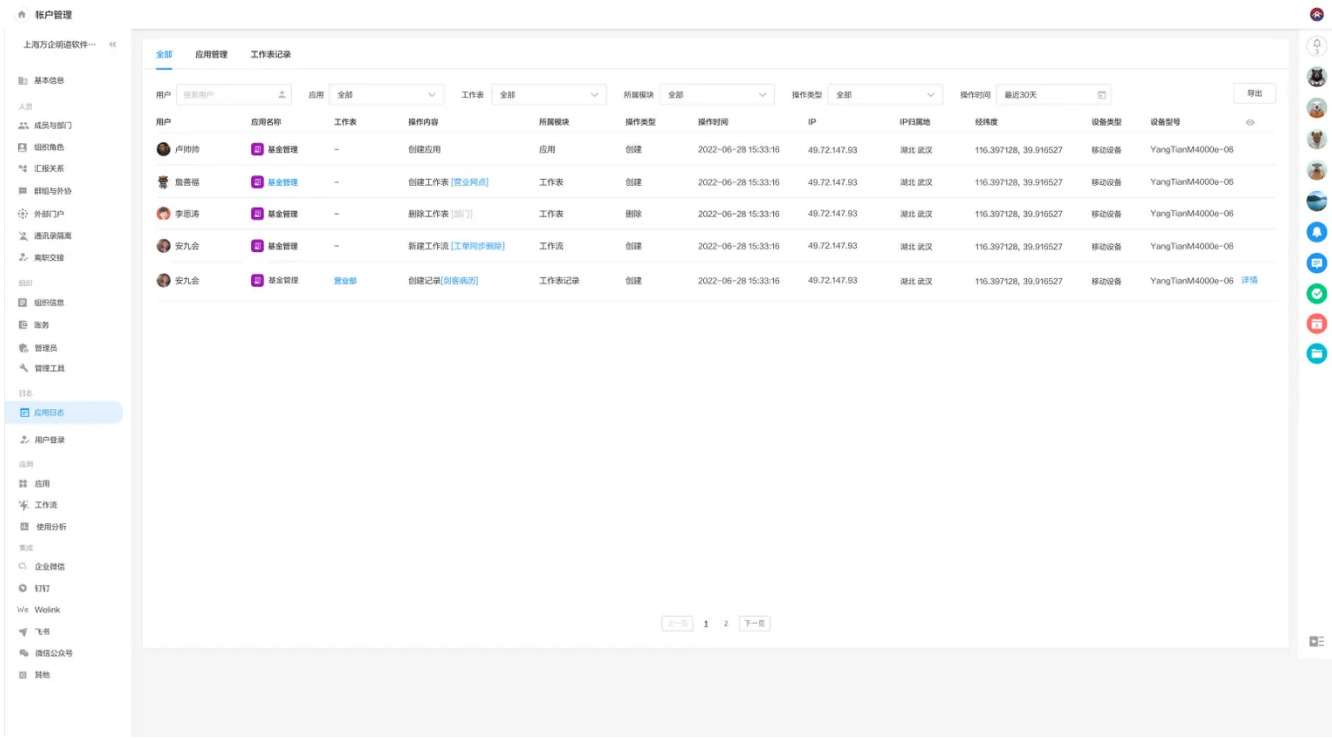
要求：§11.10(e)

合规要点：

使用安全且由计算机生成的时间戳追踪记录操作员的操作日期和时间，以不间断地记录创建、修改或删除电子记录的操作时间。记录的更改不得掩盖先前记录的信息，审计追踪记录的文件应保留并可供机构审查。

系统能力说明：

- 审计跟踪记录所有用户的输入和行动，此外，所有安全设置、用户管理或数据构造的更改都记录在审计跟踪中。



- 系统自动创建和保存记录更改后的新版本。

要求：§11.10(f)

合规要点：

根据需要使用操作系统检查来强制步骤和事件的允许排序。

系统能力说明：

- 操作序列按照应用的设计进行定义，引导用户按照步骤进行操作。例如通过工作流的审批节点控制特定数据状态的修订，通过关闭默认的增删改能力来限制特定角色的操作权限。

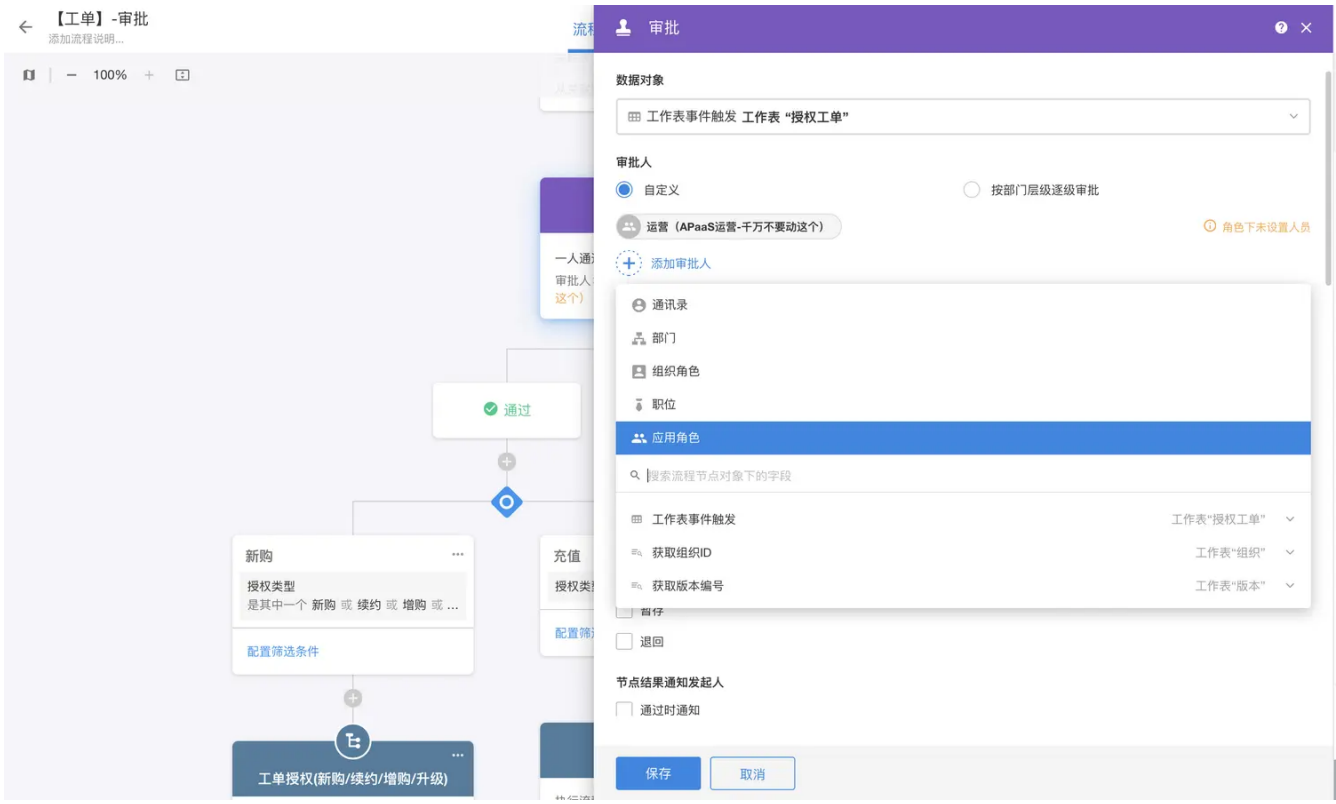
要求：§11.10(g)

合规要点：

只有授权的个人才能使用系统，电子签署记录，访问操作或者控制台系统输入或输出设备，改动记录或者执行其他操作。

系统能力说明：

- 所有应用的操作均要求合法的账户登录，在登录进程中验证用户角色所拥有的权限集合。
- 特定操作可以编排为要求电子签名，可通过工作流要求审批人和申请人不同。
- 电子签名可以要求二次密码验证，手写签名。
- 自定义用户角色，配置审批节点



要求：§11.10(h)

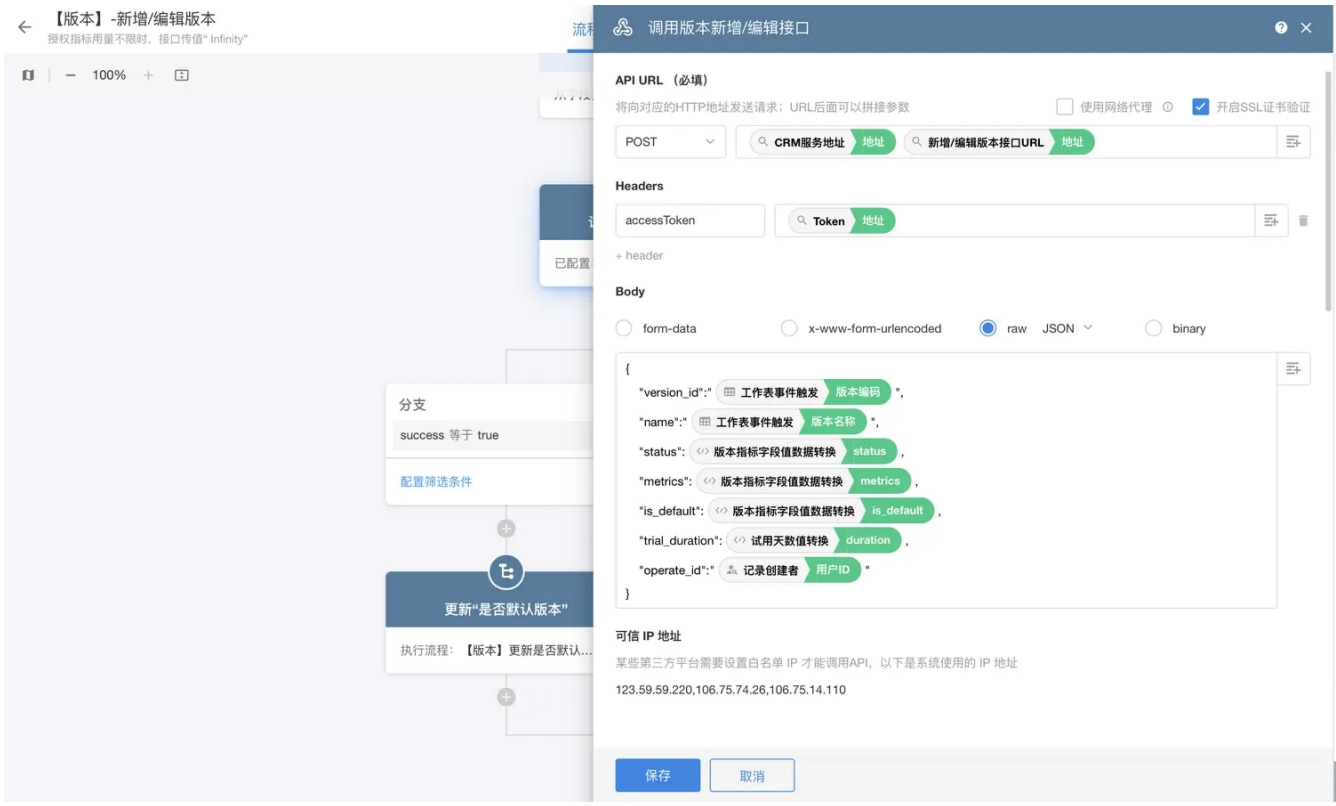
合规要点：

系统控制联接设备的有效性。

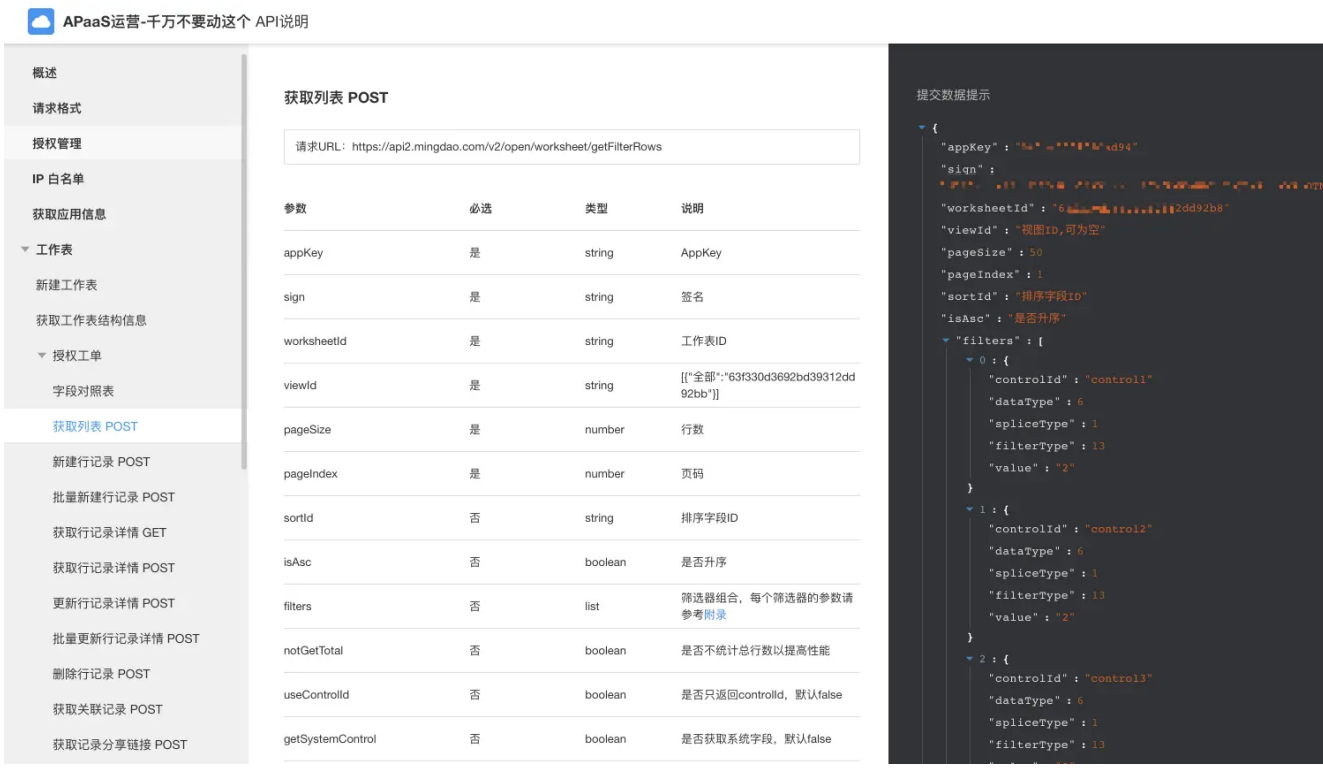
系统能力说明：

- 平台提供调用外部接口、应用接口、以及 Webhook 方式，可验证设备联接的有效性

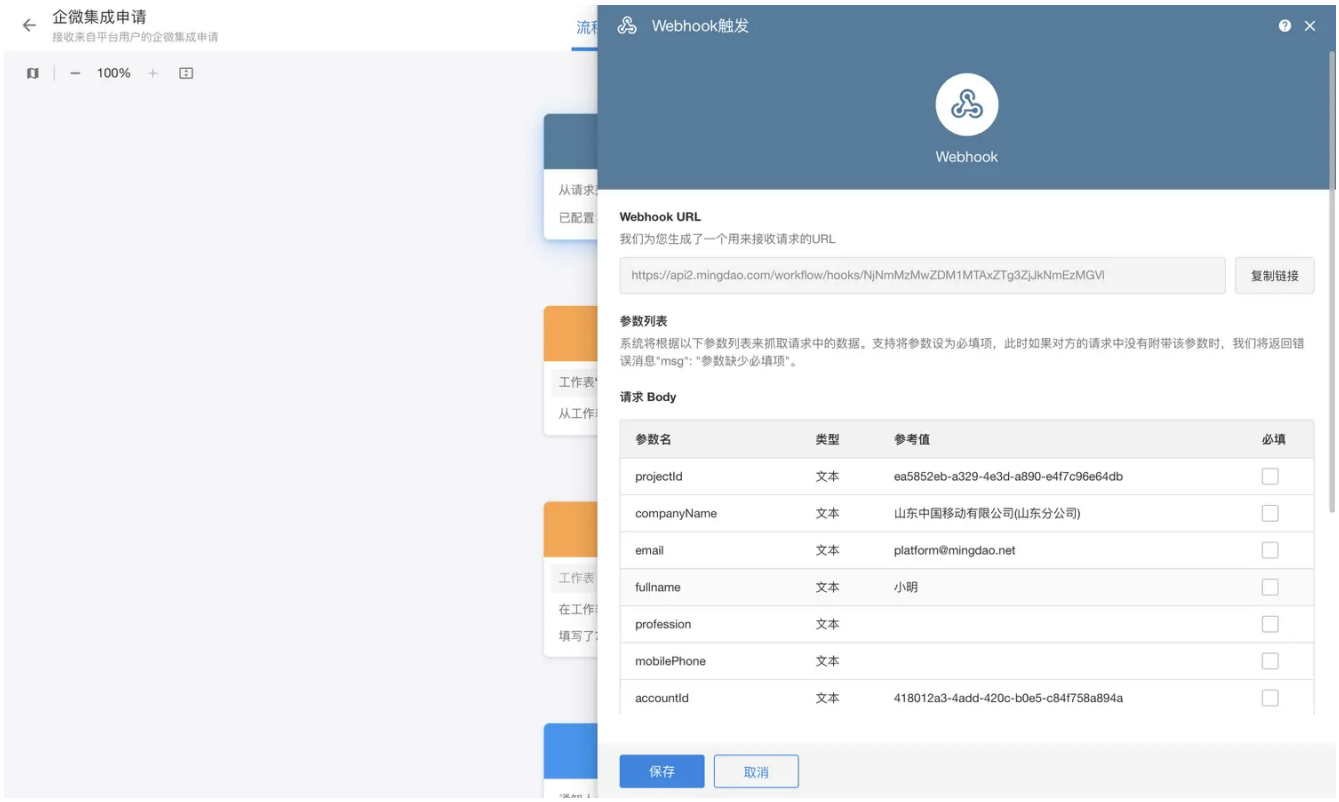
1. 调用外部接口



2. 对外提供应用接口



3. Webhook



要求：§11.10(i)

合规要点：

开发、维护或使用电子记录和签字系统的人员应具备履行所分配任务的教育和经验。

系统能力说明：

- 应用编排中，要求审批和修订记录动作时，提示和二次提示均明确而具体，并允许应用编排者自定义提示文字。

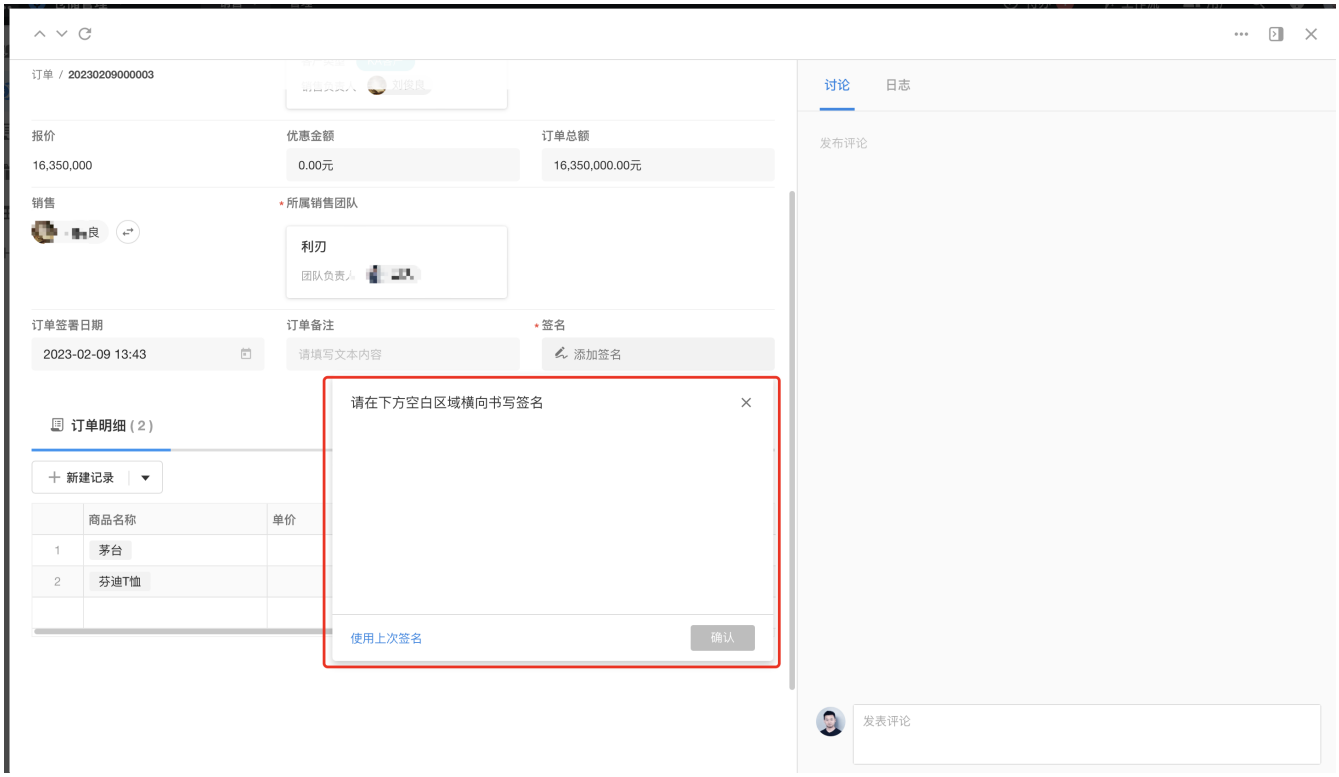
要求：§11.10(j)

合规要点：

有书面规定，对电子签字方式下发起的行为规定了责任人，以遏制篡改记录和签字的行为。

系统能力说明：

- 平台提供签名字段，用户可根据准则自行设定。



要求：§11.10(k)

合规要点：

对系统的操作和维护文档的分配、获取和使用进行控制，对系统文档形成和修改的正式变更控制程序，保持时序化的审计跟踪，创建和修改文档。

系统能力说明：

- 明道云构建的应用均提供了系统预制的使用说明配置。对合规性要求高的场景下，推荐客户自行使用其他文档平台和控制工具来发布使用文档，例如 Gitbook。

要求：§11.30

合规要点：

开放系统的控制。

系统能力说明：

- 平台默认提供了 API。API 访问控制基于业界标准的 Open Auth 规范。管理员也可关闭 API 授权。
- API 访问支持白名单管理
- API 访问支持全局和只读的配置
- API 访问同样写入系统日志

要求：§11.50(a)

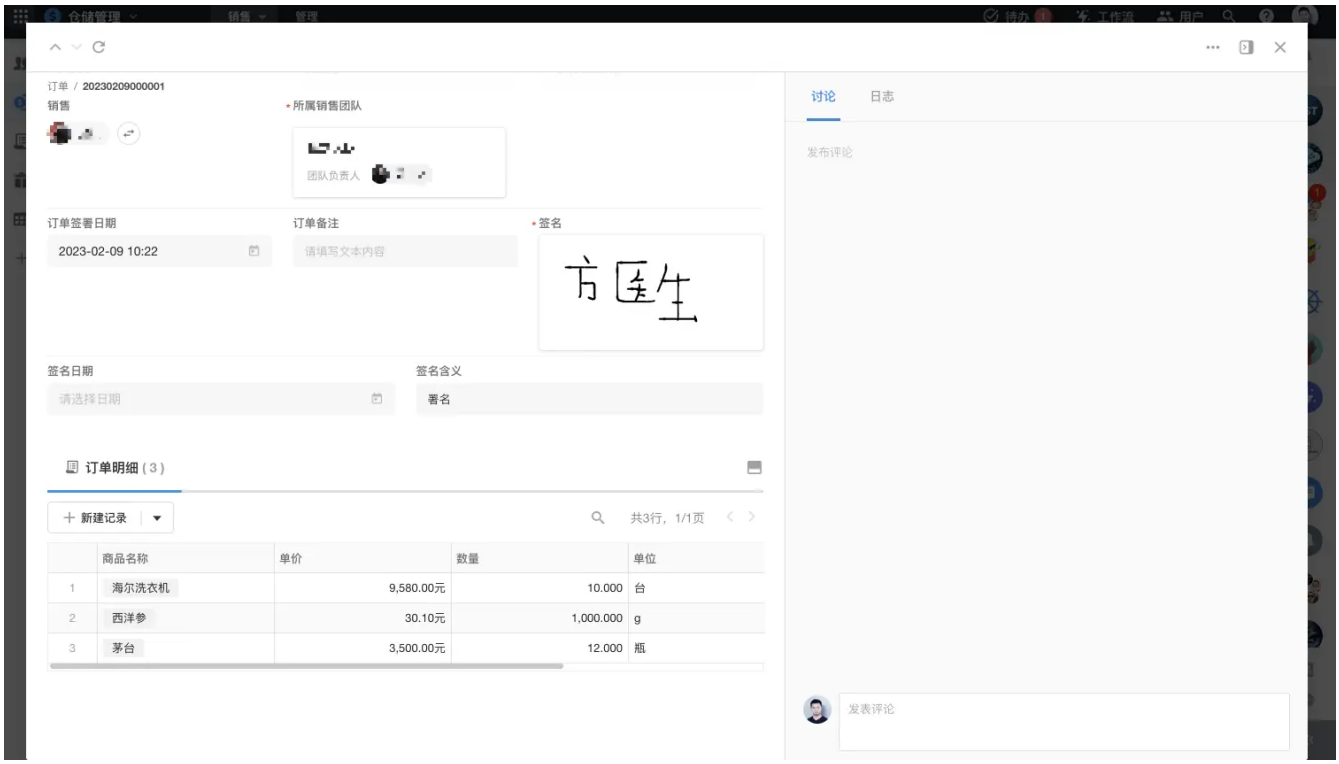
合规要点：

签字的电子记录必须包含以下信息：

- 签名者的打印名称
- 签字日期和时间
- 签字的含义（如核准、审查、责任或署名）。

系统能力说明：

- 所有签名都包含签署人的全名、签署日期和时间以及签名的含义（用户可自行定义）。



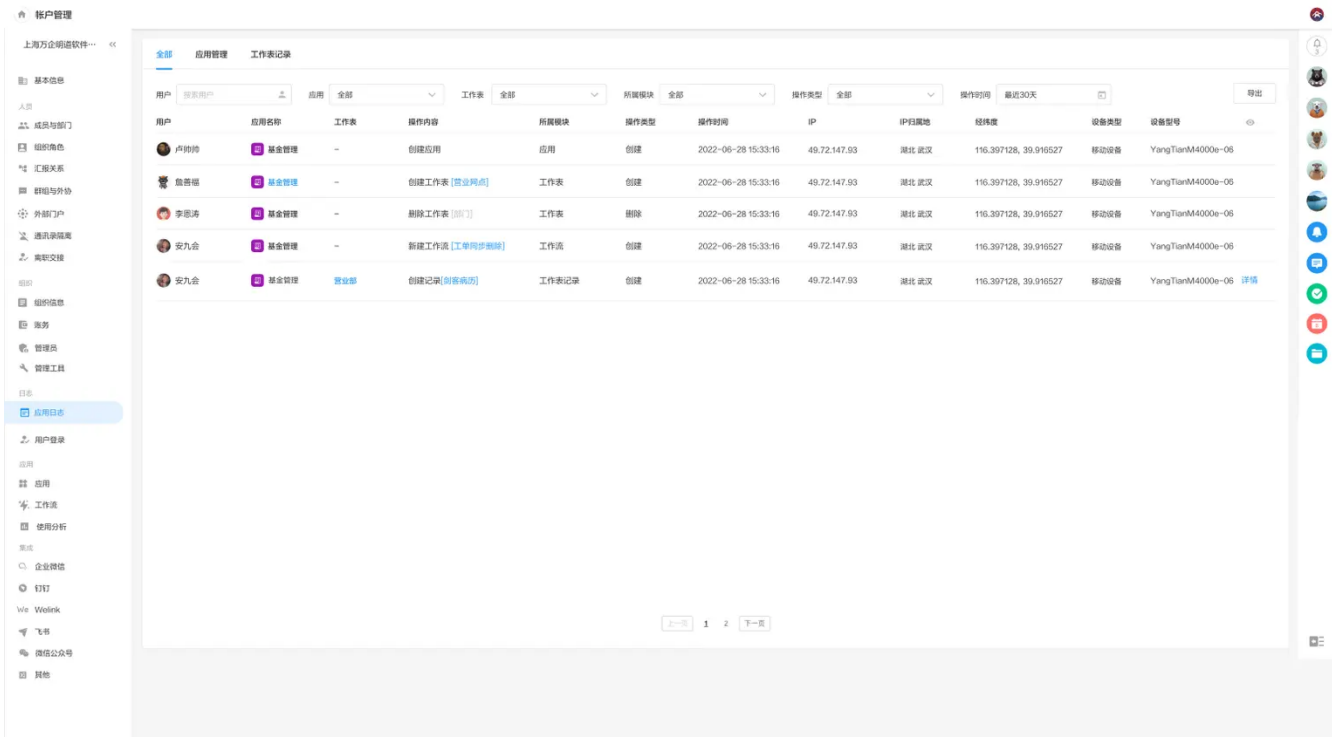
要求：§11.50(b)

合规要点：

第 11.50(a)规定的信息载于电子记录的显示和打印副本上。

系统能力说明：

- 用户 ID、日期和时间以及签名的含义均显示在页面上，并在平台的审计跟踪和用户管理报告中显示。签署人的全名也在平台的审计跟踪和用户管理中显示。



要求：§11.70

合规要点：

电子和手写签字应与相应的电子记录相关联，以确保签字不能被取消、复制或转移，通过普通手段篡改电子记录。

系统能力说明：

- 签字控制的使用与各自的配置或样本被安全关联，无法通过普通手段剪切、复制或转移。

要求：§11.100

合规要点：

每个电子签字应对于每个人都是唯一的，不得被任何其他人重复使用或重新授权给任何其他人。在建立个人电子签字之前，组织应验证个人的身份。

系统能力说明：

- 每个用户获得一个唯一的用户 ID，系统监测用户 ID 的不同性。签字权初次分配之前，必须验证个人身份。
- 用户账户可以停用，但不可以删除，必须操作上确保该用户 ID 不会被再次分配给其他人。

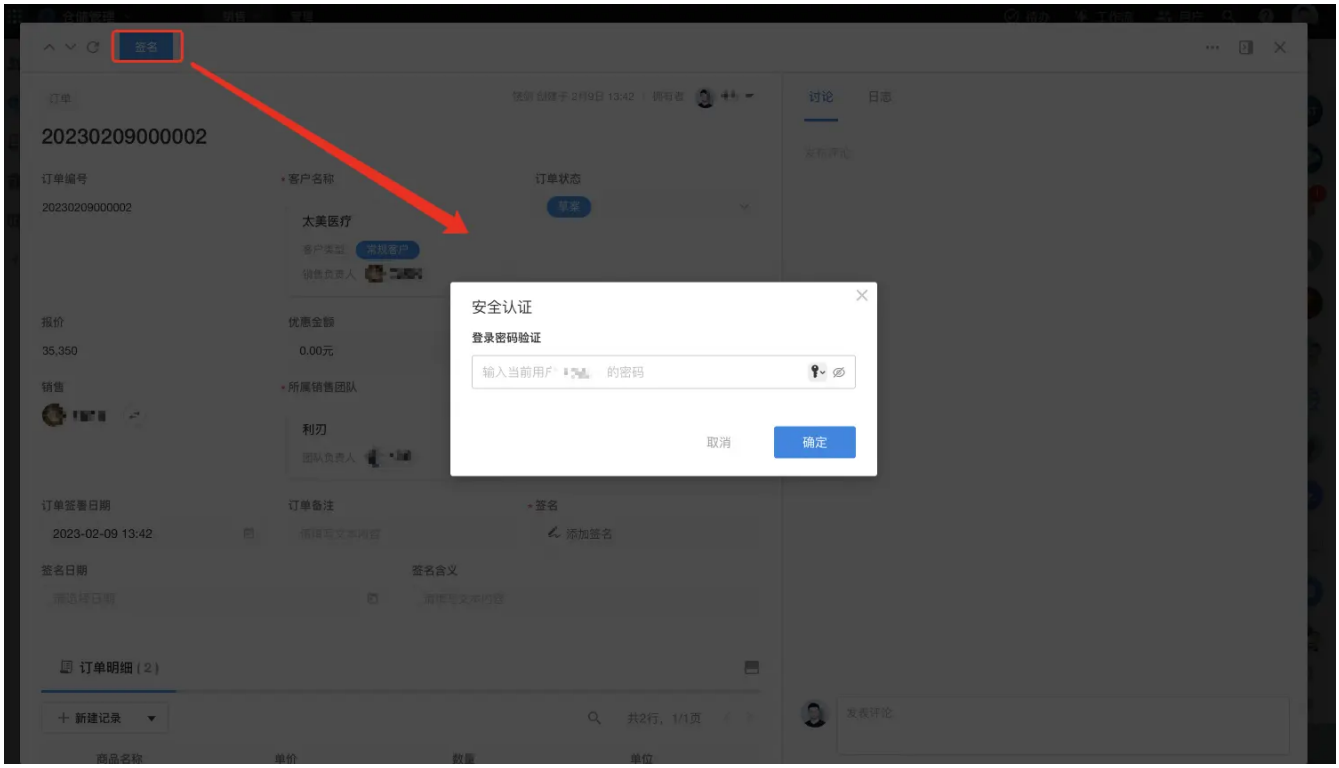
要求：§11.200(a)(1)

合规要点：

不以生物特征为基础的电子签字至少应包含两个不同的身份识别部分。

系统能力说明：

- 登录验证使用用户名和密码。



要求：§11.200(a)(1)(i)

合规要点：

在单次受控系统访问的单个连续时间段内，第一次签字应使用所有电子签字部分；后续签字要求至少一个电子签字部分。

系统能力说明：

- 签名时二次验证必须输入密码。

要求：§11.200(a)(1)(ii)

合规要点：

如果签名不在一个持续的 Session 进行，则电子签名的两个组成部分将与每一个签名一起执行。

系统能力说明：

- Session 过期后，签名人需要重新登录，则完成签名时必须输入用户 ID 和密码。

要求：§11.200(a)(2)

合规要点：

以非生物特征为基础的电子签字仅应由其真正拥有者使用。

系统能力说明：

- 操作员应确保用户只能使用自己的账户。

要求：§11.200(a)(3)

合规要点：

任何伪造电子签名的企图都必须需要至少两个人的合作。

系统能力说明：

- 任何人都无法通过普通方式伪造电子签名数据，冒用他人签名则必须获得对应的账户和密码。

要求：§11.200(b)

合规要点：

基于生物特征的电子签名必须只能由其真正所有人使用，其他任何人都不能使用。

系统能力说明：

- Web 平台的电子签名不支持基于生物识别的方式，移动设备登录支持面容或指纹验证由操作系统管理。

要求：§11.300

合规要点：

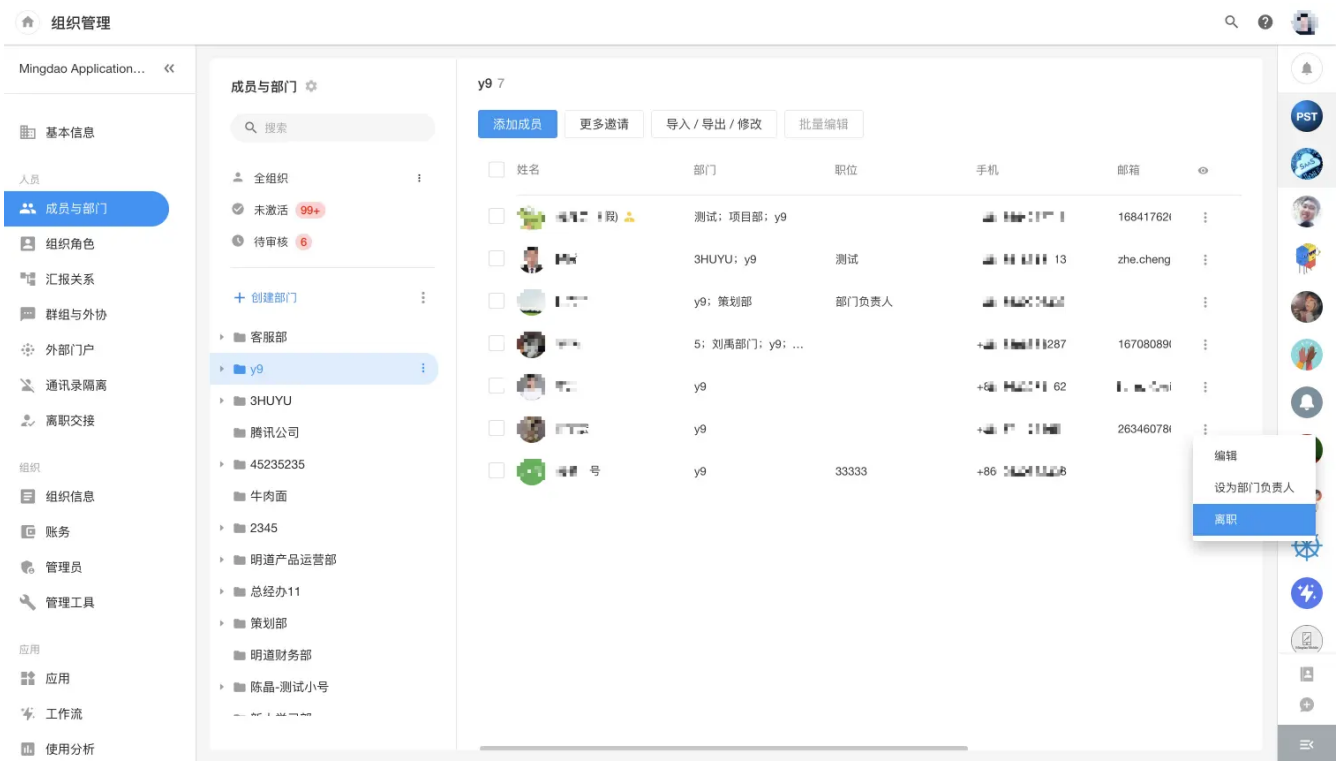
使用基于身份证号码和密码的基于生物特征的电子签名，必须采取控制措施以确保其安全性和完整性。这些控制措施应包括：

- 维护每个联合身份代码和密码的唯一性 - 确保定期检查、回收或修订身份和密码发布。
- 为电子签名可能受到攻击的身份代码或密码信息制定程序。
- 用于防止未经授权使用密码和 / 或身份代码，并防止未经授权使用的任何试图的行为的交易保护。

系统能力说明：

- 系统确保每个用户 ID 只都是唯一的，并且不可被篡改。
- 建议在整个组织范围内为所有系统提供 ID 码和指南，由运营者指定用户账户的创建和密码的使用（长度、有效期…）。

- 该系统支持操作员通过密码过期功能——有效期到期后，用户被迫更改密码。
- 如果出现可能被盗用的身份证号码或密码，则可以在系统中通过系统管理员进行离职操作，但仍然可以保存在系统中，没有任何访问权限。



- 由管理员定义的错误尝试次数达到最大值后，系统显示用户最大尝试次数达到最大值且被禁用，任何尝试连接失败的用户将记录在审计跟踪中。