ICS 03.120.10
CCS A 00

DB51

四 川 省 地 方 标 准

DB51/T 2874—2022

检验检测机构保护客户秘密实施指南

2022-02-24 发布　　2022-04-01 实施

四川省市场监督管理局 发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由四川省市场监督管理局提出、归口并解释。

本文件起草单位：四川省产品质量监督检验检测院、广元市产品质量监督检验所、成都市产品质量监督检验研究院、四川凯乐食品检测有限公司。

本文件主要起草人：胡丹、姬洪涛、张文龙、韩渝、王睿、韩勇、何羽乔、唐诗俊、赵瑞麒、江瑜、蒋美琴、谷雨、杨沐、丁劲松、曾珂、陈洁。

本文件首次发布。

检验检测机构保护客户秘密实施指南

1 范围

本文件规定了检验检测机构保护客户秘密的基本要求、涉及客户秘密过程识别及管理、内部涉密人员管理、涉密载体管理、风险管理、审核和改进等内容。

本文件适用于取得资质认定（CMA）或实验室认可（CNAS）的检验检测机构。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 17859-1999计算机信息系统安全保护等级划分准则

GB/T 24353 风险管理 原则与实施指南

GB/T27025 检测和校准实验室能力的通用要求

RB/T 214 检验检测机构资质认定能力评价 检验检测机构通用要求

3 术语和定义

GB/T 19000、GB/T 27025、RB/T 214界定的以及下列术语和定义适用于本文件。

3.1

检验检测机构 inspection body and laboratory

依法成立，依据相关标准或者技术规范，利用仪器设备、环境设施等技术条件和专业技能，对产品或者法律法规规定的特定对象进行检验检测的专业技术组织。

[来源：RB/T 214-2017,3.1]

3.2

客户 customer

能够或实际接受为其提供的，或按其要求提供的产品或服务的个人或组织，如消费者、最终使用者、零售商、公共组织、公司、集团、企事业单位、行政机构、协会、研究机构等。

[来源：GB/T 19000-2016，3.2.1,有改写]

3.3

活动 activity

由一组有起止日期的、相互协调的受控活动组成的独特过程中识别出的最小的工作项。

[来源：GB/T 19016-2005.3.1,有改写]

3.4

国家秘密 state secret

关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。

3.5

商业秘密 trade secret

不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

3.6

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息。

注：个人信息包括：自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

3.7

涉密人员 secret-related personnel

根据工作职责或者保密协议有权接触、使用、掌握涉密信息的检验检测机构员工或其他人。

3.8

涉密的载体 secret-related carrier

以文字、数据、符号、图形、实物、视频和音频等形式记载和存储秘密信息的纸介质、光介质、电磁介质、产品、样品等各类物品。

注1：纸介质涉密载体是指传统的纸质涉密文件资料、书刊、图纸等。

注2：光介质涉密载体是指利用激光原理写入和读取涉密信息的存储介质，包括CD、VCD、DVD等各类光盘。

注3：电磁介质涉密载体包括电子介质和磁介质两种，包括各类闪存盘、硬磁盘、软磁盘、磁带等。

3.9

涉密区域 secret-related area

可以接触到客户秘密信息的一切场所。

注：如实验室、办公室、档案室、机房等。

4 基本要求

4.1 检验检测机构应依据国家保密相关法规及相关标准建立保护客户秘密的制度，制定保护客户秘密的程序文件，对保密要求、保密职责、涉密载体的管理、涉密人员管理、相关活动涉及客户秘密识别、风险评估等内容做出规定，并宣贯和实施。

4.2 检验检测机构在实验室活动中获得的或产生的以下信息，均为客户秘密：

——客户提交检测的资料及样品，工艺流程、设计图纸、技术依据、外观设计（照片）、产品技术说明书、专利技术、顾客送检附带的信息，试样或产品；

——检验检测活动中所获取的有关信息，检测数据和结果；

——客户要求其他保密的信息或者特别规定的保密信息。

4.2.1 客户秘密保密要求由客户提出，必要时签订《保密协议》对保密内容和期限进行约定，机构应根据法律规定或双方约定并按以下原则采取相应保密措施：

a) 涉及国家秘密，应按照《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施条例》及相关法律法规执行。

b) 涉及客户的商业秘密，按照协议约定履行保密义务.

c) 涉及自然人的个人信息，应按照《个人信息保护法》及相关法律法规执行

4.3 如需对外披露客户秘密，以下要求需注意：

a） 依据法律要求或合同授权需透露保密信息时，应按照 GB/T 27025 中 4.2.2 要求，将所提供的信息通知到相关客户或个人；
b） 建立对外披露客户秘密审批责任，明确对外披露客户秘密审批要求和流程；
c） 对披露客户秘密进行检查，发现问题，立即采取补救措施。

4.4 涉密区域管理，根据机构实际情况有条件的机构可设置门禁、视频监控装置；可适时采用信息化手段对区域的管理进行实时记录和监控。

4.5 机构涉密人员内部沟通时，应尽量避免在任何社交媒体、即时通讯软件私自传输，发送涉及客户的信息。

4.6 机构应根据需要配置检验检测业务管理系统，制定访问控制策略，可参照 GB17859-1999 的要求进行软硬件配置，必要时可对机构信息系统保密等级及符合性进行第三方权威机构的审查认定。有条件的机构可配置终端管理程序，用于记录操作终端对涉密信息拷入拷出，截屏和屏幕拍照等操作，实现可追溯。

5 涉及客户秘密的过程识别及管理

5.1 检验检测机构与客户信息（不论是获取还是工作过程产生的）有接触的任何个人和任何活动，不论是内部还是外部，都应视为涉密，纳入保护客户秘密的管理中。

5.2 检验检测机构在合同评审阶段，应与客户就保密事项和要求予以约定，将约定内容纳入合同或协议中，如有必要可另行签订专门的保密合同，专项约定保密内容及期限。

5.3 检验检测机构应保留合同履行过程中保护客户秘密的记录。

5.4 内部活动中客户秘密的保护

5.4.1 分包,

将任务分包给满足要求的检验检测机构时，确保但不限于以下措施得以实施：
a） 应与接受分包任务的检验检测机构明确保密要求；
b） 应对保密要求及内容用合同的形式予以约定，必要时签订专门的保密协议，约定保密内容及期限。

5.4.2 采购

当检验检测机构需采购服务时，如设备检定和校准服务，设备设施的运输、维护和保养，样品制备和运输等，确保但不限于以下措施得以实施：
a） 应就保密要求与提供服务方进行约定，对保密事项提出要求；
b） 应对保存在设备或电脑中的信息进行加密；
c） 在对供应商进行评价时，应将遵守保密协议的情况纳入评价内容。

5.4.3 服务客户

当允许客户或其代表合理进入为其检验检测的相关区域观察时，确保但不限于以下措施得以实施：
a） 应确保其他客户的机密得到保护；
b） 检验检测机构应对客户进入检验检测现场的区域和路线进行限定，并经过相应审批；
c） 必要时，对现场涉及到的其他客户的检测活动暂时停止；
d） 必要时，对现场在检其他客户的样品进行遮盖或遮挡。

5.4.4 投诉

从客户以外渠道（如投诉人、监管机构）获取有关客户的信息时，确保但不限于以下措施得以实施：

a） 应在客户和实验室间保密；
b） 除非信息的提供方同意，实验室应为信息提供方（来源）保密，且不应告知客户或其他方；
c） 检验检测机构应限定知悉人员的范围，与活动无关的人员无权知悉；
d） 在调查处理时，必要时可将信息拆分，分别告知办理投诉相应职责人员。

5.4.5 数据信息管理

利用计算机或自动化设备对检验检测数据进行采集、处理、记录、报告、存储或检索时，确保但不限于以下措施得以实施：

a） 应对登陆系统操作人员进行审批；
b） 应根据岗位职责对可操作范围和内容给定权限范围；
c） 应对登陆密码设定的复杂程度作出要求；
d） 应对登陆操作特别是删除、拷贝、传输等进行记录。

5.4.6 样品处置

样品在运输、接收、处置、保护、存储、保留、清理或返回过程应予以控制和记录，以保护样品的完整性并为客户保密，确保但不限于以下措施得以实施：

a） 样品接收人员应按客户要求并遵照合同约定对样品进行分类，及时入库并妥善保管；
b） 有条件的检验检测机构可配置实时音视频记录装置，用于从样品接收、入库、流转全过程记录；
c） 检测现场待检样品应于检测前再拆封，尽量避免相关信息的暴露；
d） 在对样品进行清理和处置中，应做好登记，待审批后采取相应措施予以处置；
e） 需清理和处置的样品，应对其标签标识尽量涂抹损坏至不便于识别；
f） 对于有特殊保密要求的样品，应按签署的保密协议分类分区保存；
g） 对特殊保密样品应进行保密标识以便于识别；
h） 在检测过程中，可采用防护屏风或防护罩等措施适当隔离，并限定知悉人员数量。

5.4.7 结果传送和格式

当客户需要使用电话、传真或其他电子或电磁方式传输报告时，确保但不限于以下措施得以实施：

a） 应有客户要求的记录；
b） 如使用电子邮箱发送，应发送至客户指定的电子邮箱，发送前应对邮箱的正确性再次确认，并及时向客户确认收件情况，同时做好记录；
c） 尽量避免使用如微信或QQ此类即时通讯软件为客户传输检验检测结果，除非有证据表明客户同意；
d） 如使用传真，应确认接收方的真实身份后方可传送结果。

5.5 外部活动中客户秘密的保护

5.5.1 除内部检验检测活动外，检验检测机构因为机构间合作、资质获取、发展需要等事项而开展的实验室参观、评审、出租或租用设备设施等活动，机构应对这些活动采取适当措施以确保其他客户秘密得到保护。

5.5.2 应制定相应管理文件并采取适宜的保护措施，对外来参观人员、审核人员、合同方人员进入实验室进行控制。

a) 当外来人员到本检验检测机构参观、学习时，应对样品或结果予以控制和保护,参见本文件5.4.3的要求实施客户秘密的保护。

b) 对外出租或租用设备设施情况时，例如：EMC、电气防爆实验室等，可采取以下保护措施：

——必要时，应对出租或租用设备设施区域采取适当措施予以隔离；

——应对非本实验室人员在进入本实验室的活动范围进行限定。参见本文件5.4.3的要求实施客户秘密保护。

c) 外部评审，检验检测机构接受第二方或第三方评审时，应对需保密的事项、需保密区域以及保密要求予以说明，必要时，双方签订保密协议。

6 内部涉密人员管理

检验检测机构应采取相应措施对内部涉密人员进行相应的管理，包括但不限于以下措施：

a) 签订保密承诺书，承诺书内容包括但不限于以下内容：
   1) 保密的内容和范围；
   2) 保密的权利和义务；
   3) 保密的期限；
   4) 违约责任；
   5) 其他需约定事项。

b) 保密培训，对机构内部涉密人员开展保密教育和培训，确保其了解保密的责任和义务，包括但不限于以内容：
   1) 相关法律法规；
   2) 机构管理制度及文件；
   3) 接触涉密信息的范围及接触超越此范围涉密信息的审批程序；
   4) 风险管理要求。

c) 离职管理，对于离开本检验检测机构的涉密人员，检验检测机构应采取以下措施：
   1) 离职面谈，告知员工负有的保密义务，以及其他约定或法定的注意事项；
   2) 退还涉密载体；
   3) 签订保密承诺书。

d) 根据知悉需要，将涉及客户秘密的完整事项分割，进行分段化管理。

7 涉密载体的管理

7.1 建立涉密载体台账，实施涉密载体的制作、收发、传递、使用、复制、保存、维修、销毁的全生命周期管理，防止未授权的使用、访问，防止被盗。

7.2 涉密载体制作需明确以下事项：

a) 制作过程的保护措施和管理权限；

b) 使用或发放范围和制作数量。

7.3 指定专人负责涉密载体的传递。

7.4 涉密载体使用，需符合以下要求：

a） 涉及系统登陆，根据工作需要，给使用人授权，给定相应权限的账号；
b） 存放在相应区域的涉密载体，使用门禁装置，还可设置实时监控便于追溯；
c） 在使用涉密载体时按规定履行审批；
d） 携带涉密载体外出或外发涉密载体时按规定履行审批；
e） 携带外出或外发的涉密载体使用完毕后及时交回并做好登记。

7.5 涉密载体在需要复制时，应符合以下要求：
a） 履行审批、登记手续；
b） 加盖标识，可以是专门的复制专用章，并视同原件管理。

7.6 涉密载体的保存、清理、销毁符合以下要求：
a） 环境场所条件满足涉密载体的存放；
b） 定期清查、核对涉密载体；
c） 维修维护一般由本检验检测机构机构专人负责，确需外部人员现场维修的，应指定专人全程现场监督；
d） 销毁涉密载体应履行审批手续，并进行清点和登记；
e） 已销毁的涉密载体中的秘密信息无法还原。

8 风险管理

检验检测机构要把机构保密过程纳入风险管理，每年至少进行一次风险评估。

9 审核和改进

9.1 检验检测机构应对保护客户秘密的管理文件和保密措施进行评审评估，确保其适宜。
9.2 应对保护客户秘密实施情况进行审核检查，确保措施落实到位，满足要求，记录可追溯。
9.3 应根据风险评估、评审和审核结果、客户反馈等信息来持续改进保护客户秘密的管理。