附件 1

团　　体　　标　　准

T/CAQI xxx-xxxx

涉密印制业务管理要求

Management requirements of secret-related printing business

（征求意见稿）

2024-xx-xx 发布　　2024-xx-xx 实施

中国质量检验协会　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由提出。

本文件由归口。

本文件起草单位：

本文件主要起草人：

涉密印制业务管理要求

1 范围

本文件规定了涉密印制单位的涉密印制业务承接管理要求、印制业务加工控制要求、场所管理要求、信息设备使用要求、人员管理要求及监督检查要求。

本文件适用于涉密文件资料类与涉密档案数字化加工类国家秘密载体印制单位规范管理，提高从业人员的保密管理能力和作业规范化水平。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

本文件没有需要界定的术语和定义。

4 涉密印制业务承接

4.1 总则

4.1.1 基本原则

涉密印制业务承接应遵循“严格管理、严密防范、确保安全、方便工作”的原则。

4.1.2 过程管理

应实行全过程管理，明确岗位责任，落实各环节安全保密措施，确保管理全程可控可查。

4.1.3 保密责任

应实行以部门负责人为第一责任人的逐级保密责任制，坚持“谁主管、谁负责”和“谁使用、谁负责”的原则。

4.1.4 人员要求

参与涉密项目的营销人员、管理人员、技术人员、印制人员应为印制单位的涉密人员并进行登记备案，按照工作需要严控其对涉密信息的接触范围和知悉程度。

4.1.5 资质要求

应按照资质等级、类别、生产能力承接涉密印制业务，不应无资质或超出资质许可范围承揽业务，未经委托方书面同意不应将承接的涉密印制业务分包或转包。

4.2 业务承接

4.2.1 业务对接

印制单位应安排与项目密级一致或高于项目密级的涉密人员承接项目，与委托方进行生产工艺、生产周期、产品质量等详细对接，并核实涉密等级信息。

4.2.2 招采项目

4.2.2.1　采用招投标、比质比价、竞争谈判等方式承接涉密印制业务的，由印制单位授权与项目密级一致或高于项目密级的涉密人员领取项目招采文件，编制投标或响应文件并进行投标响应。招采文件应在涉密场所涉密计算机中输入、输出和编制，并履行相应审批登记手续。

4.2.2.2　招标过程如需使用资质证书，应履行审批手续。严禁涂改、出卖、出租、出借资质证书或者以其他方式伪造、非法转让资质证书。一般使用证书复印件，在证书复印件上加盖公章，并在证书复印上写明使用权限。

4.2.2.3　投标失败的涉密项目，投标人员按照招标方要求处置招标文件，投标人员应监督制作人员将涉密计算机中相关文件及时进行信息消除。

4.2.2.4　中标后，投标人员应及时领取中标通知书，签订涉密印制业务合同。

4.2.3　非招采项目

4.2.3.1 非招投标项目，印制单位可与委托方直接签订涉密印制合同。

4.2.3.2 对于无书面合同的涉密印制业务，或者涉密印制业务合同属于框架合同的，执行具体印制业务时，印制单位应查验、收取委托方书面委托印制证明，书面明确密级和印制数量，履行文件资料接收手续。不应无委托印制证明开展涉密印制业务。

4.3　业务管理台账

4.3.1　涉密印制业务应建立管理台账，内容包括项目编号、委印单位、印制现场保密负责人、参与印制人员及分工、主要印制设备、印制时间、品种、密级、载体形式、数量、载体交接记录、交付情况等。

4.3.2　各类信息台账中，不应出现涂抹、修改，确有必要修改的，应由经办人及上级管理人员签字确认，并记录修改时间、作业过程。

4.3.3　台账保存时间不少于3年。

5　涉密印制业务加工及交付

5.1　涉密文件资料

5.1.1　涉密文件资料印制

5.1.1.1　作业通知

印制单位接到委托方印制需求信息后，应根据作业要求填写印制作业通知单，明确生产工艺、印制数量、密级、原辅材料用量、完工时限及送货交接方式等准确信息。

5.1.1.2　生产组织

印制单位应根据项目密级安排确定知悉范围，部署具体参与印制的生产作业人员、印制设备。相关作业人员应按要求进行作业，各工序做好涉密载体交接，并填写相关记录。

5.1.1.3　扫描录入排版

作业人员应仔细阅读作业通知要求和确认原稿，文件资料如包含多项内容，应先逐条确认文件目录或内容后再进行排版、修改工作。

5.1.1.4　校对签样

设计、排版工作完成后，作业人员应征询委托方意见，是否进行校对，必要时先印制样稿交予委托方进行核对，发现问题及时沟通并改正。校对完毕应由委托方签字确认。

5.1.1.5　印刷装订

应由设计、排版作业人员将文件交至制版、印刷人员，办理交接手续进行后道工序，根据作业要求严格控制涉密制版、印刷、装订数量。半成品宜采取遮盖、缠膜或放入保密柜等方式进行载体保护，避免信息暴露。

5.1.1.6 过程文件

涉密印制过程中所形成的过程文件，包括文件草稿、废稿、废页、讨论稿、征求意见稿、审议稿等，应按照保密文件要求处理。

5.1.1.7 光盘刻录

刻录光盘严格履行审批手续，使用带编号光盘刻录，填写光盘刻录登记记录；刻录产生的废盘，应按要求放入废品柜中，并填写废品登记记录。

5.1.2 涉密文件资料成品交付

5.1.2.1 成品入出库

尚未交付的成品应存放于成品库，并填写成品入库记录；出库时应填写成品出库记录。

5.1.2.2 废品入出库

印制过程中产生的废品、残次品以及印版应存放于废品库，并填写废品入库记录；出库时应填写废品出库记录。

5.1.2.3 成品交付

成品交付前，作业人员应专门对文件中的涉密标识和封装情况进行检查，确认无误后，将成品文件、样书、样稿交付委托方，填写交接记录，及时进行电子信息消除。

委托方要求代发原件、清样和成品的，印制单位应通过机要交通、机要通信、机要文件交换站等符合安全保密要求的方式和渠道传递，或由印制单位安排封闭专车、专人发送，封闭式车辆锁具、门窗应完好，押运人员途中不得离车。

5.1.3 涉密文件资料载体管理

5.1.3.1 载体包装防护

传递、转移涉密载体应密封包装。涉密载体的外包装上应标明密级、编号和收发件单位名称。

5.1.3.2 文件带出

因工作需要携带涉密载体外出，应履行审批程序，采取可靠的安全保密措施，选择安全的交通工具和交通路线。携带绝密级载体应经本单位主管领导批准，应有两人以上同行，并明确主次责任。

5.1.3.3 电子文档留存

委托方要求涉密印制单位留存电子文档继续使用的，应将信息设备中的电子文档移存到光盘中，存放应当符合保密要求。双方办理留存保管手续，留存期限不得超过60日。

5.1.3.4 载体销毁

存放于废品库中的涉密载体需要销毁时，库管人员应当履行清点、登记、审批手续，由专人押运送交保密行政管理部门设立的销毁工作机构或者保密行政管理部门指定的单位销毁，并留存销毁记录。

5.2 涉密档案数字化

5.2.1 涉密档案数字化加工

5.2.1.1 人员备案

涉密档案数字化加工作业前，加工单位应将参与作业人员信息向委托方备案。

5.2.1.2 档案调取归还

档案实体应指定专人管理，调取、归还均应由委托方人员与加工单位指定人员当面清点，办理交接手续。作业完成后，应将全部涉密档案实体归还委托方，不得擅自留存。

委托方在作业过程中调取档案，应持审批手续，与加工单位指定人员当面清点数量，办理交接手续。

5.2.1.3 现场保管

调取档案实体后，应存放于作业场所的保密柜中。作业过程中，领取档案实体应进行登记；作业人员离开时或作业完成后，应清点登记，放回保密柜中。

5.2.1.4 各工序流转

作业人员按照作业通知要求，完成目录数据准备、拆除装订、页面修整、扫描、装订等作业，上下工序交接时，作业人员应当面清点档案实体数量，办理交接手续。

5.2.1.5 共同监管

加工单位和委托方应在涉密档案数字化加工过程中，对作业过程进行共同监督和管理，留存检查记录。

5.2.2 涉密档案数字化成果交付

5.2.2.1 验收交付

涉密档案数字化加工作业完成，经委托方验收，应将全部成果进行交付。成果交付方式应按委托方的要求，不应使用互联网及其他公共信息网络进行传递交付。交付时，应由加工单位指定人员与委托方人员当面清点，办理交接手续。

5.2.2.2 载体移交

应将全部使用过的存储介质等信息载体移交给委托方，不应擅自留存。

5.2.2.3 信息消除

所有加工设备中存储的加工信息应在委托方的监督下，按照国家保密标准要求进行信息消除，并履行审批登记手续。

5.2.2.4 过程记录

所有过程记录（包括调取、归还涉密档案实体的交接手续）均需存档，留存不少于3年。

签订合同时，委托方要求过程记录均须留给委托方的，可由委托方开具表明实施方实际有的作业过程记录清单的书面证明，签字盖章后代替作业过程记录存档。

6 涉密业务场所管理

6.1 概述

涉密业务场所专门用于处理涉密事项和存储涉密载体，包括涉密印制车间、成品库、废品库、保密室等，以及涉密档案数字化加工业务委托方所提供的涉密场所。

6.2 场所界定

涉密业务场所的界定应遵循“最小化”原则，应相互独立、封闭、可控，与非涉密业务场所有明确划分，并进行标识。场所符合保密要害部位的防护要求。

6.3 场所管理

6.3.1 涉密业务场所应实行封闭管理，控制人员进入，出入应审批登记。

6.3.2 不应携带具有摄照相、录音、存储、通信功能的信息设备进入涉密业务场所；确需带入时，携带人应填写审批记录，经审核批准后方可带入。

6.3.3 涉密业务场所出入口应设置门禁系统，内部应安装防盗报警装置，外周界应安装视频监控系统，涉密业务场所外应配备专柜供存放私人物品。在涉密场所内安装视频监控的，不应拍摄到密码以及涉密载体的内容。

6.3.4 涉密成品库和废品库应采用双人管理，一人拥有门禁系统开关权限，一人拥有机械锁开关权限。

7 信息设备使用

7.1 概述

信息设备包括涉密印制所需办公电脑、办公自动化设备、涉密信息存储介质、秘钥等。

7.2 安全防护

7.2.1 涉密计算机应设置BIOS、开机、屏保3重密码，同时配合秘钥共同使用。

7.2.2 应每半月对涉密计算机病毒库进行升级，升级完成后对涉密计算机进行全盘查杀，并将病毒查杀过程中发现的计算机病毒及其他异常状况进行及时处理。

7.2.3 应在操作系统、数据库、应用系统的补丁发布后的3个月内，为涉密计算机进行安装，并检查涉密计算机软件运行情况。

7.2.4 不应未经审批对涉密计算机进行格式化或重装操作系统。不应删除涉密计算机的任何日志记录。

7.2.5 涉密人员在涉密计算机上只能浏览、操作知悉范围内的涉密信息，使用时应填写计算机使用登记记录，记录使用痕迹。

7.2.6 涉密信息设备应张贴设备标识和保密提醒警示语。设备标识的设备编号、设备类型、用途、部门、责任人、密级等信息要素应当完整。

7.2.7 涉密存储介质应张贴标识，应包括设备编号、密级、责任人等信息。如果无法粘贴标签或粘贴后影响使用的，应采用不可擦除的标记方式标注相关信息。

7.2.8 涉密信息设备应实行全生命周期管理，并按照“一机一档”建立保密管理档案，管理档案应当包括定密记录、变更记录、启用记录、运维记录、维修记录、报废和销毁记录等。

7.3 台账建立

7.3.1 应建立涉密计算机、涉密办公自动化设备、涉密存储介质台账，台账要素包括：名称、型号、编号、密级、用途、责任部门、责任人、硬盘序列号、设备序列号、操作系统版本、操作系统安装日期、IP地址、MAC地址、启用日期、放置地点、使用情况等。

7.3.2 应建立安全保密产品和计算机病毒防护产品台账，台账要素至少包括：产品名称、产品型号、编号、密级、数量、生产厂家、检测证书名称和检测证书编号、购置时间、启用日期、责任人、使用情况等。非涉密存储介质台账宜参照涉密存储介质要求。

7.3.3 涉及身份鉴别的秘钥应单独建立台账，填写身份鉴别秘钥台账。

7.3.4　应建立光盘台账，包括操作系统安装光盘、软件安装光盘、清除工具光盘、检查工具光盘、病毒库升级光盘。

7.4　维保与报废

7.4.1　涉密打印机应指定专人更换硒鼓，旧硒鼓存放至废品库，并履行登记手续。
7.4.2　涉密信息设备进行维护检修时，应经过审批；应保证所存储的涉密信息不被泄露。第三方单位现场维修时，印制单位相关人员应全程旁站陪同，并做好相关记录，维修完成后进行保密检查和性能检查。
7.4.3　涉密信息设备报废时，应经审批同意后办理报废手续。报废前应先进行信息消除，拆除具有存储功能的部件或设备，存放至废品库，并履行登记手续。

7.5　设备携带外出

7.5.1　不应私自将身份鉴别秘钥、涉密移动存储设备带出涉密场所。
7.5.2　携带涉密设备外出应履行审批登记手续；不应携带涉密设备探亲访友、参观、购物、旅游及去往其它公众场所；涉密设备外出前及返还时，安全管理员应对其进行保密检查。

7.6　信息导入导出

7.6.1　涉密计算机与外部信息进行交互和传递应使用中间机，中间机与涉密计算机应安装不同的病毒和恶意代码样本库查杀软件，外部信息经中间机进行病毒和恶意代码查杀处理后，单向传递到指定的涉密业务机。
7.6.2　涉密信息设备中的信息导入导出应履行审批手续，并保证导入导出信息在审批和导入导出过程中的完整性和唯一性。

8　涉密人员管理

8.1　概述

涉密人员是指与涉密印制相关的营销人员、生产加工人员、管理人员等。分为核心涉密人员、重要涉密人员、一般涉密人员。

8.2　岗前管理

8.2.1　对于拟入涉密岗位工作的人员，应坚持“先审查后录用、先培训后上岗”的原则进行审查和培训。核心涉密人员、重要涉密人员应对其本人和本人父母、配偶、子女的基本情况、现实表现、主要社会关系以及可能影响国家安全利益的倾向等方面进行背景审查。
8.2.2　拟上岗的涉密人员有半年以上出国（境）外学习、工作、生活经历的，需进行国家安全背景调查。

8.3　在岗管理

8.3.1　涉密人员基本情况和调整变动情况应在公安机关出入境管理机构及保密行政管理部门定期登记备案。
8.3.2　涉密人员应定期进行复审，核心涉密人员每1年复审一次，重要涉密人员每2年复审一次，一般涉密人员每3年复审一次。
8.3.3　核心涉密人员无特殊原因禁止出国（境），重要涉密人员出国（境）每2年不应超过1次，一般涉密人员出国（境）每年不应超过1次。
8.3.4　涉密人员出入境证件应交单位集中保管。

8.3.5　涉密人员出国（境）的，应提前15个工作日提出申请，由单位批准，必要时应征求涉密业务委托方意见。
8.3.6　按期回国（境）后的涉密人员应在7个工作日内将出国（境）证件上交单位。
8.3.7　涉密印制单位应对回国（境）后的涉密人员进行回访。
8.3.8　涉密人员发生重大事项变动的应及时向单位报告。

8.4　离岗管理

8.4.1　涉密人员因调离、辞职、解聘或退休等原因离开涉密岗位的，应签订脱密期保密承诺书，经单位审批后实施脱密期管理。
8.4.2　涉密人员离岗前，应清点并清退本人负责保管和使用的国家秘密载体、涉密信息设备、涉密存储设备等，个人不得擅自销毁或做其它处理。
8.4.3　核心涉密人员脱密期为3年、重要涉密人员脱密期为2年，一般涉密人员脱密期为1年。应由单位对其进行脱密期管理，脱密期内单位要定期对脱密人员进行回访。
8.4.4　涉密人员在脱密期内，应按照规定履行保密义务，在脱密期内不应到境外驻华机构、组织或外资企业工作，不应为境外组织人员或者外资企业提供劳务、咨询或其他服务，发生重大事项变动的应及时向单位报告。不应以任何方式泄露国家秘密。

8.5　教育培训

8.5.1　凡进入涉密岗位的员工，应经保密教育培训、掌握保密知识技能，考核合格、签订保密承诺书后方能上岗。
8.5.2　在岗涉密人员每年参加保密教育与保密知识、技能培训的时间不少于10学时。
8.5.3　涉密人员离岗离职前，单位应对其进行保密教育，提醒其在离岗离职后认真履行保密义务，加强保密法律法规、失泄密案例、保密制度等方面的教育。
8.5.4　涉密人员出国（境）前，单位应对其进行保密教育。
8.5.5　举办涉密会议前，会议主办部门应对参会人员进行保密教育。
8.5.6　上下半年应各举行保密知识考试不少于1次，满分100分，80分为及格。

9　监督检查

9.1　总则

9.1.1　印制单位应定期组织开展保密检查，并对保密检查中发现的问题进行督促整改及验证。
9.1.2　保密检查应当有书面记录，记录内容包括：检查时间、检查人、检查对象、检查事项、存在问题、整改措施及落实情况等。

9.2　范围与频次

9.2.1　保密检查应针对业务承接、印制加工、业务场所、信息设备、涉密人员等全方面开展。
9.2.2　全面检查每半年1次，部门自查每季度1次，专项检查按照保密行政管理部门或上级管理单位要求不定期开展。

参 考 文 献

［1］ BMB 21—2007 涉及国家秘密的载体销毁与信息消除安全保密要求

［2］ BMB 48—2020 保密要害部位安全保密防护要求

［3］ GA/T 367 视频安防监控系统技术要求