中鸿认证（江苏）有限公司

隐私信息管理体系认证实施规则

规则编号：ZHCC-R-08-A

文件版本：C/1

受控状态：受控文件

编写人员：技术部

审核人员：韩自鹤

批准人员：丁泽林

发布日期：2023年4月12日

修订日期：2025年8月25日

实施日期：2025年8月25日

目录

1.适用范围

2.对认证机构的基本要求

3.对认证人员的基本要求

4.认证依据

5.初次认证程序

6.监督审核程序

7.再认证程序

8.认证证书状态管理要求（暂停、撤销、注销、恢复、失效）

9.认证证书及认证标志要求

10.与其他管理体系的结合审核

11.受理转换认证证书

12.证书的更换

13.受理组织的申诉

14.认证记录的管理

15.其他

附录 A 认证审核时间要求

1.适用范围

1.1 本规则用于规范中鸿认证（江苏）有限公司（简称中鸿认证）开展隐私信息管理体系（PISMS）认证活动。

1.2 本规则是依据认证认可相关法律法规及认可规范，对（PISMS）认证实施过程作出具体规定，强化 ZHCC 对认证过程的管理和责任。

1.3 本规则是对 ZHCC 从事 PISMS 认证活动的基本要求，ZHCC 从事该项认证活动应当遵守本规则。

1.4《国家认监委关于加强认证规则管理的公告》（2025 年第 9 号）

2.对认证机构的基本要求

2.1 ZHCC应获得国家认监委备案后方可开展隐私信息管理体系认证。

2.2 建立可满足 GB/T 27021《合格评定 管理体系审核认证机构的要求》的内部管理体系，以使从事的认证活动符合法律法规及技术规范的规定。

2.3 建立内部制约、监督和责任机制，实现受理、培训（包括相关增值服务）、审核和作出认证决定等环节的相互分开。

2.4 鼓励 ZHCC 通过认可机构的认可，证明其从事的认证能力符合要求。

3.认证人员的基本要求

3.1 审核人员应当具有 CCAA 注册的信息安全或信息技术服务管理体系审核员注册资格。

3.2 云服务信息安全审核员专业评定要求如下：通过公司组织的云服务信息安全管理体系标准知识及相关内容的培训考试，可获得云服务信息安全管理体系相关技术领域专业。

3.3 云服务信息安全管理体系审核组长应具备审核组长资格。

3.4 认证规则、认证方案制定人员和合同评审人员、认证决定人员、人员能力评价人员、审核方案管理人员应经评价确认满足 ZHCC 人员能力的要求，应具备项目管理人员资格。

3.4.1 如认证规则、认证方案制定人员和认证决定人员、人员能力评价人员同时为审核员时，对其审核员资格的评价可替代其认证管理人员的能力评价。

3.5 云服务信息安全管理体系技术专家应具备大专学历以上；3 年以上与云服务信息安全管理相关的全职工作经历；技术专家专业能力评定至各技术领 域。

认证人员应当遵守与从业相关的法律法规，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

4.认证依据

4.1 ISO/IEC 27001:2022 信息安全 网络安全和隐私保护 信息安全管理体系 要求

4.2 ISO IEC 27701:2019 《安全技术 针对ISO/IEC27001和ISO/IEC27002在隐私信息管理的扩展－要求和指南》

5.初次认证程序

5.1.初次认证

5.1.1. 受理认证申请

ZHCC 市场部应向申请认证的组织（以下简称申请组织）进行信息公开，信息公开可采用公司官网进行公开，也可以在客户进行合同洽谈的时机，通过钉钉、微信、邮箱等单一方式或者多种方式相结合，公开的信息至少包含以下信息：

（1）可开展认证业务的范围，以及获得认可的情况。

（2）本规则的完整内容。

（3）ZHCC 的授予、保持、扩大、更新、缩小、暂停或撤销认证及其证书等环节的制度规定。

（4）认证证书样式。

（5）对认证决定的申诉程序。

（6）认证流程及公开文件。

5.1.2 ZHCC 市场部应当要求申请组织提交以下资料：

（1）认证申请书，包括业务活动、组织架构、联系人信息、物理位置和体系范围等基本内容。

（2）法律地位的证明文件（包括：企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书、党政机关设立文件等）的复印件。PISMS 覆盖多场所活动时，应提交每个场所的法律地位证明文件的复印件（适用时）。

（3）PISMS 覆盖的活动所涉及法律法规要求的行政许可证明、资质证书、强制性认证证书等的复印件。

（4）PISMS 管理体系手册

（5）必要的程序文件及证明公司符合本标准中的各项要求所必需的适当的记录等

（6）PISMS 已有效运行 3 个月以上的证明材料。

（7）其他与认证审核有关的必要文件。

5.1.3 认证申请的审核确认

ZHCC 审核部申请评审人员应对申请组织提交的申请资料进行审核，并确认：

（1）申请资料齐全。

（2）申请组织从事的活动符合相关法律法规的规定。

（3）申请的认证范围、申请组织的运作场所和任何其他影响认证活动的因素已经得到识别和确认。

5.1.4 根据申请组织申请的认证范围、生产经营场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

对被执法监管部门责令停业整顿或在国家企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，认证机构不应受理其认证申请。

5.1.5 对符合 5.1.3、5.1.4 要求的，ZHCC 可决定受理认证申请；对不符合上述要求的，ZHCC 市场部应通知申请组织补充和完善，或者不受理认证申请。

5.1.6 ZHCC 应完整保存认证申请的审核确认工作记录。

5.1.7 签订认证合同

在实施认证审核前，ZHCC应与申请组织订立具有法律效力的书面认证合同，合同应至少包含以下内容：

（1）申请组织获得认证后持续有效运行PISMS的承诺。

（2）申请组织对遵守认证认可相关法律法规，协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺。

（3）申请组织承诺获得认证后发生以下情况时，应及时向ZHCC通报：

① 相关方有重大PISMS有关方面的投诉。

② PISMS范围内业务活动或行为被执法监管部门认定不符合法定要求。

③ 有严重与PISMS相关事故的信息；

④ 组织的体系文件和业务重大变化；

⑤ 出现影响PISMS运行的其他重要情况。

（4）申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息；不擅自利用PISMS认证证书和相关文字、符号误导公众认为其产品或服务通过认证。

（5）拟认证的PISMS覆盖的企业活动、产品和服务范围。

（6）在认证审核及认证证书有效期内各次监督审核中，ZHCC和申请组织各自应当承担的责任、权利和义务。

（7）认证服务的费用、付费方式及违约条款。

5.2 建立审核方案

5.2.1 审核时间

5.2.1.1 为确保认证审核的完整有效，ZHCC 市场部申请评审人员应以附录 A 所规定的审核时间为基础，根据申请组织 PISMS 覆盖的活动范围、特性、技术复杂程度、认证要求和员工人数等情况，核算并拟定完成审核工作需要的时间。

5.2.1.2 整个审核时间中，现场审核时间不应少于 70%。

5.2.2 审核组

5.2.2.1 ZHCC 审核部审核计调人员应当根据 PISMS 覆盖的活动的专业技术领域选择具备相关能力的审核员和技术专家组成审核组。审核组中的审核员应承担审核责任。

5.2.2.2 技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

5.2.2.3 审核组可以有实习审核员，实习审核员要在审核员的指导下参与审核，不计入审核时间，在审核过程中的活动由审核组中的审核员承担责任。

5.2.3 审核计划

5.2.3.1 ZHCC 应制定书面的审核计划交审核组实施。审核计划至少包括以下内容：审核目的，审核准则，审核范围，现场审核的日期和场所，现场审核持续时间，审核组成员（其中：审核员应标明认证人员注册号；技术专家应标明专业代码、工作单位及专业技术职称）。

5.2.3.2 如果人工智能管理体系覆盖范围包括在多个场所进行相同或相近的活动，且这些场所都处于申请组织授权和控制下，认证机构可以在审核中对这些场所进行抽样，但应根据相关要求实施抽样以确保对所抽样本进行的审核对环境管 理体系包含的所有场所具有代表性。如果不同场所的活动存在明显差异，或不同 场所间存在可能对环境管理有显著影响的区域性因素，则不能采用抽样审核的方 法，应当逐一到各现场进行审核。

对多个相似场所可进行抽样审核，抽样数量不少于按以下方法计算的结果：

①初审：一般样本量应当为场所数量的平方根（$Y=\sqrt{X}$）。

②监督审核：每年度的样本量为场所数量的平方根乘以系数 0.6($Y=0.6\sqrt{X}$)。

③再认证审核：样本数量应与初审相同，如证明管理体系在认证周期中有效，

则样本的数量可最低为 0.8（$Y=0.8\sqrt{X}$）。

注：其中 Y 为抽样的数量，结果向上取整：X 为相似场所的总体数量。5.2.3.4 在审核活动开始前，审核组应将书面审核计划交申请组织确认。遇特殊情况临时变更计划时，应及时将变更情况书面通知受审核的申请组织，并协商一致。

5.3 实施审核

5.3.1 审核组应当全员完成审核计划的全部工作。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员（技术专家和实习审核员除外）。

5.3.2 审核组应当会同申请组织按照程序顺序召开首、末次会议。审核组应当提供首、末次会议签到表，参会人员应签到。申请组织要求时，审核组成员应向申请组织出示身份证明文件。

5.3.3 审核时应采用文件调查和现场调查的方式，包括查阅文件和记录、询问工作人员、观察现场、访问顾客和利益相关方、诚信行为调查等。

5.3.4 审核过程及环节

5.3.4.1 初次认证审核，分为第一、二阶段实施审核。

5.3.4.2 第一阶段审核应至少覆盖以下内容：

（1）结合现场情况，确认申请组织实际情况与管理体系成文信息描述的一致性，特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、生产或服务过程 等是否与申请组织的实际情况相一致；

（2）结合现场情况，审核申请组织有关人员理解和实施标准要求的情况，评价管理体系运行过程中是否实施了内部审核与管理评审，确认管理体系是否已有效运行并且超过3个月；

（3）确认申请组织建立的管理体系覆盖的活动内容和范围、申请组织的员工人数、活动过程和场所，遵守相关法律法规及技术标准的情况；

（4）结合管理体系覆盖活动的特点识别对目标的实现具有重要影响的关键点，并结合其他因素，科学确定重要审核点；

（5）与申请组织讨论确定第二阶段审核安排。

在第一阶段审核中，如发现组织存在违反审核依据的情况， 审核组将以《一阶段问题点清单》指出，不开具《不符合报告》。在《一阶段问题点清单》中问题没有得到有效处理前，不会进行第二阶段审核。现场审核结束前，审核组将与受审核方进行沟通，通报第一阶段审核结论，出具第一阶段《审核报告》。

5.3.4.3 在下列情况，第一阶段审核可以不在申请组织现场进行：

（1）申请组织已获本 ZHCC 颁发的其他管理体系认证证书，ZHCC 已对申请组织 PISMS 有充分了解。

（2）ZHCC 有充足的理由证明申请组织的业务简单，通过对其提交文件和资料的审查可以达

到第一阶段审核的目的和要求。

（3）申请组织获得过其他经认可或备案的认证机构颁发的有效的 PISMS 认证证书，通过对其文件和资料的审查可以达到第一阶段审核的目的和要求。

除以上情况之外，第一阶段审核应在申请组织的生产经营或服务现场进行。

5.3.4.4 审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键因素，要及时提醒申请组织特别关注。

5.3.4.5 第一阶段审核和第二阶段审核应安排适宜的间隔时间，使申请组织有充分的时间解决第一阶段中发现的问题。

5.3.4.6 第二阶段审核应当在申请组织现场进行，重点是审核 PISMS 符合 ISO IEC 27701:2019 标准要求和有效运行情况应至少覆盖以下内容：

（1）在第一阶段审核中识别的重要审核点的监视、测量、报告和评审记录的充分 性和有效性。

（2）为实现总目标而建立的各层级目标是否具体、有针对性、可测量并且可实 现。

（3）对管理体系覆盖的过程和活动的管理及控制情况。

（4）申请组织实际工作记录是否真实。

（5）申请组织的内部审核和管理评审是否有效。

5.3.5 发生一些问题时，审核组应终止审核，并向 ZHCC 审核部报告，等待审核部确认且向认监委办理了终止审核计划后，方可终止审核，离开现场，可终止审核计划的情况包含：

（1）申请组织对审核活动不予配合，审核活动无法进行。

（2）受审核方实际情况与申请材料有重大不一致。

（3）申请组织的 PISMS 有重大缺陷，不符合 ISO IEC 27701:2019 标准的要求。

（4）发现申请组织已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益；

（4）其他导致审核程序无法完成的情况。

5.4 审核报告

5.4.1 审核组应对审核活动形成书面审核报告，由审核组组长签字。审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：

（1）申请组织的名称和地址。

（2）审核的申请组织活动范围和场所。

（3）审核的类型、准则和目的

（4）审核组组长、审核组成员及其个人注册信息。

（5）审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。

（6）叙述从 4.3 条列明的程序及各项要求的审核工作情况，其中：对 4.3.3.6 条的各项审核要求应逐项就审核证据、审核发现和审核结论进行详细描述；对目标和过程控制及要素管理情况进行评价。

（7）识别出的不符合项。不符合项的表述，应基于客观证据和审核依据，用写实的方法准确、具体、清晰描述，易于被申请组织理解。不得用概念化的、不确定的、含糊的语言表述不符合项。

（8）审核组对是否通过认证的意见建议。

5.4.2 审核报告应随附必要的用于证明相关事实的证据或记录，包括文字或照片摄像等音像资料。

5.4.3 ZHCC 应将审核报告提交申请组织，并保留签收或提交的证据。

5.4.4 对终止审核的项目，审核组应将已开展的工作情况形成报告，ZHCC 应将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

5.5 不符合项的纠正和纠正措施及其结果的验证

5.5.1 对审核中发现的不符合项，ZHCC 应要求申请组织分析原因，并要求申请组织在规定期限内采取措施进行纠正。

5.5.2 ZHCC 应对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。

5.6 认证决定

5.6.1 ZHCC 技术部应该在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，作出认证决定。

5.6.2 审核组成员不得参与对审核项目的认证决定。

5.6.3 ZHCC 技术部在作出认证决定前应确认如下情形：

（1）审核报告符合本规则第 4.4 条要求，能够满足作出认证决定所需要的信息。

（2）反映以下问题的不符合项，ZHCC 已评审、接受并验证了纠正和纠正措施及其结果的有效性。

① 未能满足 PISMS 标准的要求。

② 制定的目标不可测量或测量方法不明确。

③ 对实现目标具有重要影响的要素的监视和测量未有效运行，或者对这些要素的报告或评审记录不完整或无效。

④ 其他严重不符合项。

（3）ZHCC 对其他不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

5.6.4 在满足 4.6.3 条要求的基础上，ZHCC 有充分的客观证据证明申请组织满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书。

（1）申请组织的 PISMS 符合标准要求且得到有效实施与保持。

（2）认证范围覆盖的企业活动、产品和服务符合相关法律法规要求。

（3）申请组织按照认证合同规定履行了相关义务。

5.6.5 申请组织不能满足上述要求的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因。

5.6.6 ZHCC 在颁发认证证书后，应当在 30 个工作日内按照规定的要求将相关信息报送国家认监委。国家认监委在其网站（www.cnca.gov.cn）开设专栏向社会公开各 ZHCC 上报的认证证书等信息。

5.6.7 ZHCC 不得将申请组织是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

6.监督审核

6.1 ZHCC 应对持有其颁发的 PISMS 认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织通过认证的 PISMS 持续符合要求。

6.2 为确保达到 5.1 条要求，ZHCC 应根据获证组织的产品或服务的风险程度或其他特性，确定对获证组织的监督审核的频次。

6.2.1 作为最低要求，在初次认证的第二阶段审核后至少 12 个月内应进行一次监督审核。此后，每次监督审核的时间间隔不超过 12 个月。

6.2.2 在达到监督审核期限而有证据表明获证组织暂不具备实施监督审核的条件时，可以适当延长监督审核期限，但最长间隔不能超过 15 个月。

6.2.3 超过期限而未能实施监督审核的，应按 6.6 条款处理。

6.3 监督审核的时间，按照附录 A。

6.4 监督审核的审核组，应符合 5.2.2 条和 5.3.1 条的要求。

6.5 监督审核应在获证组织现场进行，且应满足第 5.2.3.3 条确定的条件。由于生产经营活

动的季节性原因，在每次监督审核时难以覆盖所有生产经营活动的，在认证证书有效期内的监督审核需覆盖认证范围内的所有活动。

6.6 监督审核时至少应审核以下内容：

（1）上次审核以来 PISMS 覆盖的活动及运行体系的资源是否有变更。

（2）已识别的重要关键因素是否按 PISMS 的要求在正常和有效运行。

（3）对上次审核中确定的不符合项采取的纠正和纠正措施是否继续有效。

（4）PISMS 覆盖的活动涉及法律法规规定的，是否持续符合相关规定。

（5）方针、目标是否实现。目标没有实现的，获证组织在内部管理评审时是否及时调查并采取了改进措施。

（6）获证组织对认证标志的使用或对认证资格的引用是否符合相关的规定。

（7）内部审核和管理评审是否规范和有效。

（8）是否及时接受和处理投诉。

（9）针对内审发现的问题或投诉的问题，及时制定并实施了有效的持续改进。

6.7 监督审核的审核报告，应按 6.6 条列明的审核要求逐项描述审核证据、审核发现和审核结论。审核组应提出是否继续保持认证证书的意见建议。

6.8 ZHCC 根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

7.再认证程序

7.1 认证证书期满前，若获证组织申请继续持有认证证书，ZHCC 应当实施再认证审核决定是否延续认证证书。

7.2 ZHCC 应按 5.2.2 条要求组成审核组。按照 5.2.3 条要求并结合历次监督审核情况，制定再认证计划并交审核组实施。审核组按照要求开展再认证审核。

在 PISMS 及获证组织的内部和外部环境无重大变更时，再认证审核可省略第一阶段审核，但审核时间应不少于按 5.2.1 条计算人日数的 2/3。

7.3 对再认证审核中发现的不符合项，应按 5.5 条要求实施纠正和纠正措施并进行验证，验证应在原证书有效期满前完成。

7.4 ZHCC 参照 5.6 条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

7.5 如果在当前认证证书的终止日期前完成了再认证活动并决定换发认证证书，新认证证书的终止日期可以基于当前认证证书的终止日期。新认证证书上的颁证日期应不早于再认证决

定日期。

如果在当前认证证书终止日期前，认证机构未能完成再认证审核或对严重不符合项实施的纠正和纠正措施未能进行验证，则不应予以再认证，也不应延长原认证证书的有效期。

在当前认证证书到期后，如果认证机构能够在 6 个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。认证证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期。

8.认证证书状态管理要求（暂停、撤销、注销、恢复、失效）

8.1 认证机构应制定暂停、撤销认证证书或缩小认证范围的规定和文件化的管理制度，规定和管理制度应满足本规则相关要求。认证机构对认证证书的暂停和撤销处理应符合其管理制度，不得随意暂停或撤销认证证书。执行本机构的《认证授予、拒绝、保持、变更、暂停、恢复、撤销程序》。

8.2 暂停证书

8.2.1 获证组织有以下情形之一的，认证机构应在调查核实后的 5 个工作日内暂停其认证证书。

（1）云服务信息安全管理体系持续或严重不满足认证要求，包括对云服务信息安全管理体系运行有效性要求的。

（2）不承担、履行认证合同约定的责任和义务的。

（3）被有关执法监管部门责令停业整顿的。

（4）持有的与云服务信息安全管理体系范围有关的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证的。

（5）主动请求暂停的。

（6）其他应当暂停认证证书的。

8.2.2 认证证书暂停期不得超过 6 个月。但属于 8.2.1 第（4）项情形的暂停期可至相关单位作出许可决定之日。

8.2.3 认证机构应以适当方式公开暂停认证证书的信息，明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

8.3 撤销证书

8.3.1 获证组织有以下情形之一的，认证机构应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书。

（1）被注销或撤销法律地位证明文件的。

（2）被国家行政机关列入严重失信企业名单。

（3）拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的。

（4）拒绝接受国家监督抽查的。

（5）出现重大的云服务信息安全管理事故，经执法监管部门确认是获证组织违规造成的。

（6）有其他严重违反法律法规行为的。

（7）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的云服务信息安全管理体系范围有关的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）。

（8）没有运行云服务信息安全管理体系或者已不具备运行条件的。

（9）不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者认证机构已要求其纠正但超过 2 个月仍未纠正的。

（10）其他应当撤销认证证书的。

8.3.2 撤销认证证书后，认证机构应及时收回撤销的认证证书。若无法收回，认证机构应及时在相关媒体和网站上公布或声明撤销决定。

8.4 认证机构暂停或撤销认证证书应当在其网站上公布相关信息，同时按规定程序和要求报国家认监委。

8.5 认证机构应采取有效措施避免各类无效的认证证书和认证标志被继续使用。

8.6 注销认证证书

获证组织主动申请不再保持认证资格时，本机构会注销其认证资格，并保留 相应证据。在机构与客户沟通确认后，向获证客户发送注销通知，要求停止认证 证书、认证标志使用和一切宣传活动，并要求获证客户立即寄回认证证书。同时，注销信息上网公示。

8.7 认证证书的恢复

8.7.1 证书恢复的条件

获证客户对存在问题采取整改措施并在规定的时限内，解决了造成暂停的问题，认证资格的恢复符合相关的认证要求，同时在暂停期内没有使用、引用认证证书（如广告宣传）和使用认证标志。

8.7.2 证书恢复的程序

获证客户在规定时限内解决了造成暂停的问题后，向公司提出恢复使用认证证书申请并提供证明资料，可分两种情况：一种可立即办理恢复手续，经确认后 办理恢复手续；另一种要经现场评审确认后办理恢复手续，根据暂停的原因，经 评定后做出证书恢复／现场评审确认的评定意见确认后办理恢复手续。

8.7.3 在机构确认原因消除后，按流程进行恢复，机构将恢复信息上网公示，并向获证客户发送恢复通知，通知获证客户恢复认证证书和认证标志使用和宣传。

8.8 证书失效

8.8.1 认证证书有效期为三年，到期自动失效；

8.8.2 认证标准发生变更时，旧版使用期限到期，证书自动失效；

8.8.3 证书失效不需要向客户发送失效通知书。

9.认证证书要求

9.1 认证证书应至少包含以下信息：

（1）获证组织名称、地址和组织机构代码。该信息应与其法律地位证明文件的信息一致。

（2）PISMS 覆盖的生产经营或服务的地址和业务范围。若认证的 PISMS 覆盖多场所，表述覆盖的相关场所的名称和地址信息，该信息应与相应的法律地位证明文件信息一致。

（3）PISMS 符合 ISO IEC 27701:2019 标准的表述。

（4）证书编号。

（5）ZHCC 名称。

（6）证书签发日期及有效期的起止年月日。

对初次认证以来未中断过的再认证证书，可表述该获证组织初次获得认证证书的年月日。

（7）相关的认可标识及认可注册号（适用时）。

（8）证书查询方式。ZHCC 除公布认证证书在 ZHCC 网站上的查询方式外，还应当在证书上注明：“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询”，以便于社会监督。

9.2 认证证书有效期最长为 3 年。

9.3 ZHCC 应当建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

10.与其他管理体系的结合审核

10.1 当申请组织在运行隐私信息管理体系的同时还运行了其他管理体系，若其他管理体系在

中鸿认证的认证业务范围内，中鸿认证可以根据申请组织的需求对管理体系进行单独的审核，或者对多个管理体系进行结合审核，但中鸿认证需确保在结合审核的情形下，对诸如审核范围的界定、审核时间的确定、审核方案的策划等进行有效地管理。

10.2 对于结合审核，必须以审核活动满足体系认证所有要求为前提，并且审核的质量不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与管理体系有关的重要因素的描述并易于识别。

11.受理转换认证证书

11.1 认证机构应当履行社会责任，严禁以牟利为目的受理不符合 ISO IEC 27701:2019 标准、不能有效执行 PISMS 的组织申请认证证书的转换。

11.2 认证机构受理组织申请转换为本机构的认证证书，应该详细了解申请转换的原因，必要时进行现场审核。

11.3 转换仅限于现行有效认证证书。被暂停或正在接受暂停、撤销处理的认证证书以及已失效的认证证书，不得接受转换申请。

12.证书的更换

获证组织需更改获准认证/注册的企业隐私信息管理体系时，应及时将更改情况报本公司市场部。 在管理体系认证证书有效期内，当证书覆盖的范围、认证依据的标准、证书持有者、注册地址等发生变更时，应重新换证。

13.受理组织的申诉

13.1 申请组织或获证组织对认证决定有异议时，认证机构应接受申诉并及时进行处理，在 60 日内将处理结果形成书面通知送交申诉人。

13.2 书面通知应当告知申诉人，若认为认证机构未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。

14.认证记录的管理

14.1 认证机构应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

14.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文，保存时间至少应当与认证证书有效期一致。

15.其他

15.1 本规则内容提及 ISO IEC 27701:2019 标准时均指认证活动发生时该标准的有效版本。

认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。

附录 A：隐私信息管理体系认证审核时间要求

下表为PISMS初次认证的审核人日基数，具体审核时间需要考虑受审核方的规模、特性、业务复杂程度、PISMS涵盖的范围、认证要求和其承担的风险等因素。根据受审核方的特点在项目方案制定过程中可以在人日基数上进行增减。

审核人日包括一阶段审核、现场审核、现场见证以及报告编写的时间。

当PISMS与其他管理体系结合审核时，PISMS的审核时间可根据结合审核的其他管理体系的特点进行减少。

监督审核的人日数为初次认证人日数的三分之一，再认证的人日数为初次认证人日数的三分之二，上述原则仅限于获证组织的认证范围和组织规模未发生变化的情况。

ISMS审核时间表

在组织控制下工作的人员的数量	ISMS初次审核时间	在组织控制下工作的人员的数量	ISMS初次审核时间
1～10	5	626～875	17.5
11～15	6	876～1175	18.5
16～25	7	1176～1550	19.5
26～45	8.5	1551～2025	21
46～65	10	2026～2675	22
66～85	11	2676～3450	23
86～125	12	3451～4350	24
126～175	13	4351～5450	25
176～275	14	5451～6800	26
276～425	15	6801～8500	27
426～625	16.5	8501～10700	28
		>10700	沿用以上规律

注：

1.有效人数，包括认证范围内涉及的所有全职人员，原则上以组织的社会保险登记证所附名册等信息为准。

2.对非固定人员（包括季节性人员、临时人员和分包商人员）和兼职人员的有效人数核定，可根据其实际工作小时数予以适当减少或换算成等效的全职人员数。

3.组织正常工作期间（如轮班制组织）安排的审核时间可以计入有效的管理体系认证审核时间，但往返多审核场所之间所花费的时间不计入有效的管理体系认证审核时间。

4.隐私信息管理体系监督审核的人日数为初次认证人日数的 1/3（不得少于1人日），再认证的人日数为初次认证审核人日数的2/3。

修订记录

发布日期	实施日期	版本	修订内容概要	拟制	审核	批准
2023.4.12	2023.4.12	A/0	新版发行	韩自鹤	张凯	张凯
2025.06.15	2025.06.15	C/0	增加证书更换、认证资格变更内容	技术部	韩自鹤	丁泽林
2025.8.25	2025.8.25	C/1	依据《国家认监委关于加强认证规则管理的公告2025年第9号》进行修订	技术部	韩自鹤	丁泽林

中鸿认证（江苏）有限公司

编号：ZHCC-P11-C1

认证授予、拒绝、保持、变更、暂停、恢复、撤销程序

修 订 记 录

发布日期	实施日期	版本	修订内容概要	拟制	审核	批准
2025.3.15	2025.4.1	C/1	内部变更，更新文件版本	技术部	韩自鹤	丁泽林

1 目的

旨在保证中鸿认证（ZHCC）授予、拒绝、保持、变更、暂停、恢复、撤销认证注册资格的工作符合规定要求以及签发的证书能正确使用。

2 适用范围

对 ZHCC 所颁发证书的授予、拒绝、保持、变更、暂停、恢复、撤销的管理。

3 职责和权限

3.1 技术部负责证书的授予、拒绝、保持，扩大、缩小、暂停及撤销决定的协调管理；

3.2 总经理负责对证书的授予、拒绝、保持，扩大、缩小、暂停及撤销的确认；

3.3 市场部负责证书以及暂停、恢复和撤销通知书的发放。

4 程序

4.1 管理体系认证证书的授予

4.1.1 申请认证的组织在中鸿认证对其实施了必需的评审后，符合以下条件，中鸿认证将作出批准注册的决定。

(1) 组织的管理体系健全，符合所选定标准的要求，执行情况良好；有合法的法律地位；产品的实物质量符合相关规定的要求。

(2) 组织实施了有效的内审和管理评审，体系运行有效，且予以保持。

(3) 对所有反映以下问题的不符合，ZHCC 已评审、接受并证实了纠正和纠正措施的有效性：

① 未能满足管理体系标准的一项或多项要求；或

② 使人对客户管理体系实现预期结果的能力产生重大怀疑的情况；

(4) 对于任何其他不符合，ZHCC 在公司规定的期限内已评审并接受了客户计划采取的纠正和纠正措施。

(5) 支付所有的认证费用；

4.1.2 收到审核部上报的审核材料后，技术部经理根据管理层批准的认证决定人员清单协调人员按《认证评定表》要求对上报审核档案以及审核以外得到的信息，如投诉、市场反馈等进行评定，参与评定的人员必须为非审核人员，认证决定人员作出认证决定后交技术部，技术部对认证决定过程进行再次确认无误后，由技术部报总经理。

4.1.3 总经理确认后，由技术部制作证书中英文各一份，证书发放前需经总经理批准。

4.2 认证的拒绝

4.2.1 当认证条件或认证结果不符合本文 4.1 的要求时，ZHCC 将拒绝授予认证。

在拒绝授予认证前，如因不符合整改超过规定的期限导致无法完成认证授予，则由技术部发《不符合整改跟踪通知书》给市场部，由市场部负责与客户沟通。

如沟通后仍未在规定的期限内完成则由技术部发《审议不通过通知书》给市场部，市场部通知客户后，技术部在 ERP 系统上进行不予注册的认证决定。

4.2.2 当受理时拒绝认证后，由审核部合同评审人员将拒绝认证的理由及相关信息传递给市场业务人员，由业务人员通知认证申请方。

4.2.3 当认证决定拒绝认证时，由技术部认证决定人员将拒绝认证的理由及相关信息传递给市场业务人员，由业务人员通知认证申请方。

4.3 认证证书的保持

4.3.1 证书保持条件：

(1) 获证方在认证证书有效期内按期接受监督审核；

(2) 管理体系有效保持，管理无重大变更；

(3) 对现场审核中出现的不合格项能够按要求整改且纠正措施实施有效；

(4) 对现场检查中出现的不合格项能够按要求整改且纠正措施实施有效；

(5) 在认证证书有效期内如有认证要求变更，ZHCC 将变更要求以公开文件及其他方式通报获证组织执行，并经 ZHCC 验证在认证范围内相关产品满足变更的要求；

(6) 需要换发证书情况下，经必要的审核和认证决定小组对相关材料进行审定，认为获证（申请）组织在认证范围内能满足保持认证资格的条件，经 ZHCC 总经理批准换发认证证书；

(7) 没有重大投诉；

(8) 没有重大产品事故；

(9) 没有严重违法违纪行为；

(10) 按时支付审核费用。

4.3.2 技术部收到审核部的监督审核的审核报告后，根据《认证决定审批表》进行评审。

4.3.3 如果发现获证组织发生了与 OHS 有关的严重事件，如严重事故或严重违法，实施独立于监管机构的特殊审核是必要的，以便调查管理体系是否存在严重问题以及是否有效发挥作用；此时应记录调查的结果。

4.4 认证证书范围的变更（扩大或缩小）

4.4.1 当获证组织要求变更（扩大）认证范围时，审核部应对扩大认证范围的申请进行评审，

并确定任何必要的审核活动，以做出是否可予扩大的决定。

这种变更包括（但不限于）与下列方面有关的变更：

(1) 法律地位、经营状况、组织状态或所有权；

(2) 组织和管理层（如关键的管理、决策或技术人员）；

(3) 联系地址和场所；

(4) 获证管理体系覆盖的范围，能源管理体系还包括能源核算边界的变化；

(5) 管理体系和过程的重大变更。

4.4.2 此时，获证组织需提交更改的管理体系文件、数据信息和工商证明文件（必要时），适用时还需提交相应许可证书。

4.4.3 合同评审人员按照认证管理程序要求，对变更部分的申请进行评审。

4.4.4 审核部按各认证管理程序要求对其现场进行审核（可结合监督审核或再认证进行），并将审核结果报技术部。

4.4.5 ZHCC 以公开文件的方式要求获证组织向 ZHCC 通报管理体系变更，以及其他可能影响其符合性的变更。

4.4.6 如果获证组织在认证范围的某些部分持续地或严重地不满足认证要求，ZHCC 将缩小其认证范围，以排除不满足要求的部分。认证范围的缩小应与认证标准的要求一致。

4.4.7 技术部根据《认证决定审批表》中相关的项目进行评定，作出决定后交总经理，总经理确认后由技术部制作证书，给予换发，并及时修改相关客户认证信息。

4.5 认证证书的暂停

不能持续符合认证要求的，中鸿认证应当在确认相关情况后 5 日内，暂停认证对象相应的认证证书。暂停期限届满仍不符合要求的，应当撤销其相应认证证书。

4.5.1 出现下列情况之一会导致证书的暂停：

a) 由于质量、环境、职业健康安全管理体系发生重大变更而导致原有认证失效；

b) 客户的获证管理体系持续地或严重地不满足认证要求（包括有效性）。

c) 监督审核发现严重不符合项，且未在规定时间内进行有效整改；

d) 获证产品持续地或严重地不满足认证要求（包括有效性）。

e) 认证证书所涉及的产品质量监督抽查发现重大不合格的；

f) 未按规定使用认证证书和认证标志，且在规定的时间内未进行有效整改；

g) 发生影响质量、环境、职业健康安全管理体系的重大事故的；

h) 发生重大质量、环境污染、职业健康安全事故，但未造成严重后果者；

i) 未按照 ZHCC 规定的时限进行监督审核；

j) 不承担、履行认证合同约定的责任和义务的。如未按期交纳认证费用且经指出后仍未交纳的；

k) 被有关执法监管部门责令停业整顿的。

l) 持有的与质量管理体系范围有关的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证的。

m) 获证客户主动请求暂停。

n) 特殊行业，在特定时期国家有要求予以暂停的，证明材料须附国家有关要求的文件；

4.5.2 审核部发现 4.5.1a-n 的现象后，应在审核报告中说明，市场部发现上述 i-n 的现象后，应通知技术部，由技术部协调认证决定人员进行认证决定并予以记录，由技术部向客户发出证书暂停通知。

对于超过证书签发日期 12 个月还未进行第一次年度审核，或超过上次审核完成日 12 个月（特殊情况下间隔可延长但不能超过 15 个月且不能跨越公历年份）还未进行后一次年度审核（含再认证）的客户，市场部人员应向技术部提交名单，由技术部作出暂停决定，报技术经理或总经理。由技术部制作《管理体系认证证书暂停通知书》，在该客户的审核档案中备案，更新客户数据库中做相应标识，并将《管理体系认证证书暂停通知书》抄送市场部，由市场部安排人员负责通知客户、跟踪；市场部负责更新客户总表。在这个期限之前，市场部人员应提前及时通知客户不能按时进行年度审核的后果。

认证证书暂停期一般为 3 至 6 个月（最长不应超过 6 个月），应在该期限内采取措施消除引起暂停的原因。如果获证组织未能在规定的时限内解决造成暂停的问题，ZHCC 应撤销或缩小其认证范围。如果客户持有的行政许可证明已经过期或失效，但已重新提交相应的行政许可申请且申请已被相应的行政许可机关受理的，暂停期可至行政许可机关作出行政许可决定之日。

4.5.3 市场部负责监督审核安排的人员负责对由于未能按时进行年审而暂停的客户的跟踪；技术部、市场部对由于其他原因而暂停的客户的纠正情况进行跟踪。如认证证书暂停的 6 个月内没有采取有效措施，年度审核安排人员和市场部应通知技术部，由技术部制作《管理体系认证证书撤销通知书》、在审核档案中备案、更新客户数据库，并将《管理体系认证证书撤销通知书》抄送市场部，由市场部通知客户、跟踪，更新客户信息总表。

4.5.4 在暂停期限内，如客户对导致暂停的原因采取了有效措施，经相关部门确认，技术部复核并报总经理批准后，方可恢复其认证证书。

4.5.5 由获证客户提供的，或在特殊审核期间，审核组直接收集的有关导致监管机构参与（调查）的事件信息，如严重事故或严重违法（行为）， 应为 ZHCC 提供决定采取措施的理由，包括，一旦证明体系严重地不能满足管理体系认证要求而采取的暂停或撤销认证的措施。这些要求应是 ZHCC 和组织签署的合同协议的一部分。

4.6 认证资格的恢复

4.6.1 恢复认证资格的条件：

获证组织提供的证明材料表明，已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，重新符合了相关的认证要求，包括：

(1) 受审核方未在规定的时限内接受监督审核被暂停的，需附重新安排的监督审核计划和监督审核报告；

(2) 发生重大事故被暂停的，需附组织事故调查分析报告（自身的和国家有关部门的）以及 ZHCC 就该事故进行追踪审核的审核报告，可表明其纠正及纠正措施充分有效；

(3) 因投诉被暂停的，需提交组织针对投诉原因采取的纠正措施及验证材料；

(4) 因未交纳审核费用被暂停的，需附交费证明（如汇款凭证复印件）

(5) 其他针对暂停证书原因提交的纠正材料或证明性文件。

4.6.2 可恢复认证资格的组织，经评审通过，技术部复核并报总经理批准后，方可恢复其认证证书。技术部应更新获证组织数据库并抄送市场部，市场部负责更新获证组织信息总表。

4.7 认证证书的撤销/终止注销

4.7.1 客户的全部或部分产品/服务出现下列情况，将导致证书的撤销/终止（注销）或证书的认证范围的缩小：

(1) 客户主动提出申请终止（注销））；

(2) 客户被终止（注销）或撤销法律地位证明文件；

(3) 客户被国家质量监督检验检疫总局列入质量信用严重失信企业名单；

(4) 拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息；

(5) 拒绝接受国家产品质量监督抽查的；

(6) 出现重大的产品和服务等质量安全事故，经执法监管部门确认是获证组织违规造成的；

(7) 暂停期限内未能对引起暂停的原因采取有效的纠正措施；

(8) 暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的与质量管理体系范围有关的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）；

(9) 不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者认证机构已要求其纠正但超过 2 个月仍未纠正的；

(10) 严重违反法律法规；

(11) 管理体系发生重大变更且在暂停期间未能采取有效纠正措施，经评审其管理体系不符合要求；

4.7.2 发生上述情况之一时，由技术部向客户发出《管理体系认证证书撤销通知书》，通知中应明确要求客户将认证证书交回并不可在任何商业活动中使用证书或其复印件进行宣传活动，并通知客户如未按通知规定的有关要求执行，将采取必要的法律手段。同时技术部应负责将撤销状态予以公告，并将证书被撤销的客户从中鸿认证客户名录中删除。对于部分产品/服务持续或严重地不满足认证要求，则应撤销原证书后，换发缩小认证范围的证书。

4.7.3 撤销认证证书后，ZHCC 将通知企业及时收回撤销的认证证书，并及时在相关媒体和网站上公布或声明撤销决定。

4.7.4 如果终止（应客户要求）认证，ZHCC 认证将根据与客户方达成的协议，形成《管理体系认证证书注销通知书》，发放给客户方，并同时声明所有相关的认证已不再保持。ZHCC 还会对已授予客户方的正式认证文件、公布的信息、标志使用的授权等做出所有必要的更改，以确保没有任何信息显示该产品仍持续获得认证。

4.7.5 凡被暂停、撤销、终止（注销）认证证书及认证证书到期而未申请复审的组织，在作出相应认证决定后的两个工作日内报告认证监管机构。

5 记录

5.1 认证评定表

5.2 认证决定审批表

5.3 不符合整改跟踪通知书

5.4 审议不通过通知书

5.5 管理体系认证证书暂停通知书

5.6 管理体系认证证书撤销通知书

5.7 管理体系认证证书注销通知书

6 附录

无 None

7 引用文件

7.1 CNAS-CC01_2015 《管理体系认证机构要求》