受　控

个人可识别信息保护管理体系认证实施规则

编　号：HNXH/PIIPMS-01-K/01

版　本：A1

编　制：技术部

修　订：技术部

审　核：

批　准：

2024年05月27日**发布**　　2024年05月27日**实施**

2026年04月27日**修改**

北京华诺信和认证有限公司

目 录

个人可识别信息保护管理体系认证实施规则

1 适用范围

1.1 本规则用于规范北京华诺信和认证有限公司（以下简称 HNXH）依据 GB/T 22080-2025/ISO/IEC 27001：2022《网络安全技术 信息安全管理体系 要求》及 ISO 29151：2017《信息技术、安全技术—个人可识别信息保护实践指南》（PIIPMS）标准在中国境内开展的认个人可识别信息保护管理体系认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准，个人可识别信息保护管理体系认证实施过程作出具体规定，明确认证机构对认证过程的管理责任，保证个人可识别信息保护管理体系认证活动的规范有效。

2 认证依据

GB/T 22080-2025/ISO/IEC 27001：2022《网络安全技术 信息安全管理体系 要求》

ISO 29151：2017《信息技术、安全技术—个人可识别信息保护实践指南》

3 对认证机构的基本要求

3.1 获得国家认证认可监督管理委员会（以下简称国家认监委）批准、取得管理体系认证资质。遵守国家认监委备案管理、取得个人可识别信息保护管理体系认证资格。

3.2 开展个人可识别信息保护管理体系认证活动，应当围绕国家经济和社会发展目标，重点服务于经济社会高质量发展，不得影响国家安全和社会公共利益，不得违背社会公序良俗。

3.3 认证能力、内部管理和认证活动符合 GB/T27021《合格评定管理体系审核认证机构要求 第 1 部分：要求》，确保持续满足开展 PIIPMS 认证的基本要求。

3.4 建立风险防范机制，对从事个人可识别信息保护管理体系认证活动可能引发的风险和责任采取合理有效措施。

3.5 对认证活动中所知悉的国家秘密、商业秘密负有保密义务。应通过在法律上具有强制实施力的协议，确保认证活动中所获得的信息在未经申请组织书面同意的情况下，不向第三方透漏，认证行政监管有要求的除外。

3.6 应对 PIIPMS 认证活动的真实性、有效性负责，加强认证人员的管理及素质、能力提升，合理安排审核员的工作量。每个审核员参加包括管理体系现场审核时间的总和不应超过 180 天/周期年。

3.7 HNXH 拥有的管理体系有效认证证书的数量应与该机构管理体系审核员数量相匹配，人均每个审核员匹配的管理体系有效认证证书总数不应超过 50 张/周期年。

3.8 不得委派未取得管理体系注册资格的审核员开展个人可识别信息保护管理体系认证审核活动。

3.9 不得以“认证证书在国家认监委网站可查”或近似表述进行广告宣传。

3.10 不得将认证委托人（以下简称申请组织）是否获得认证和参与认证审核的审核员及其他人员的薪酬挂钩。

4 对认证人员的基本要求

4.1 审核员为 HNXH 内部注册资格，不设实习资格，具有 CCAA 注册管理体系正式审核员资格，经培训后，方可注册成为个人可识别信息保护管理体系审核员，具有管理体系实习审核员注册资格
不能注册成为个人可识别信息保护管理体系审核员。

4.2 认证审核员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

4.3 认证审核员还应具有个人可识别信息保护管理体系相关知识和技能。

PIIPMS 审核员应经培训具备以下知识和技能：

4.3.1 个人可识别信息保护管理体系知识

理解 GB/T 22080-2025/ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》及 ISO 29151:2017《信息技术、安全技术—个人可识别信息保护实践指南》的术语及各条款的内容和要求；

a） 理解个人可识别信息保护管理体系在不同类型组织中的应用，包括：

- 不同类型组织的个人可识别信息保护管理体系的范围和组织环境；
- 不同类型组织的网络空间安全对资源的要求；
- 不同类型组织网络空间安全的策划、支持、运行、绩效评估和改进过程；
- 不同类型组织网络空间安全风险和组织业务的关系；
- 不同类型组织特定的管理过程。

4.3.2 网络空间安全基础知识

a） 理解网络空间安全术语、定义、类型和特点；

b） 理解网络空间安全相关的基础知识，包括：

- 网络空间安全议题：包括组织治理、人权、劳工实践、环境、消费者问题、公平运行实践、参与和发展网络空间安全的社会期望，包括但不限于对员工、消费者、相关方、社区、社会带来的影响；

✹网络空间安全风险评估方法、周期、应对措施的实施；

✹网络空间安全相关内容、运行和持续改进的应用。

4.3.3 法律法规知识

c） 了解网络空间安全相关的法律法规、实施细则、工作规程和指南等要求及其与个人可识别信息保护管理体系的关系，了解其在审核中的应用；

d） 了解组织应遵守的其他管理要求。

4.4 认证决定人员

PIIPMS 认证决定人员应具备不低于 PIIPMS 审核员的知识和能力要求，并评价授权。基于认证决定人员授权评价结果，授予 PIIPMS 审核员的认证决定人员资格和范围。审核部参照相关规定对 PIIPMS 认证决定人员进行工作表现的持续评价。

4.5 其他各类认证人员

具备 HNXH 任一管理体系申请评审/审核方案/认证决定管理人员/人员能力评价人员资格授权的，经 PIIPMS 标准和认证规则培训合格，了解 PIIPMS 标准、相关法规，并熟悉掌握 HNXH 认证管理要求的，由审核部授予其 PIIPMS 相应的资格授权。

审核部按照要求，对 PIIPMS 申请评审/审核方案/认证决定管理人员/人员能力评价人员进行工作表现的评价持续评价。

5 认证程序

5.1 认证申请

5.1.1 应向申请组织至少公开以下信息：

（1）可开展的认证业务范围，以及分包境外认证机构业务的情况；

开展个人可识别信息保护管理体系认证活动所依据 GB/T 22080-2025/ISO/IEC27001：2022 及 ISO 29151：2017 标准以及相关的认证方案、认证流程；

（2）授予、拒绝、保持、更新、暂停（恢复）、注销、撤销认证证书以及扩大或缩小认证范围的程序规定；

（3）拟向申请组织获取的信息以及保密规定；

（4）认证收费标准，认证费用由申请组织向 HNXH 直接支付；

（5）认证证书、认证标志及相关的使用规定；

（6）对认证过程和结果的申诉、投诉规定；

（7）认证标准换版的规定（适用时）；

（8）“提前较短时间通知的审核”的情形；

（9）其他需要公开的信息。

5.1.2 提出认证申请时，申请组织应具备以下条件：

（1）取得合法主体资格，并处于有效期内；

（2）取得相关法律法规规定的行政许可（适用时），并处于有效期内；

（3）已按认证标准建立个人可识别信息保护管理体系，且运行满三个月；

（4）因获证组织自身原因被原发证机构暂停或撤销认证证书已满一年（适用时）；

（5）原管理体系认证证书发证机构被国家认监委撤销管理体系认证资质已满三个月（适用时）；

（6）当前未被行政监管部门责令停产停业整顿；

（7）当前未列入“国家企业信用信息公示系统”和“信用中国”发布的严重违法失信名单；

（8）一年内未发生被行政监管部门责令停产停业整顿的重大质量事故；

（9）一年内申请认证范围内的网络空间安全未发生国家监督抽查不合格，或发生国家监督抽查不合格但已按相关规定整改合格；

（10）其他应具备的条件。

5.1.3 申请组织提供以下信息和文件资料：

（1）认证申请，包括申请组织的名称、地址、认证依据的标准、申请的认证范围、认证范围内人员数量及影响体系有效性的外包过程；

（2）法律地位的证明文件，当个人可识别信息保护管理体系覆盖多个法律实体时，应提供每个法律实体的法律地位证明文件；

（3）申请认证范围所涉及的网络空间安全法律法规要求的行政许可文件、资质证书、强制性产品认证证书等；

（4）组织机构及职责；

（5）生产/服务的流程、班次及轮班情况和季节性信息；

（6）个人可识别信息保护管理体系运行满三个月的证据；

（7）一年内所发生的网络空间安全事故、与网络空间安全相关的行政处罚、国家监督抽查不合格、其他抽查不合格的情况以及整改情况（适用时）；

（8）其他需要提供的文件。

5.2 申请评审

5.2.1 HNXH 应按照相应评审程序，对申请组织提交的申请信息和文件资料实施申请评审，仔细鉴别申请信息和文件资料的真伪，确定是否受理认证申请，并保存相应评审记录。

5.2.2 满足以下条件的，本机构可以受理认证申请：

（1）申请组织已具备受理条件（见 5.1.2）；