关于《信息安全管理体系认证规则》要求的客户告知函

尊敬的认证组织及相关方:

根据国家认证认可监督管理委员会（CNCA）发布的《信息安全管理体系认证规则》（CNCA-ISMS-01:2026，以下简称“规则”），《规则》将于 2026 年 3 月 1 日起正式实施。为帮助认证组织理解新版规则，满足相关要求，北京中鼎乾元认证有限公司(简称“ZDQY”)将认证规则中对认证委托人/获证组织的相关要求进行整理并公告如下(具体要求请阅读各信息安全管理体系认证规则及释义原文，详见附件):

一、认证委托人应具备条件

认证申请

提出认证申请时，认证委托人应满足以下基本条件：

根据新版规则 5.1.2 条款规定，

（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 ISMS，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、注销或撤销 ISMS 认证证书已满一年（适用时）；

（5）原 ISMS 认证证书发证机构被国家认监委撤销 ISMS 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）一年内未发生重大及以上级别的网络安全事件；

注：网络安全事件级别依据 GB/T20986 判定。

（9）其他应具备的条件。

二、认证委托人应提供信息和文件资料及评审要求

1、根据新版规则 5.1.3 条款规定，认证机构应要求认证委托人提供以下信息和文件资料：

（1）认证申请，包括认证委托人的名称、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 ISMS 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安全法律法规要求的行政许可文件、资质证书等（适用时）；

（4）组织机构及职责；

（5）生产/服务的流程、班次及轮班情况；

（6）ISMS 运行满三个月的证据；

（7）一年内所发生的与网络安全相关的行政处罚以及整改情况（适用时）；

（8）其他需要提供的文件。

2、根据新版规则 5.2.3 条款规定，对于新的认证委托人，仅在同时满足下列情况的前提下，认证机构可实施认证转换，否则应按照初次认证开展认证活动：

（1）认证机构具有认证委托人申请认证的 ISMS 认证范围的认可资格；

（2）认证委托人持有其他被认可的认证机构（原认证机构）颁发的带认可标识的 ISMS 认证证书（原认证证书）；

（3）原认证证书处于有效期内，未被原认证机构实施暂停或撤销；

（4）原认证机构认证业务正常运行，不存在认可资格到期、被暂停或撤销的问题；

（5）认证机构应获得认证委托人初次认证审核报告或最近一次的再认证审核报告、监督审核报告、审核中发现的不符合及其纠正措施。

三、认证合同签署及认证费用支付

根据新版规则 5.3.1 条款规定，每个认证委托人应与 ZDQY 签订具有法律效力的认证合同，明确认证服务的费用、付费方式和违约条款，以及认证委托人、认证机构和获证组织的责任。认证费用应由认证委托人向认证机构 ZDQY 直接支付。证委托人的上级单位(如所属的集团公司、事业单位、社会团体或机关)或下级单位向 ZDQY 支付费用是可接受的形式。

四、审核过程的配合及实施

1、审核现场

根据新版规则 5.4.1、5.4.3、5.4.5 条款规定，审核现场应按 ZDQY 对认证委托人审核方案策划要求覆盖认证范围内典型过程/活动、产品/服务、班次、多场所现场。认证委托人应提前确认审核计划，确保审核现场处于生产/服务正常运行状态。

2、审核时间

根据新版规则 5.4.2 条款规定，审核时间以人日计，1 人日为 8 小时，不应通过增加工作日的工作小时数以减少审核人日数。如果认证委托人工作日的实际工作时间不足 8 小时，则应延长现场审核天数以满足审核时间要求。

3、首末次会议

根据新版规则 5.5.3 条款规定，审核组应会同认证委托人召开首、末次会议，认证委托人的最高管理者、ISMS 相关职能部门负责人应参加首、末次会议，认证机构应保留首末次会议签到记录、图片/音像证明材料。认证委托人的最高管理者不能参加首、末次会议的，应由获得书面授权的其他高级管理层成员参会，审核组应记录最高管理者缺席理由。

4、面对面访谈

根据新版规则 5.5.4/5 条款规定，审核组应通过面对面访谈等形式，对认证委托人的最高管理者在 ISMS 中发挥领导作用的情况进行重点审核，并保留现场图片/音像、审核记录等证明材料。最高管理者不熟悉组织自身的信息安全方针、信息安全目标，未亲自参与并推动 ISMS 实施的，认证审核应不予通过。

5、终止审核

根据新版规则 5.5.5 条款规定，发生下列情况的，审核组应向认证机构报告后终止审核：

（1）认证委托人对审核活动不予配合，审核活动无法进行；

（2）认证委托人的最高管理者或经授权的高级管理层成员缺席首、末次会议；

（3）认证委托人实际情况与申请材料有重大不一致；

（4）其他导致审核程序无法完成的情况。

6、不符合项及其验证

根据新版规则 5.10.4 条款规定，认证委托人应在规定的时限内按要求完成不符合项整改并通过审核组长验证，如未完成，ZDQY 不作出授予认证、保持认证或更新认证的决定。

根据新版规则 5.10.3 条款规定：严重不符合的验证时限应满足以下要求：

（1）初次认证：在第二阶段审核结束之日起 6 个月内完成；

（2）监督审核：在审核结束之日起 3 个月内完成；

（3）再认证：在原认证证书到期前完成。

五、审核时间间隔及时限

1、初次认证审核:根据新版规则 5.6.1 条款规定，初次认证审核应分为两个阶段实施:第一阶段审核和第二阶段审核。两个阶段审核时间间隔最短不少于 5 日，最长不超过 6 个月。如需要更长的时间间隔，应重新实施第一阶段审核。

2、监督审核:根据新版规则 5.4.1.4 条款规定，初次认证及再认证后的第一次监督审核应在认证证书签发之日起 12 个月内进行，第二次监督审核应在认证证书签发之日起 24 个月内进行，两次监督审核的时间间隔不应超过 12 个月。除再认证的年份外，监督审核每个日历年需要进行一次。

3、再认证审核:根据新版规则 5.8.2、5.10.3/4 条款规定，再认证审核应在获证组织现场进行，并应在认证证书到期前完成。再认证审核时间距离上一次监督审核不应超过 12 个月，否则应暂停认证证书。如有严重不符合，纠正和纠正措施的验证也应在原认证证书到期前完成，否则将不能授予再认证注册资格。只能通过重新进行初次认证审核获得认证证书。

4、提前较短时间通知的审核:根据新版规则 5.9.2 条款规定，为调查投诉，对变更作出回应或对被暂停的客户进行追踪，可能需要在提前较短时间或不通知获证组织的情况下进行审核，此时：

（1）认证机构应说明并使获证组织提前了解将在何种条件下进行此类审核；

（2）由于获证组织缺乏对审核组成员的任命表示反对的机会，认证机构应在指派审核组时给予更多的关注。

六、认证证书和认证标志

根据新版规则 6.1.2 条款规定：获证组织可以在认证证书有效时使用 ISMS 认证证书和认证标志，并接受认证机构的监督管理。认证证书处于暂停期间、被撤销或注销后，不得继续使用认证证书和认证标志。

根据新版规则 6.1.3 条款规定：获证组织应当在广告等有关宣传中正确使用 ISMS 认证标志，不得在产品上仅标注 ISMS 认证标志，只有在注明获证组织通过 ISMS 认证及认证机构名称的情况下，方可在产品包装上标注 ISMS 认证标志。

七.认证证书的暂停、撤销和注销

1、认证证书的暂停:

根据新版规则 7.2 条款规定，获证组织有以下情形之一的，ZDQY 在调查核实后 5 日内暂停其认证证书，并保留相应证据：

（1）ISMS 持续或严重不满足认证要求的，包括 ISMS 文件与实际业务运作严重脱离；

（2）不满足 ISMS 适用的法律法规要求，且未采取有效纠正措施的；

（3）受到与网络安全相关的行政处罚，且尚未完成整改的；

（4）发生重大及以上级别网络安全事件，反映获证组织 ISMS 运行存在重大缺陷的；

（5）拒绝配合市场监管部门的认证执法监督检查，或者提供虚假材料或信息的；

（6）持有的与 ISMS 认证范围有关的行政许可文件、资质证书等过期失效的；

（7）不能按照规定的时间间隔接受监督审核的；

（8）未按相关规定正确引用和宣传获得的认证证书和有关信息，包括认证证书和认证标志的使用；

（9）不承担、履行认证合同约定的责任和义务的；

（10）被有关行政监管部门责令停产停业整顿的；

（11）发生与网络安全相关重大舆情的；

（12）主动请求暂停的；

（13）监督审核时发现的严重不符合的纠正措施未能在 3 个月内完成验证的；

（14）其他应暂停认证证书的。

2、认证证书的撤销：

根据新版规则 7.3 条款规定，获证组织有以下情形之一的，ZDQY 在获得相关信息并调查核实后 5 日内撤销其认证证书，并保留相应证据：

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 日内撤销其认证证书，并保留相应证据：

（1）被注销或撤销法律地位证明文件的；

（2）被“国家企业信用信息公示系统”和“信用中国”列入严重违法失信名单的；

（3）认证证书的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的；

（4）经行政监管部门确认因获证组织违规而造成重大及以上级别网络安全事件的；

（5）ISMS 没有运行或者已不具备运行条件的；

（6）其他应撤销认证证书的。

3、认证证书的注销

根据新版规则 7.4 条款规定，获证组织主动申请不再保持认证证书时，ZDQY 确认在不存在暂停或撤销情形后，注销其认证证书，并保留相应证据。

八、信息及时通报

获证组织应按认证合同要求及时通报相关信息，包括但不限于:组织重大变化;相关资质变更或失效等;发生违法违规行为，被“国家企业信用信息公示系统”“信用中国”列入严重违法失信名单;信息安全事故等。

九、认证记录保持

根据新版规则 10.5 条款规定，为了证实认证活动的实施，获证组织应留存认证证书有效期内相应的认证记录，至少包括：

（1）认证合同；

（2）审核计划；

（3）首、末次会议签到表；

（4）不符合报告及原因分析和纠正措施；

（5）审核报告；

（6）暂停、撤销通知（适用时）。

需保留认证证书有效期内相应的认证记录，存留的认证记录应为纸质文件原件或不可编辑的电子文档。

十、ZDQY 服务支持

ZDQY 将通过多种方式持续提供支持，协助认证委托人、获证组织深入学习与理解规则要求，推动组织信息安全管理体系运行有效性的持续提升。随函附上《信息安全管理体系认证规则》及其释义，敬请详细查阅。如遇疑问或有相关需要，欢迎联系北京中鼎乾元认证有限公司及各分支机构。

规则的实施旨在提升认证价值，助力组织信息安全管理的持续改进。

感谢贵组织的信任与支持，让我们携手确保认证活动合规、高效过渡！

见：1、《信息安全管理体系认证规则》

2、《信息安全管理体系认证规则释义》