关于“新版《信息安全管理体系认证规则》”的客户告知函

尊敬的客户及相关方：

国家认证认可监督管理委员会（CNCA）正式发布了《信息安全管理体系认证规则》（CNCA-ISMS-01:2026，以下简称“新版规则”），新版规则将于**2026 年 03 月 01 日**起正式实施。为确保贵组织顺利适应新版规则要求，保证认证活动的持续合规性与有效性，现将相关重点变化内容通告如下：

一、与贵组织相关的要求/内容摘要（节选）

（一）认证申请

1、申请条件（5.1.2）

（1）取得合法主体资格及相关法律法规规定的行政许可，并处于有效期内；

（2）已按认证标准建立 ISMS，且运行满**三个月**；

（3）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）；

（4）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）；

（5）当前未被行政监管部门责令停产停业整顿，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**；

（6）ISMS 一年内未发生**重大及以上级别的网络安全事件**。

2、申请信息和文件资料（5.1.3）

贵组织需要提供认证申请、法律地位文件、行政许可文件、组织机构及职责、生产或服务流程图、班次及轮班情况、一年内发生的与网络安全相关的行政处罚信息以及 ISMS 运行满 3 个月的证据。贵组织申请认证前应**先建立、实施 ISMS 并有效运行 3 个月以上，并已实施内部审核、管理评审、留存 ISMS 运行记录**。如相关申请信息和文件资料存在虚假情况，APRZ 将终止认证活动。

（二）认证合同与认证费用

1、认证费用支付（5.3.1）

认证费用应由贵组织**直接**向 APRZ 或 APRZ 分支机构支付。贵组织的上级单位(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 APRZ 支付费用是可接受的形式。

2、贵组织的责任义务（5.3.3、5.3.4）

贵组织应遵守认证程序要求，如实提供相关材料和信息，配合认证行政监管部门的监督检查和 APRZ 对投诉的调查，及时向 APRZ 通报 ISMS 及 5.1.2 中条件的变更情况，通过 ISMS 认证后持续有效运行 ISMS，在广告、宣传等活动中正确使用 ISMS 认证证书、认证标志和有关信息。

（三）认证审核安排

1、审核方案和审核计划（5.4.1、5.4.3、5.4.5）

（1）审核现场应按 APRZ 对贵组织 ISMS 审核方案策划要求，覆盖 GB/T 22080/ISO/IEC 27001 的所有要求，以及认证范围内主要信息安全风险及所涉及的相应产品/服务、班次、多场所现场。

(2) 贵组织应提前确认审核计划，确保现场审核期间**生产/服务处于正常运行状态**。

2、审核时间计算（5.4.2.1）

审核时间按人日计算，**1 人日为 8 小时**，如果贵组织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、初审阶段时间间隔（5.6.1）

初次认证审核应分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。

4、监督审核间隔（5.4.1.4）

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。此后，监督审核间隔不应超过 12 个月。

5、再认证审核要求（5.8.1、5.8.2、5.10.4）

再认证现场审核必须在**原 ISMS 认证证书到期前**完成，目的是评价 ISMS 作为一个整体的持续符合性和有效性。如有严重不符合，纠正和纠正措施的验证也应在**原 ISMS 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。

6、提前较短时间通知的审核（5.9.2）

为**调查投诉、重大及以上级别的网络安全事件**，对**重大变更**作出回应或对被暂停的客户进行追踪时，APRZ 将实施提前较短时间通知的审核。

（四）认证审核实施

1、首末次会议（5.5.3）

贵组织**最高管理者**应参加首、末次会议，因故不能参加的，应提前书面授权其他高级管理层成员参会，并向审核组说明缺席理由。此情况将被记录。

2、最高管理者审核重点（5.5.4、5.7.1）

贵组织**最高管理者**应接受审核组**面对面访谈**，对其在 ISMS 中发挥领导作用的情况、以及亲自参与并推动 ISMS 实施的情况进行重点审核。APRZ 将保留现场图片/音像等证明材料。若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，将不予通过认证。

3、审核终止的情形（5.5.5）

(1) 发生下列情况的，审核组向 APRZ 报告后终止审核：

①贵组织对审核活动**不予配合**，审核活动无法进行；

②贵组织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贵组织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。

(2) APRZ 通过第一阶段审核发现相关**申请信息和文件资料存在虚假情况**的，应终止认证活动。

4、不符合整改（5.10）

贵组织未能在**规定的时限内**完成对不符合所采取措施的，APRZ 将不做出授予认证、保持认证或更新认证的决定。

（五）认证证书和认证标志

1、认证证书有效期（6.2.1、6.2.3）

认证证书有效期**最长为 3 年**。对于未能在原 ISMS 认证证书到期前完成再认证决定的，贵组织的 ISMS 认证证书到期后自动失效，新签发的认证证书有效期将不足 3 年。

2、认证证书暂停、撤销和注销（7.2、7.3、7.4）

新版规则细化了证书暂停（如体系严重不符、受到与网络安全相关的行政处罚、发生重大及以上级别网络安全事件、拒绝配合认证执法监督检查等）、撤销（如法律地位注销、被列入严重违法失信名单、暂停期满未整改、因违规造成重大及以上级别网络安全事件等）及注销（组织主动申请且无暂停/撤销情形）的具体情形、程序和时限：认证机构应在调查核实后 5 日内作出暂停/撤销决定。请贵组织务必关注自身状况，确保证书持续有效。

3、认证证书和认证标志的使用（6.1.2、6.1.3）

贵组织应在广告、宣传等活动中正确使用认证证书、认证标志和有关信息，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 APRZ 名称的情况下，方可在产品包装上标注 ISMS 认证标志**。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**。

（六）认证信息通报（5.3.4、5.1.2）

贵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”和“信用中国”列入“严重违法失信名单”；发生的网络安全事件。

（七）认证记录保存（10.4）

为了证实认证活动的实施，贵组织应留存认证证书有效期内相应的认证资料，至少包括：**认证合同，审核计划，首/末次会议签到表，不符合报告及原因分析和纠正措施，审核报告和暂停/撤销通知**（适用时）。

二、共同遵守与配合执行

新版规则对认证机构和受审核组织都提出了更明确、更细化的要求。请贵组织务必重视上述要求，提前做好准备，积极配合我机构完成相关审核与认证工作。

新版规则过渡期为 2026 年 1 月 15 日至 2026 年 2 月 28 日。在过渡期内，APRZ 将组织相关认证人员完成对规则的研究学习和相关管理文件的修订，确保认证各项工作合规。同时，我们将协助贵组织顺利过渡至新版规则要求，共同提升信息安全管理体系运行的有效性和成熟度。

感谢贵组织一直以来对我们工作的理解与支持!

《信息安全管理体系认证规则》及其释义的查阅网址如下：

信息安全管理体系认证规则：https://www.cnca.gov.cn/zwxx/gg/2026/art/2026/art_d7d0a45aa5294b56a26dbda7a30b33f5.html

信息安全管理体系认证规则释义：https://www.cnca.gov.cn/zwxx/tz/2026/art/2026/art_a2898e7e35b04806957ad2fcfe77ab62.html

如有任何疑问或需进一步解读，请联系奥鹏认证有限公司。

联系电话：023-86826965；88195587。

奥鹏认证有限公司

2026 年 01 月 23 日