版本/版次	修订内容	修订日期	修订人
C/0	管理体系修订（原版 B/5 失效）	2024.08.02	田斌斌
C/1	2025 年 1 月 26 日组织结构变化（部门合并）	2025.01.26	尹东升
C/2	基于预访问问题点修订	2025.09.09	尹东升
C/3	基于文审问题点修订	2026.01.05	尹东升

批准_____刘 芳_____

审核_____尹东升_____

制订_____技术部_____

发布日期：	修订日期：	实施日期：
2020.05.26	2026.01.05	2026.01.05

1、目的和适用范围

1.1 目的

为规范从事认证活动时获得或产生的信息的保密，防止因保密信息的泄露、损坏或丢失而导致经济或其他方面的损失，提高认证的公信力，特制定本程序。

1.2 适用范围

本程序适用于对从事认证活动时获得或产生的信息进行分类、安全与保密的实施等过程的管理。

2、引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。规范性引用文件中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

2.1 CNAS-R02《公正性和保密规则》

2.2 CNAS-CC01《管理体系认证机构要求》

2.3 CNAS-CC170《信息安全管理体系认证机构要求》

2.4 CNAS-CC175《基于 ISO/IEC 20000-1 的服务管理体系认证机构要求》

3、术语定义

3.1 保密性：指认证信息不被泄露给非授权的用户、实体或过程。即认证信息只为授权用户使用。保密性是在可靠性和可用性基础之上，保障认证信息安全的重要手段。

3.2 认证信息:指通过机构对产品、服务、管理体系或人员是否符合特定标准或要求进行书面确认的过程中产生的信息，以及客户提供或审核人员观察到的所有客户信息。包括：

a）认证过程中获取或产生的信息，如客户提供的供应商信息、生产工艺流程图等；

b）来自认证过程之外的信息，如国家监督抽查的不合格信息，与产品或客户有关的投诉等。

4、工作职责

4.1 管理者代表

4.1.1 负责统筹监督各部门信息安全与保密工作的实施。

4.2 行政部

4.2.1 负责员工保密类协议的签订。

4.2.2 负责落实与本部门相关的其他信息安全与保密工作。

4.3 运营部

4.3.1 负责员工保密类协议的签订。

4.3.2 负责保密信息的区分及认证业务活动过程中保密工作的落实。

4.4 其他部门

4.4.1 负责与本部门相关的信息安全与保密工作的落实。

5、工作程序

5.1 信息区分

认证信息须按照《信息通报与处理管理程序》的要求分为“公开信息”和“保密信息”两种。

5.1.1 公开信息

按照《信息通报与处理管理程序》要求，必须主动公开、以及在有特定请求或要求时需要提供的信息属于公开信息。需要公开的信息，运营部负责提前告知客户。

5.1.2 保密信息

除公开信息之外的所有其他信息都属于保密信息，客户或其他信息来源方自己公开的信息除外，保密信息包括但不限于：

a) 申请方和获证组织提交的文件与资料；

b) 在审核过程中获取的信息（申请方和获证组织已公开的或通过其他渠道获取的例外）；

c) 申请方和获证组织要求进行保密的信息；

d) 认证审定过程信息；

e) 公司认证市场开发信息；

f) 公司的认证人员档案；

g）公司受理的申、投诉信息；

h）公司（书面或电子方式）非公开的管理体系文件；

i）公司将其拟对公众公开的信息（客户自己公开的信息除外）；

j）未经特定客户或个人书面同意允许对外披露的信息。当法律要求认证机构向第三方提供保密信息时，除法律限制外，须将拟提供的信息提前通知有关客户或个人；

k）从其他来源（如投诉人、监管机构）获得的关于客户的信息须根据认证机构的政策按保密信息处理；

l）其他需要保密的技术和商业信息（如监管部门提供的信息等）；

m）其他要求保密的信息。

5.2 安全与保密实施

5.2.1 确定保密责任

5.2.1.1 行政部负责每位员工在入职时与广汇联合签定劳动合同或劳务协议，在保密管理相关的条款中明确员工对其从事认证活动时获得或产生的所有信息的保密责任和义务。每位员工及委员与广汇联合签订《公正性及保密承诺书》，向广汇联合承诺对其从事认证活动时获得或产生的所有信息按保密规则实施保密，并承担违规的相应责任和后果。

5.2.1.2 当广汇联合确定选择使用外包方时，按照《外包管理程序》的要求与外包方签订《认证外包协议》，在保密管理相关的条款中明确外包方须对其从事认证活动时获得或产生的所有信息的保密责任和义务。广汇联合还要求外包方签订《公正性及保密承诺书》，承诺把所有与认证有关的受控文件和信息视为秘密，未经广汇联合书面授权不向任何第三方透露（法律法规明文规定的除外），并承担违反承诺的一切后果。

5.2.2 信息公开限制

5.2.2.1 需要公开的信息除外，特定获证客户或个人的信息，未经其书面同意，广汇联合不向任何第三方披露，特定获证客户或个人书面同意，须按照书面同意的公开范围进公开。当法律要求广汇联合向认证监管部门或其他利益相关的第三方提供保密信息时，除法律有明确限制情况之外的，广汇联合须将拟提供给第三方的信息以电话、邮件、函件或其他适宜的方式提前通知有关客户或个人。

5.2.2.2 当法律要求公司或者合同安排（例如与认可机构签订的）授权广汇联合提供特定获证

客户或个人的保密信息时，除法律明确禁止外，广汇联合须将拟提供的信息以电话、邮件、函件或其他适宜方式提前通知有关客户或个人。

5.2.2.3 广汇联合从投诉人、监管机构或其他来源获得的关于客户的信息按照 5.2.2.1、5.2.2.2 条的保密信息措施处理。

5.2.2.4 广汇联合的人员，包括代表广汇联合工作的任何委员会成员、合同方、外部机构人员或个人，都须遵守与广汇联合签定的“保密协议”及《公正性及保密性承诺书》，除法律有要求外，对广汇联合认证活动获得或产生的所有信息予以保密，并对违反协议或承诺产生的一切后果负责。

5.2.3 安全过程及适用的设施设备

5.2.3.1 需要保密的各类文件、记录、资料、信息，各部门都要指定专人管理，妥善保存，未经批准，任何人不得抄录、复制，不得在公众场所阅读或议论需要保密的信息，不私下探听与自身工作无关的信息，不得在任何场合以任何方式扩散和传播需要保密的信息。

5.2.3.2 需要向外部组织或人员提供非公开文件、记录和信息，需经总经理批准。特定获证客户或个人的信息，还须按照 5.2.2.1、5.2.2.2 要求执行。

5.2.3.3 对需要列入公开文件和公开网络的信息需经总经理确认同意才可。

5.2.3.4 保密信息的存放需配备相应的设备和设施，认证项目纸质档案须放置在档案柜中，电子档案存放在专门的计算机存储设备中，并定期做备份处理。

5.2.3.5 纸质文件存放须保证干燥、防潮、防盗。电子文档设置适当权限，防止文件以各种方式泄密。所有存档文件的借阅须按照《文件控制程序》或《记录控制程序》要求实行借阅审批。

5.2.3.6 对于已经处理的不需要保留的资料，做销毁处理。

5.2.3.7 计算机硬件和软件、网页、公司网站、公司信息数据、互联网及其他一切与信息系统安全有关的使用和管理，由专门部门行政部统一负责实施。

5.2.3.8 审核过程中的信息安全管理

现场审核以及应用 ICT 的远程审核时涉及到的客户组织及广汇联合双方信息都须做好安全管理，严格遵守保密要求，包括但不限采取如下措施：

a）审核前的沟通，尤其是在应用 ICT 审核时，审核组长负责须事先与客户沟通，了解客户组织的信息安全规定，明确哪些信息因保密要求不能抽样取证、哪些信息不能使用 ICT 抽样

取证以及其他相关的信息安全特殊规定。

b）计划制定时，须充分考虑客户组织的信息安全要求，在保证审核有效性的前提下选择合适的抽样取证方式；

c）审核过程中须定公正性及保密承诺。须在不违背客户的信息安全管理要求及保证审核有效性的前提下，合理取证，涉及到保密等级较高的信息，须事先征得客户组织的允许。所获得的审核取证信息都须采取适当的方式（例如:设置电脑屏保密码、备份）安全保存，防止信息泄漏或丢失。审核现场结束后须及时删除不必要的信息。现场查阅的各种文件资料，审核结束时必须原数归还，不得他用。

d）审核获取用于存档的各种信息须严格按照保密要求保管，纸质案卷邮寄给案卷受理的专人，形成档案后按照《记录控制程序》附录 A:认证项目档案管理规定要求保管，电子部分以点对点的方式提供给案卷受理专人，形成档案后按照《记录控制程序》附录 B:电子档案的相关规定要求保管。除法律法规要求外，未经客户组织允许，禁止向第三方泄漏。

e)ISMS 及 ITSMS 审核还须在审核前与客户沟通，要求客户口头或书面报告是否存在因包含保密信息或敏感信息（例如，ISMS 或 ITSMS 记录或关于控制的设计与有效性的信息）而导致不能提供给审核组审查的 ISMS 或 SMS 相关信息，审核组讨论确定是否能在缺少这些文件或记录的情况下得到充分审核。若已识别的保密信息或敏感信息不属于国家保密信息，且审核组讨论的结论是缺少这些信息就不能对 ISMS 进行充分地审核，审核组长负责告知客户只有在适当的访问安排获得许可后才能进行认证审核，并及时反馈计划调度人员，以便调整审核日程安排。若已识别的保密信息或敏感信息属于国家保密信息，应将其排除在认证审核之外，若审核组讨论的结论是缺少这些信息就不能对 ISMS 进行充分地审核，应终止审核或通过替代的审核方法（如审查非涉密的管理流程、由客户提供脱敏证明、或由上级保密部门出具合规声明等）以实现审核的充分性。

f)ISMS/ITMS 认证审核还须：

1)直接接触客户信息的认证人员(例如,审核组成员)须按照客户的保密要求与客户签署保密协议，或向客户做出保密承诺。

2)如果客户事先没有禁止公司接触某一信息和相关资产，或未告知公司应满足的要求，但公司在认证过程中发现自己并不具备接触该信息资产的资格和条件，应立即向客户提

出。

3)审核组成员不宜在审核过程中以任何方式记录客户的保密或敏感信息。审核组在离开客户前，请客户检查和确认审核组携带的文件、资料和设备中未夹带客户的任何保密或敏感信息。

5.2.4 违反保密规定的处理

5.2.4.1 公司内部和外部人员均有权向公司保密工作主管部门反映、举报泄密行为。

5.2.4.2 经保密工作主管部门核实情况后，按照已签署的保密协议规定，提出处理意见，报总经理批准后执行。

5.2.4.3 对违反本程序规定，但未造成泄密，或已造成泄密而影响程度轻微的从轻处理，如批评、警告；对违反本程序规定，而造成泄密，并影响严重的从重处理，如行政处分、经济赔偿、直至追究法律责任。

5.2.4.4 行政部负责保存处理结果的记录，并作为评价人员工作的重要依据。

6、相关文件

6.1 《信息通报与处理管理程序》

6.2 《外包管理程序》

6.3 《文件控制程序》

6.4 《记录控制程序》

7、相关记录

7.1 《公正性及保密性承诺书》（员工用）；

7.2 《公正性及保密性承诺书》（公正性委员会用）；

8、 附录

无