10240 — CONFIDENTIALITY OF CLIENT INFORMATION

Effective Date

Issued April 25, 2008; effective immediately.

[Superseded Guidance: AAPMS GEN 240 (3-93)]

Introduction

This Section of the Manual provides policies and guidance on maintaining the confidentiality of Client information.

Policies and Guidance

General

1. Rule 301 of the AICPA Code of Professional Conduct states, in part, that "a member in public practice shall not disclose any confidential client information without the specific consent of the client." Also, various states have statutes or rules relating to the disclosure of Client information; our personnel should be familiar with such statutes or rules for the states in which they practice. In addition, Section 7216 of the Internal Revenue Code provides for penalties for unauthorized use or disclosure of any information furnished by a Client in connection with the preparation of the Client's tax returns or declarations of estimated tax ("tax information"). If we perform both audit and tax services for an entity, we consider tax information to be limited to the information that we would not have obtained in connection with our audit had we not also been engaged to prepare the Client's tax return.

2. We have access to a significant amount of confidential information about an entity's affairs not otherwise available to the public. Much of the information concerning an entity that we obtain in connection with performing an audit, tax, or consulting service is confidential. Accordingly, as stated in the Codes of Ethics and Professional Conduct for Deloitte LLP and each of its function-specific subsidiaries (see Section 10110, Codes of Ethics and Professional Conduct — Deloitte U.S. Entities), we should preserve the confidentiality of information we obtain in performing such professional services and should not disclose confidential Client information to:

- Anyone who works outside the Client's organization
- Anyone within the Client organization without a need to know
- Anyone within the Deloitte U.S. Entities or other DTT Member Firms, unless there is a legal or professional right or duty to disclose, or a written Client consent has been obtained.

When there is doubt as to the duty or a right to disclose, the matter should be discussed with the applicable functional Professional Practice Director (PPD) or National Risk Management, and, if necessary, advice should be sought from the Office of the General
3. Disclosure may be required by law if, for example:
   - We have been subpoenaed to produce confidential Client information in connection with legal proceedings
   - We have been requested to produce confidential Client information by state or federal agencies or regulators who have the authority to require such production under subpoena.

A professional duty or a right to disclose may arise, for example, in the course of
   - Complying with technical standards, and professional and ethical requirements (e.g., peer reviews or practice reviews)
   - Protecting the interests of the Deloitte LLP and its subsidiaries (collectively, the Deloitte U.S. Entities) in legal proceedings.

When there is doubt as to the duty or a right to disclose, the matter should be discussed with the applicable functional PPD or Lead Risk Manager, and, if necessary, advice should be sought from the Office of the General Counsel.

4. Confidentiality is not only a matter of nondisclosure of information, but it also requires that information acquired in the course of performing professional services should neither be used nor appear to be used for personal advantage or for the advantage of Deloitte Touche Tohmatsu (DTT), another Client, or a third party. Confidential Client information is deemed to be any information that is not generally known or available to the general public (e.g., published in a book, periodical, newspaper, or in an entity document that has been released to the public or is otherwise a matter of public knowledge).

5. Unless we know that particular Client information is generally known or available, we treat such information as confidential. Even with information that has been disclosed to the public (e.g., quarterly operating results), we are discreet in deciding where and with whom we discuss such information as any remarks we make may be assumed to have an unwarranted degree of authority. Additionally, we should preserve the confidentiality of information after the completion of an Engagement, after we are no longer employed by one of the Deloitte U.S. Entities, and even after the end of the relationship between us and the Client.

6. The requirements of confidentiality extend to dealings with an entity's employees. If we deal with personnel in the entity's organization, we should not disclose sensitive information to those for whom the information is not intended. Care is taken so that information acquired in the course of performing professional services is disclosed only to those employees who are authorized by entity management to have access to it. Any doubt is resolved by not discussing the information with others in the entity's organization or, alternatively, by inquiring of an appropriate entity official (who may be the source of such information) as to those with whom the information can be discussed.

7. In working with confidential information (e.g., compensation or a sensitive transaction) or documents relating to such information, we take steps to prevent inadvertently allowing unauthorized entity personnel access to such confidential information or documents. Preferably, our work is performed in an area that is not accessible to unauthorized personnel. Alternatively,
we arrange our work area so that confidential documents cannot be accessed by unauthorized persons. **We should maintain adequate security over working papers (in paper or electronic form) and all entity records in our possession.** In no event do we leave confidential documents unattended, except in a secure file or room (to which unauthorized Client personnel do not have access). Policies and guidance relating to audit working papers are addressed in [AAPMS AAM P020, Prepare and Control Working Papers](https://dart.deloitte.com/nxt/gateway.dll/USDPM/major%20section00104/section00119.htm).

8. In performing services for one Client, we may become aware of information that could impact our services for another Client. For example, in performing audit services for Client A, we may become aware that the owners of Client A are officers of a Subsidiary of Client B, a public company. Such information is confidential and is not disclosed except with the consent of the Client (in the foregoing example, Client A). Prohibition against disclosure of confidential Client information does not, however, preclude internal discussion, using National Office (Quality Assurance) as a conduit, of information concerning financial transactions that appear to be illegal, of a questionable nature, or that affect the scope of audit work or financial statement disclosure at another Client (for example, the Subsidiary of Company B made significant purchases from Company A). Such information may have an effect on the nature, timing, and extent of our auditing procedures with respect to the other Client (in the foregoing example, Client B). **If we become aware of information that (1) affects another Client served by us which creates a potential conflict or (2) involves transactions of such a nature that personnel serving the other Client might have need of that information, the matter should be discussed with the applicable functional PPD or Lead Risk Manager and, if necessary, with the Office of General Counsel before a conclusion is reached concerning the appropriate course of action in the circumstances. If we provide audit or other attest services to the "other Client," National Office (Quality Assurance) should also be consulted.**

9. For International Engagements, application of the policies pertaining to confidentiality of Client information requires careful consideration when a participating Member Firm (including us as a participating Member Firm) is performing professional services for a referring Member Firm. **Ordinarily, Client information (e.g., regional sales data and inventory statistics) gathered during the work of the participating Member Firm should be available to the Parent Company and the referring Member Firm — they should not be considered "third parties."** However, laws, regulations, professional requirements, and codes of conduct of some countries may prevent a participating Member Firm from passing certain information to anyone, even to the Parent Company, without the prior approval of local management. **In such a situation, if the participating Member Firm obtains information that should be communicated to the Parent Company and the referring Member Firm, the participating Member Firm should discuss the matter with local management. In those rare circumstances when local management refuses to agree to the communication and the participating Member Firm is unable to reach a resolution, the matter should be resolved in accordance with the policies set forth in [Section 3620, Addressing Differences of Opinion](https://dart.deloitte.com/nxt/gateway.dll/USDPM/major%20section00104/section00119.htm).**

10. **We should limit internal discussions of confidential Client information to persons serving the Client or as required under our policies or professional standards.** Such discussions are held in a manner so as to otherwise continue to preserve the confidentiality of such Client information.

11. **In accordance with ethical standards of the profession and our ethical standards, we should not use information obtained in the course of performing Client services for personal gain, such as through insider trading or other means.**
12. A copy of the relevant Code of Ethics and Professional Conduct (see Section 10110) is provided to all personnel when they are employed. It is each individual's responsibility to read their applicable Code of Ethics and Professional Conduct, to become familiar with its contents, and to comply with its guidance. All personnel are required to provide an annual representation as to compliance with their applicable Code of Ethics and Professional Conduct.

**Industrial Security Clearance**

13. Before partners and staff can have access to government classified information or visit Client locations where a clearance is required, they are ordinarily required to obtain security clearance. Operational responsibility is assigned to the Facility Security Officer presently in our Washington, D.C. office. Other practice offices involved in significant classified work may be granted "facility clearance." Facility Security Officers, assisted by Security Supervisors in each cleared location, are responsible for the supervision and direction of security measures within their offices and for the processing of applications for partners and staff assigned to a "cleared facility" or related office.

14. All requirements for security clearance originate with a user agency of the Department of Defense (DoD) or with an entity under a classified contract with one of those agencies. Requirements must be documented on DoD Form 254, "Contract Security Classification Specification." The form is prepared by the entity and sent to the Defense Investigative Service. The entity is asked to provide a copy of the form or a letter confirming the request for security clearance to our Facility Security Officer. On receipt of such documentation of the request, the Facility Security Officer can process the application. **Any questions regarding clearance procedures or policies should be addressed to the Facility Security Officer in Washington, D.C.**

15. No information pertaining to classified contracts or projects should be released (even if we have obtained the entity's permission), until after clearance by the Directorate for Freedom of Information and Security Review, Office of the Secretary of Defense (Public Affairs).

**Confidentiality Agreements in Connection With Audit or Other Attest Services**

16. When a Client or a prospective Client requests that we enter into a confidentiality agreement or commitment in connection with a proposal opportunity to provide audit or other attest services, or in connection with the actual audit or other attest services we are to perform, the Audit Engagement Partner should inform the entity or the prospective Client that we are bound by professional standards (e.g., ET Section 301, Confidential Client Information, and ET Section 391, Ethics Rulings on Responsibilities to Clients, in the Code of Professional Conduct of the American Institute of Certified Public Accountants) regarding the confidentiality of Client information, and, therefore, it is unnecessary that a separate confidentiality agreement or commitment be signed. We recognize that, notwithstanding the foregoing, certain Clients or prospective Clients may insist on our entering into a separate confidentiality agreement or commitment in connection with a proposal opportunity to provide audit or other attest services or in connection with the actual audit or other attest services we are to perform.

17. If, notwithstanding our obligation to abide by professional standards, the entity or the prospective Client still insists that we enter into a separate confidentiality agreement or commitment (even one limited to acknowledging our professional obligations) in connection
with a proposal opportunity to provide audit or other attest services, or in connection with the actual audit or other attest services we are to perform, the Audit Engagement Partner should consult with the Audit PPD and, as applicable, the Audit RPPD prior to agreeing to enter into a separate confidentiality agreement or commitment with the entity or a prospective Client, as follows:

- The Audit Engagement Partner should consult with the Audit PPD and obtain the Audit PPD's approval prior to agreeing to enter into a separate confidentiality agreement or commitment with a prospective Client in connection with a proposal opportunity. In situations in which the Audit PPD agrees that we should enter into a separate confidentiality agreement or commitment in connection with a proposal opportunity, we should use the illustrative confidentiality agreement in Example A, "Confidentiality Agreement in Connection With a Proposal for the Provision of Audit or Other Attest Services," of Form GEN240, *Illustrative Confidentiality Agreements — U.S. Firm*.

- The Audit Engagement Partner, in consultation with the Audit PPD, should also consult with the Audit RPPD and obtain the Audit RPPD's approval prior to agreeing to enter into a separate confidentiality agreement or commitment with the entity in connection with the actual provision of services. Situations in which we agree to enter into a separate confidentiality agreement or commitment with a Client in connection with the actual provision of services are expected to be rare. In those rare situations in which the Audit PPD and the Audit RPPD agree that we should enter into a separate confidentiality agreement or commitment in connection with the actual provision of services, we should use the illustrative confidentiality agreement in Example B, "Confidentiality Agreement in Connection With the Provision of Audit or Other Attest Services," of Form GEN240.

The Audit PPD and, as applicable, the Audit RPPD should consult with the Office of General Counsel if we are requested to modify the standard wording in the illustrative confidentiality agreements in Form GEN240. The concurrence of the Audit PPD and, as applicable, the Audit RPPD, following consultation with the Office of General Counsel, should be obtained prior to agreeing to modify such wording. Situations in which we agree to modify the standard wording in the illustrative confidentiality agreements are expected to be rare. Any disagreements should be resolved through consultation with the Partner-in-Charge of Quality Assurance (see Section 10610, *Consultation Resources*).

**Deloitte Radar Access and Information**

18. Electronic access to the Deloitte Radar website is not to be given to any entity or outside party. Certain information from the Deloitte Radar website may be provided to the entity under the conditions set forth in paragraphs 19–21. These conditions vary, depending on the type of information:

- Proprietary risk indices of financial statement fraud and business failure risk
- Benchmarking information.

**Proprietary Risk Indices**

19. Deloitte Radar uses risk indices to score and determine the entity's susceptibility to business failure and financial statement fraud, which are expressed as different levels of risk. The risk
indices are for use by our personnel only and are not to be provided in whole or in part to any other person or entity. While we can share general information with the entity's management or audit committee about the model, the restriction for use of risk indices applies to all entity-specific information related to the business failure or financial statement fraud indices (i.e., "green," "yellow," or "red" results) contained on the "risk management" home page, the "category" page, and the "metrics" pages within Deloitte Radar.

Benchmarking Information

20. Users of Deloitte Radar are able to benchmark Client data against other entities using the "Benchmark Report." This information may only be shared with the Client for whom the Benchmark Report was created. Benchmark Reports for other entities are not to be shared with other Clients or third parties.

21. Any information provided to a Client needs to include the following disclaimer:

At the request of XYZ Enterprise, Inc. (the "Organization"), we derived benchmarking information for the Organization based solely upon information obtained from public and third-party information sources.

Disclaimer — Deloitte & Touche LLP has made no attempt to verify the reliability of the information obtained from these public and third-party sources. This benchmarking data is limited in nature and does not comprehend all matters relating to benchmarking that might be pertinent to the Organization's intended use.

We make no representation as to the sufficiency of this benchmarking data for your purposes.

This benchmarking data should not be viewed as a substitute for other forms of analysis that management should undertake in order to assess whether such benchmarking data is adequate or appropriate for the Organization's purposes. The information in this report is not intended to constitute legal, accounting, tax, investment, consulting, or other professional advice or services. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional advisor. This benchmarking data is solely for your informational purposes and internal use and you should not disclose it to any other person or entity. THIS BENCHMARKING DATA AND THE INFORMATION CONTAINED HEREIN IS PROVIDED "AS IS" AND DELOITTE & TOUCHE LLP MAKES NO EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES REGARDING THIS INFORMATION. YOUR USE OF THIS BENCHMARKING DATA IS AT YOUR OWN RISK. DELOITTE & TOUCHE LLP WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE DAMAGES, OR OTHER DAMAGES, WHETHER IN AN ACTION OF CONTRACT, STATUTE, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE), OR OTHERWISE, RELATING TO THE USE OF THIS BENCHMARKING DATA OR INFORMATION CONTAINED HEREIN.

Principal Professional Pronouncements

22. The following professional pronouncements may provide additional requirements and information about the topics discussed in this Section:

- ET Section 301, Confidential Client Information
ET Section 391, *Ethics Rulings on Responsibilities to Clients.*