

IEEE Guide to Classification of Documents

October 2019

This IEEE Guide to Classification of Documents (Guide) provides procedures for the implementation of IEEE Policies, Section 9.24 Information Disclosure Policy. The procedures are applicable to all members of the IEEE community, including employees, subcontractors, and volunteer leaders. This Guide does not and is not intended to supersede the provisions of IEEE policies and procedures for records retention.

The initial version of this Guide was approved in June 2015 by the IEEE Board of Directors.

Preface

The Guide shall be maintained by the IEEE Governance Committee who shall 1) report appropriate amendments to the Guide to the IEEE Board of Directors, and 2) report any issues with compliance to this policy and the procedures contained in the Guide at least annually.

This policy and the supporting guide shall apply to all IEEE Organizational Units, the creation of OU specific policies or classifications, beyond those described here or in the Guide, is not permitted.

The Guide shall be made accessible on the IEEE Website at <http://www.ieee.org/about/corporate/governance/index.html> (IEEE Policies, Sections 9.24 – Information Disclosure Policy)

Any comments on this document or suggestions for improvement should be submitted to the Governance Committee of the IEEE Board of Directors at info-disclosure@ieee.org

Approved by the IEEE Governance Committee 5 October 2019

9.24 Information Disclosure Policy

1. *As an educational, scientific organization dedicated to the benefit of the public, IEEE recognizes and endorses the fundamental importance of transparency and accountability in all its activities. Accordingly, it is IEEE's policy to be open about its activities and to welcome and seek out opportunities to explain its work to the widest possible audience.*
2. *Notwithstanding the dedication to the fundamental importance of transparency IEEE also recognizes that some aspects of its operations need to be kept confidential. Thus certain types of information are protected when unrestricted availability would be detrimental to its operation and/or membership. Such information includes verbal or non-verbal communication or information recorded on paper or electronically recorded.*
3. *When information is recorded in a document embodied in a medium that can be stored, read and or transmitted, such media including but being not limited to paper or electronic media, IEEE has defined two levels of classification for documents that should be restricted to the IEEE community. These classifications include:*
 - *Proprietary. The classification Proprietary shall be applied to documents available to members of IEEE and IEEE staff.*
 - *Confidential. The classification Confidential shall be applied to documents whose distribution to authorized volunteer leaders* and IEEE staff on a need to know basis. Within this classification any documents that are to be limited to stricter controls on distribution, shall be classified as "Confidential – Controlled Distribution".*
 - *The treatment of information that is subject to attorney-client privilege is governed by statutory and judicial pronouncements and, therefore, not addressed, regulated or administered by this policy.*

Details and procedures related to the identification of documents that should be classified, proper classification, sharing, distribution, storage and disposal of IEEE documents that carry these classifications, shall be maintained in the IEEE Guide to Classification of Documents. The Guide shall also include but not be limited to providing guidance on the appropriate expiration of such classifications, the identification of authorized volunteer leader positions, the handling of reclassification when appropriate and minutes of executive sessions.

The Guide shall be maintained by the IEEE Governance Committee who shall 1) report appropriate amendments to the Guide to the IEEE Board of Directors, and 2) report any issues with compliance to this policy and the procedures contained in the Guide at least annually.

This policy and the supporting guide shall apply to all IEEE Organizational Units, the creation of OU specific policies or classifications, beyond those described here or in the Guide, is not permitted.

*The Guide shall be made accessible on the IEEE Website at
<http://www.ieee.org/about/corporate/governance/index.html>*

**For purposes of this Policy, the term "authorized volunteer leader(s) or AVLs" refers to individuals holding specific volunteer positions within IEEE who shall complete an online training course acknowledging an understanding of the appropriate handling of IEEE information. The list of positions that are considered AVLs, shall be specified in the IEEE Guide to Classification of Documents.*

Table of Contents

IEEE Guide to Classification of Documents	1
Preface	1
Table of Contents	3
1 Quick Reference Summary of Concepts and Procedures	4
2 Key Information	6
2.1 Purpose	6
2.2 Objectives	6
2.3 Scope and Limits	6
2.4 Key Terms	7
2.4.1 Document	7
2.4.2 Authorized Volunteer Leader (AVL)	7
2.4.3 Classification	7
2.4.4 Need to Know	7
2.4.5 Originators and Readers	7
2.4.6 Records Retention	8
3 Protecting and Sharing Classified Information	9
4 Handling Classified Documents in Meetings	10
5 Disposing of Classified Documents	12
6 Reclassifying Documents	13
7 Creating Classified Documents	14
8 Assigning Classification	16
8.1 Product Data	16
8.2 Operations Data	17
8.3 Strategic Data	18
8.4 Data regarding Relationships with Other Organizations	18
8.5 Governance Data	19
8.6 Personnel Data	20
8.7 Legal Data	21
9 Authorized Volunteer Leaders (AVLs)	22
10 Use Within Organizational Units	23

1 Quick Reference Summary of Concepts and Procedures

The following table summarizes information found elsewhere in this document:

	(Not classified)	IEEE Proprietary	IEEE Confidential	IEEE Confidential-Controlled Distribution
Frequency of use	The norm	Common	Rare	Exceedingly rare
Characterization	IEEE products, public communications, and records of volunteer activities		Information that could adversely affect the business operations, privacy commitments, or legal obligations of IEEE if disclosed	Information that, in accordance with law, bylaws, policies, or procedures shall be restricted to a defined list of individuals
Availability	Available to the public—may be subject to copyright, fees, etc.	Available to all IEEE staff and members	Available to all IEEE staff and Authorized Volunteer Leaders with a need to know	Availability limited to those on the distribution list. May not be redistributed.
Examples (See § 8)	Business cards, products, publications, price lists, annual report	Organization charts, financial data, statistical abstractions of higher-classified data	R&D plans, product strategies, consideration of policy changes, compilations of lower-classified data	Most personnel information, negotiable prices and terms, trade secrets and patents, mergers and acquisitions, executive session minutes
Need to know is determined by (See § 2.4.4)	Not applicable	Reader	Reader	Distribution list provided by originator

Classification markings (See § Error! Reference source not found.7)	Not applicable	Classification Level, Originator	Classification Level, Originator	Classification Level, Originator, Distribution list
Protection (See § 3)	Not applicable	Reasonable care	Locked drawer, restricted access, delivery tracking	Locked drawer, encryption, delivery receipt and tracking
Disposal* (See § 5)	Not applicable	Normal deletion from computer. For small quantities of paper, normal trash. For large quantities, treat like IEEE Confidential.	Paper: shred, burn or dispose in designated container. Electronic: secure deletion	Paper: return to originator, shred, burn or dispose in designated container. Electronic: secure deletion
Meeting audience (See § 4)	Not applicable	IEEE members and IEEE staff	May need Executive session e.g., AVL, volunteer leaders)	Executive session

2 Key Information

2.1 Purpose

IEEE Policy 9.24.1 states that:

As an educational, scientific organization dedicated to the benefit of the public, IEEE recognizes and endorses the fundamental importance of transparency and accountability in all its activities. Accordingly, it is IEEE's policy to be open about its activities and to welcome and seek out opportunities to explain its work to the widest possible audience.

The purpose of this document is to provide guidance on the application of IEEE's policy on information disclosure. Accordingly, much of IEEE's information should be available to the public and nearly all of it should be available to its members. Procedures for information disclosure are appropriate to deal with the small fraction of information that should receive a more restricted distribution.

2.2 Objectives

IEEE's information disclosure policy has two objectives:

- To increase the flow of information among volunteers and staff
- To protect the small amount of information that requires protection

It follows from these objectives that the procedures should give everyone—both volunteers and staff—the information that they need to discharge their duties; reduce the need for and use of executive session; and comply with any applicable laws.

An information disclosure policy necessarily exists between two needs:

- Should the information be disclosed to provide benefit to the public, to fulfill the members' right to know, and to provide the information needed for everyone to do their jobs?
- Should the information be protected to preserve competitive advantages, to fulfill legal obligations, and to protect privacy?

Every person in the IEEE community needs to be mindful of both sets of needs and apply judgment to find the right balance. This document is intended to provide assistance in making those informed decisions.

2.3 Scope and Limits

These procedures apply to all information created and maintained by IEEE and its organizational units, with the exception of privileged information created by attorneys or in correspondence with attorneys. Any privilege markings provided in the course of correspondence with legal counsel preempt any markings provided by this set of procedures.

2.4 Key Terms

2.4.1 Document

A “document” is any written, printed, or electronically stored information that can be read, viewed or heard [listened to], by a human, regardless of whether the information is stored on social media accounts, chats, instant messages, or contained in collaborative work environments and other databases. Databases are not necessarily documents, but the reports and information retrieved from a database are documents. For purposes of this Policy, video and audio recordings are considered documents.

2.4.2 Authorized Volunteer Leader (AVL)

An Authorized Volunteer Leader is an IEEE volunteer who has undergone the appropriate procedures (as described in IEEE Policies, Section 9.24 - Information Disclosure Policy) to be entrusted with IEEE confidential information. For the purposes of this Guide, AVLs and IEEE employees have the same privileges and responsibilities in dealing with IEEE’s information. *See Section 9, Authorized Volunteer Leader (AVLs), for more information.*

2.4.3 Classification

Classification is used on documents to indicate the nature of the content and the audience that may have access to the document. Not all documents are required to have a classification. As noted earlier in this document, IEEE has two levels of classification: IEEE Proprietary and IEEE Confidential. Some information is subject to stricter controls on distribution, such information is marked as IEEE Confidential—Controlled Distribution.

2.4.4 Need to Know

The basis for sharing confidential information inside the IEEE community. If AVLs or staff members need the information in a document in order to perform their duties, then they have a “need to know”.

In the case of “IEEE Confidential” documents, the need to know is determined by the reader of the document.

In the case of documents marked “IEEE Confidential—Controlled Distribution”, the need to know is determined by the originator of the document. Before such a document can be shared, the originator shall add recipients to a distribution list. (*section 3 for additional information*)

2.4.5 Originators and Readers

The “originator” of a classified document is the person who created the document. If it is a team effort, then the originator might be the lead person of the team. The originator selects the appropriate classification level, and, in the case of “IEEE Confidential—Controlled Distribution”, determines and maintains the list of people who may have access to the document.

The “reader” is anyone who has access to a classified document.

In the case of documents marked “IEEE Confidential”, the reader is free to share the document with an AVL or staff if the reader determines that they have a “need to know”.

2.4.6 Records Retention

In addition to its policy on Information Disclosure, IEEE also has a policy on records retention. The two are distinct—Records Retention regulates the preservation of documents while Information Disclosure regulates the sharing of the information in those documents. Nothing in this Guide supersedes the requirements of the records retention policy.

3 Protecting and Sharing Classified Information

Every person in the IEEE community has the responsibility to protect classified documents that are in their custody. This section describes the requirements.

IEEE Proprietary documents

- may be shared with any IEEE member or staff.
- shall not be left unattended in public places
- require no special protection aside from reasonable care.

IEEE Confidential documents

- may be shared with any Authorized Volunteer Leader or staff if they have a *need to know*.
 - To share with others, it must be determined if the receiver:
 - is, in fact, an employee or an Authorized Volunteer Leader.
 - has a need to know the information in order to conduct their duties and responsibilities.
- shall be in the physical possession of the responsible individual when in active use
- shall be stored in a locked container when not in active use
- when traveling, IEEE Confidential documents shall be secured in a manner similar to a valuable object, e.g., out of sight in a locked automobile, locked briefcase, hotel safe, etc.
- when mailed, shall be via a method that provides delivery tracking confirmation

IEEE Confidential—Controlled Distribution documents

- may be shared only with those who appear on the distribution list.
- To share with others not on the distribution list, one shall seek the agreement of the originator or the originator's superior to modify the distribution list
- when mailed, shall be via a method that provides delivery tracking confirmation.
- shall be encrypted* when storing on an electronic device or transmitted electronically, except when in actual use. (Note that there are common software packages that include an encryption* option.)

Documents labeled IEEE Proprietary or above may be disclosed to individuals outside IEEE only after staff has executed a non-disclosure agreement with the party outside of IEEE.

*** Pending additional study of encryption policy across IEEE, the provision above is a recommendation that should be applied whenever possible.**

4 Handling Classified Documents in Meetings

This section describes the treatment of classified information in meetings. In particular, it addresses the use of executive session.

According to IEEE Bylaw I-300.1 Governance; Parliamentary Procedures; Meeting Protocol, IEEE meetings are open only to IEEE members and staff. Therefore, IEEE Proprietary documents can be discussed without executive session. The meeting chair should take reasonable precautions to ensure that no non-members are present. A non-member may remain in the room for an item in which the non-member has a “need to know” only after the non-member has executed a non-disclosure agreement.

To consider documents classified IEEE Confidential or above, it *may* be advisable to enter executive session. The chair, subject to the will of the body, normally controls attendance in executive session. In the normal course of business, items are designated for executive session by adoption of the agenda. However, this can be changed during the meeting by majority vote.

An executive session to consider IEEE Confidential (not Controlled Distribution) documents could have a liberal rule regarding attendance. For example, all staff and AVLs might be allowed to remain in the room.

A topic might be described in both a Proprietary document and a Confidential supplement to enable some consideration of an issue in open session. If more in-depth consideration is needed, further discussion can proceed in executive session.

The minutes of an executive session are inherently IEEE Confidential—Controlled Distribution. It may be desirable, though, to distribute results from an executive session, based upon whatever actions were taken. In that case, possible actions for this situation include:

- The executive session itself may determine that its minutes are to be classified at some other level. This could be done during the executive session itself or during the executive session that approves the minutes of a previous executive session.
- The body, in general session or executive session, could delegate to a committee the responsibility for preparing “sanitized” minutes that could be classified at a lower level.
- The body, in general session or executive session, could delegate to a committee the responsibility for preparing a report of the executive session that could be classified at a lower level.

If an executive session is convened to consider an IEEE Confidential document, the minutes of the executive session are Controlled Distribution, but the original document retains its Confidential classification. The classification of a document is *not* increased merely because

it was considered during executive session. Furthermore, if the executive session results in the creation or modification of a document, the normal guidelines for classification still apply. The minutes are the only product of an executive session that are inherently Controlled Distribution.

5 Disposing of Classified Documents

Volunteers and staff are encouraged to routinely dispose of obsolete documents. However, disposal of classified documents may require some additional care.

IEEE Proprietary documents

- Electronic documents may be deleted in the usual manner
- Paper documents
 - small quantities, may be discarded in the normal trash if intermixed with large quantities of other trash.
 - large quantities of documents should be disposed in the same manner as IEEE Confidential documents.

IEEE Confidential documents

- Electronic documents should be deleted in a manner that prevents easy recovery of the document.
- Paper documents should be either shredded or burned, or placed in containers designated for secure disposal.

IEEE Confidential—Controlled Distribution

- Paper documents can be disposed of in one of two manners
 - return the document to the originator. (providing evidence that the document was not passed on to others)
 - shred, burn, or place in a secure disposal container.
- Electronic documents should be deleted in a manner that prevents easy recovery of the document.

6 Reclassifying Documents

The originator of any document classified as IEEE Confidential or above are encouraged to include a date for reclassification to Proprietary¹ and depending on the content would normally be suitable for reclassification after one year.

The Board of Directors or the top deliberative body of any OU may reclassify a document that was originated within their purview. (In such cases, it may be appropriate to designate a representative of the Board as the “originator” of the reclassified document.)

In some cases, there may be disputes regarding the appropriate classification of a document. Such disputes are to be resolved by the Governance Committee. The Governance Committee and the Board of Directors shall be provided access to any classified documents for the purpose of resolving any disputes regarding the appropriate level of classification.

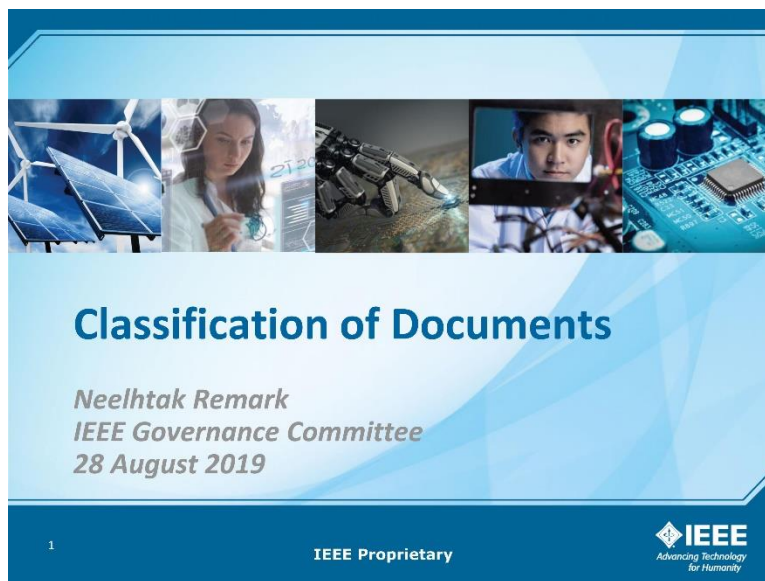
The Governance Committee may, at its discretion, propose that the Board of Directors consider reclassifying any document.

¹ There are some exceptions (described in Section 8) for personnel and governance documents that are the subject of legal regulation. Such documents are never lowered in classification, but are instead destroyed when no longer useful. (Note that the IEEE Policy on Records Retention may require that an archival copy be retained for legal purposes.)

7 Creating Classified Documents

The selection of an appropriate classification level for a document is an important decision. Selecting a level that is too high has the effect of withholding important information from volunteers and staff who need it. Selecting a level that is too low may inadequately protect IEEE's important intellectual assets. The next chapter of this Guide provides guidance in selecting a level. Because the decision is an important one, originators may wish to consult with others before selecting a level.

Experience suggests that many documents primarily consist of a large amount of information at one classification level and a small amount of information at a higher level. In such cases, best practice is to create a document that contains the lower level information and a distinct annex—a separate document—that contains the more highly classified information. This allows the majority of the information to be shared more freely. This practice also permits the use of labor-saving word-processing techniques, such as headers and footers, to apply the classification label to each page.



Example of IEEE Proprietary

If the document is classified IEEE Confidential or above, the cover page may include a date on which the classification will be lowered to IEEE Proprietary. Normally this should be one year from the date of creation.

If the document is classified IEEE Confidential—Controlled Distribution, it shall include an authorized distribution list. The distribution list does not necessarily consist solely of person’s names. It might include the names of positions, e.g. “Members of Products and Services Committee.”



Example of IEEE Confidential - Controlled-Distribution

8 Assigning Classification

In determining the classification of a document, one needs to make two decisions:

- What level of classification is appropriate?
- What should be the period of time until the classification expires?

This section provides guidance in making both of those decisions. The examples are simply the types of documents that might be considered for classification. Minutes from some types of meetings, for example, may need to be classified, while many more may not. This classification guide rests on human judgment, not simply a document name.

8.1 Product Data

Examples of product data include the following:

A document containing this type of data...	... might be classified at this level for this duration.	Notes
Non-negotiable prices, terms and conditions	Unclassified		
Negotiable Prices, Terms and Conditions	IEEE Confidential—Controlled Distribution	The effective period of time plus one year	
Internal documents developing prices, terms, and conditions	IEEE Confidential	The intended effective period plus one year.	
Market Share	IEEE Confidential	The date of the data plus two years.	
Competitive Intelligence	IEEE Confidential	The date of the data plus two years.	Some competitive intelligence may merit higher classification.
Product R&D plans and results	IEEE Confidential	The period of the plan plus two years.	
Trade secrets	IEEE Confidential—Controlled Distribution	The expected period of utility.	Consult counsel.
Invention disclosures, patent claims and related materials.	IEEE Confidential—Controlled Distribution	The expected date of patent grant plus two years.	Consult counsel.

A document containing this type of data...	... might be classified at this level for this duration.	Notes
Product Evolution Strategies	IEEE Confidential	The period of the strategy plus two years	
New Business Proposals	IEEE Confidential	The anticipated commencement of the new business plus two years	
Product Business Cases (forecast and actual revenue, expenses, margins)	IEEE Confidential	The period of the plan plus two years	
Sales Analysis and Territory Reviews	IEEE Confidential—Controlled Distribution	The period studied by the analysis or review plus two years.	This is classified highly because it is related to compensation. When that consideration does not apply, the appropriate classification is Confidential
Discussions of Potential Product Policy Changes (e.g. conference and authors' fees)	IEEE Confidential	The intended date of implementation plus two years.	

8.2 Operations Data

Examples of operations data include the following:

A document containing this type of data...	... might be classified at this level for this duration.	Notes
Annual report	Unclassified		
Financial budget and performance data (except for individual compensation)	IEEE Proprietary		
Organization charts and lists	IEEE Proprietary		
IEL (and other product) activity measures	IEEE Confidential	The period of time measured plus two years	

A document containing this type of data...	... might be classified at this level for this duration.	Notes
Information from other parties held in trust	IEEE Confidential	The period of time agreed when accepting the information	In some cases, a higher classification may be appropriate
Operations goals	IEEE Proprietary		In some cases, a higher classification may be appropriate
Executive performance plans	IEEE Confidential—Controlled Distribution	The period of time plus two years	

8.3 Strategic Data

Examples of strategic data include the following:

A document containing this type of data...	... might be classified at this level for this duration.	Notes
Brand strategies	IEEE Confidential	The period of the plan plus two years	
Data of other organizations held under an NDA	IEEE Confidential unless otherwise specified by the NDA	The period of time agreed when accepting the data	In some cases, a higher classification may be appropriate.

8.4 Data regarding Relationships with Other Organizations

Examples of this data include the following:

A document containing this type of data...	... might be classified at this level For this duration.	Notes
Executed Contracts	IEEE Confidential unless otherwise specified in an NDA or contractual provision		Consult IEEE counsel

A document containing this type of data...	... might be classified at this level For this duration.	Notes
Partnership and alliance proposals (e.g., memorandum of understanding (MOU)).	.		There may be antitrust considerations. Consult IEEE counsel.
Mergers and acquisitions			There are considerations of insider trading. Consult IEEE counsel.

8.5 Governance Data

Examples of governance data include the following:

A document containing this type of data...	... might be classified at this level For this duration.	Notes
All except as noted below	IEEE Proprietary		
Documents cleared for public release	Unclassified		
Minutes of meetings (except for executive session)	IEEE Proprietary		
Minutes of executive session (unless reclassified)	IEEE Confidential—Controlled Distribution	Indefinite	See implementation note below
Secret ballots			These should be destroyed immediately after certification.
Consideration of candidates for awards and offices	IEEE Confidential—Controlled Distribution	Indefinite	See implementation note below
Information where distribution is regulated by law	IEEE Confidential—Controlled Distribution	In accordance with law	Consult counsel

8.6 Personnel Data

Personnel data is generally held in databases that are protected in accordance with legal requirements. This section concerns reports produced from those databases as well as personnel-related documents utilized in the everyday course of doing business.

Note that the disclosure of personnel data by Human Resources is a distinct issue. This discussion concerns only the use of personnel-related reports and documents by others.

A document containing this type of data...	... might be classified at this level for this duration.	Notes
Employee name, title; business address, email addresses, and phone numbers	Unclassified		This is intended for the situation of business cards and signature blocks on correspondence.
Position descriptions	IEEE Proprietary		HR may choose to treat some as unclassified, e.g. when advertising a position.
Statistical abstractions and summaries of HR data	IEEE Proprietary		For example, individual salaries are highly classified; average salaries for large groups of employees are not.
Personal and emergency contact information	IEEE Confidential	Indefinite. See implementation note below.	This is the sort of information typically gathered by a department administrative assistant.

A document containing this type of data...	... might be classified at this level for this duration.	Notes
Substantial compilations of proprietary HR data	IEEE Confidential	Indefinite. See implementation note below.	For example, it's OK to publicly disclose that an individual works at IEEE. It's not OK to publish a substantial list of employees.
Compensation (aside from the legal requirements of IRS Form 990)	IEEE Confidential—Controlled Distribution	Indefinite. See implementation note below.	

Implementation note: Holders of such documents should securely dispose of them when their useful period has passed.

8.7 Legal Data

Markings provided by counsel and those corresponding with counsel preempt any other markings. Guidance on dealing with such documents should be obtained from the IEEE Legal and Compliance Department.

9 Authorized Volunteer Leaders (AVLs)

An IEEE member becomes an Authorized Volunteer Leader (AVL) by completing an online training course and acknowledging an understanding of the appropriate handling of IEEE information. Such acknowledgement applies to the individual for a three-year period at which time a refresher online training course will be required.

A list of AVLs will be made available so that it may be consulted prior to sharing information.

Becoming an AVL is a pre-requisite to many volunteer leadership positions. The current list includes individuals serving on the following Boards and Committees or holding the positions as provided below:

- IEEE Board of Directors (BoD)
- IEEE Director-Elects
- Major Boards (Educational Activities Board, Member and Geographic Activities Board, IEEE-USA Board, IEEE Standards Association Board, Publication Services and Products Board, Technical Activities Board)
- Chairs and members of Committees of IEEE
- Conference Treasurers (Financial Interest)
- Annual Election Candidates
- TAB/PSPB Products and Services Committee
- Editors-in-Chief
- Section Chairs
- Section Treasurers
- Society and Council Treasurers
- Designated persons in non-US offices of IEEE
- All other positions, boards, or committees designated by OUs

Any changes to this list shall be reported to the IEEE Legal and Compliance Department.

10 Use Within Organizational Units

The Information Disclosure Policy and procedures implementing that policy apply to all of IEEE. Organizational units of IEEE are not permitted to create their own policies and/or markings. The standard practice of OUs shall be in accordance with this Guide. The terms “Confidential” and “Proprietary” may not be extended to similar organization-specific markings. For example, it is not permissible to mark an item as “Shiny Toys Society Confidential”.

Nevertheless, it is understood and expected that situations arise where IEEE societies or OUs may be engaged in a friendly competition or wish to operate with some level of privacy. In such cases, one might put a marking on a document that says, “Please keep this within the Shiny Toys Society”. Such a label results only in a request and would have no legal basis for enforcement. Otherwise, IEEE’s information disclosure policy is legally enforceable.