IEEE Guide to Classification of Documents

13 May 2016

This guide provides procedures for the implementation of IEEE Policy 9.25, Information Disclosure. The procedures are applicable to all members of the IEEE community, including employees, subcontractors, and volunteer leaders.

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

Preface

The IEEE Governance Committee shall be responsible for the contents and maintenance of this Guide in line with IEEE Policies, Section 9.25, Information Disclosure Policy. Any revisions to the Guide shall be reported to the IEEE Board of Directors.

The latest copy can be downloaded from the IEEE Governing Documents website at http://www.ieee.org/about/corporate/governance/index.html.

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

Table of Contents

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 related to IEEE decision-making, operations, and governance, except as described below	Information that could adversely affect the business operations, privacy commitments, or legal obligations of the IEEE if disclosed	Information that, in accordance with law, bylaws, policies, or procedures must 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	Provided to those on the distribution list. May not be redistributed.
Examples (See § 9)	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 § 4)	Not applicable	Reader	Reader	Distribution list provided by originator
Classification markings (See § 8)	Not applicable	Level, Originator	Level, Originator, Declass date	Level, Originator, Declass date, Distribution list
Protection (See § 3)	Not applicable	None	Locked drawer, delivery tracking	Locked drawer, delivery receipt, encryption
Disposal* (See § 6)	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 § 5)	Not applicable	IEEE members and staff	Executive session	Executive session

* Notes to table:
1. “Available” does not imply that the information is pushed to the parties. “Secure deletion” means that the electronic document is not simply placed in the “recycle bin” of the computer, but is actually deleted. “Normal trash” is meant to suggest that small quantities of proprietary trash may be intermixed with large quantities of other trash. If large quantities are to be discarded, they should be shredded, burned or disposed in a designated secure container.
2. Nothing in these procedures is intended to supersede the provisions of IEEE policies and procedures for Records Retention.

2 What are the key ideas?

2.1 IEEE Policy on Information Disclosure

IEEE policy 9.25 (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.*

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 retrieve more restricted distribution. The purpose of this document is to provide guidance on the application of the IEEE's policy on information disclosure.

2.2 Objectives

IEEE's information disclosure policy has two objectives:

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

It follows from these objectives that the procedures should give everyone—both staff and volunteers—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 in a tension 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 must be mindful of both sets of needs and must 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 sub-organizations, 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 Important Concepts

In order to apply these procedures, it is important to understand a few important concepts.

2.4.1 Document

A "document" is any communication recorded in a form that can be read by a human, regardless of whether the information is recorded on paper or an electronic medium. PowerPoint presentations are examples of documents. An email note is an example of a document. Databases are not necessarily documents, but the reports produced from the database are 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 9.25 - Information Disclosure Policy) to be entrusted with IEEE confidential information. For the purposes of this guide, AVLs and IEEE employees[1] have the same privileges and responsibilities in dealing with IEEE's information.

2.4.3 Levels of Classification

In addition to information that is not classified at all, IEEE has chosen to have two levels of classification: IEEE Proprietary and IEEE Confidential. IEEE Proprietary information is available to any staff member or member of IEEE. IEEE Confidential information is available to AVLs and staff members who have a "need to know". However, some information is subject to stricter controls on distribution. Such information is marked as IEEE Confidential—Controlled Distribution.

2.4.4 Need to Know

This concept is the basis for sharing confidential information inside the IEEE community. If an AVL or a staff member needs 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, any reader of the document judges the "need to know"; in other words, any reader of an IEEE Confidential document may make the judgment that the document should be shared with some other AVL or staff member.

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 is shared, the originator must add the new recipient to the distribution list for the document.

2.4.5 Originators and Readers

The "originator" of a classified document is the person who created the document. If it's 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

[1] It is assumed that IEEE employees (or contractors with similar responsibilities) will have taken training similar to that provided to AVLs and will have entered into an employment agreement or a contractual agreement that provides for the protection of IEEE classified information.

documents marked “IEEE Confidential”, the reader is free to share the document with an AVL or staff member 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 How do I protect IEEE's confidential documents?

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 require no special protection aside from normal care. Obviously, they should not be left unattended in public places, nor should they be provided to persons outside the IEEE community.

Any paper document labeled IEEE Confidential must be stored in a locked container when not in active use. When in use, the document must be in the physical possession of the responsible individual. When traveling, IEEE Confidential documents must be secured in a manner similar to a valuable object, e.g., out of sight in a locked automobile, locked briefcase, hotel safe, etc.

Every employee should be trained that if they see an unattended paper document classified IEEE Confidential, they should immediately take the document, secure it, and report the fact to their supervisor.

If a document labeled IEEE Confidential is to be mailed, it must be mailed via a method that provides a delivery tracking confirmation.

If a document labeled IEEE Confidential—Controlled Distribution is to be mailed, it must be mailed via a method that provides a signed receipt. (Confidential documents require only delivery tracking, a service provided inexpensively by the US Postal Service. Controlled Distribution documents require a signed receipt. This can be accomplished via registered mail or by the optional receipt service of most express delivery services.)

If an electronic document labeled IEEE Confidential—Controlled Distribution is to be stored on an electronic device or transmitted electronically, it must be encrypted except when in actual use. (Note that there are common software packages that include an encryption option.)

4 How do I share IEEE's confidential documents?

4.1 Sharing information inside IEEE

This section deals with the sharing of information inside the IEEE community. The next section addresses sharing with those outside the IEEE.

IEEE Proprietary information can be shared with any IEEE staffer or member.

IEEE Confidential information can be shared with any IEEE staffer or Authorized Volunteer Leader if they have a *need to know*. The person giving the information has the responsibility to determine if the receiver is, in fact, an employee or an Authorized Volunteer Leader. The person giving the information has the responsibility to assess if the receiver has a credible need to know the information in order to conduct their duties and responsibilities.

IEEE Confidential—Controlled Distribution documents may be shared only with those who appear on the distribution list. To share with others, one must seek the agreement of the originator or the originator's superior to modify the distribution list.

4.2 Sharing information outside IEEE

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

5 How do I consider confidential documents in a meeting?

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 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.

To consider documents classified IEEE Confidential or above, it *may* be advisable to enter executive session. According to Robert's Rules of Order, a motion to enter executive session is privileged and is adopted by majority vote. 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.

A typical topic might be described in a Proprietary document with a Confidential supplement. This would permit most issues to be considered in open session.

It should be noted that minutes of an executive session are inherently IEEE Confidential—Controlled Distribution. This is often an undesirable result because it prohibits the distribution of the results of the consideration to persons who may need them. There are several possible remedies for this situation:

- 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 could be classified at a lower level.

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

Now, there is one misconception that must be avoided. 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 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 apply. The minutes are the only product of an Executive Session that are inherently Controlled Distribution.

6 How do I dispose of a confidential document?

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

IEEE Proprietary documents in electronic form may be deleted in the usual manner. Small quantities of proprietary paper documents may be discarded in the normal trash if intermixed with large quantities of other trash. Large quantities of proprietary paper documents should be disposed in the same manner as IEEE Confidential documents.

Greater care is required for the disposal of IEEE Confidential documents. Paper documents should be either shredded or burned, or placed in containers designated for secure disposal.

Electronic documents classified as IEEE Confidential should *not* be deleted in a manner that simply moves them to a "recycle bin". Instead, they should be deleted in a manner that prevents easy recovery of the document. On some computers, one can accomplish this by pressing Shift-Delete. Alternatively, one could delete the document in a normal fashion and then "dump the trash".

Documents classified as IEEE Confidential—Controlled Distribution require greater care in disposal. One straightforward way to delete a paper document is to return it to the originator. This has the benefit of providing evidence that the document was not passed on to others. Alternatively, it could be shredded or burned, or placed in a secure disposal container.

Electronic documents classified as IEEE Confidential—Controlled Distribution should be deleted with a so-called "secure deletion" mechanism. Basically, this is a software program that over-writes the disk space where the document formerly resided.

7 Can a confidential document be reclassified?

As mentioned previously any document classified as IEEE Confidential or above must carry a date for reclassification to Proprietary[2]. Any document lacking a reclassification date will be reclassified automatically one year after its creation.

The Board of Directors or the top deliberative body of any OU or sub-organization 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.)

Supervisors and volunteer leaders should regularly review and, if necessary, change classification decisions made by subordinates, as well as counsel those demonstrating repeated poor judgment.

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

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.

[2] There are some exceptions (described in Section 9) 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.)

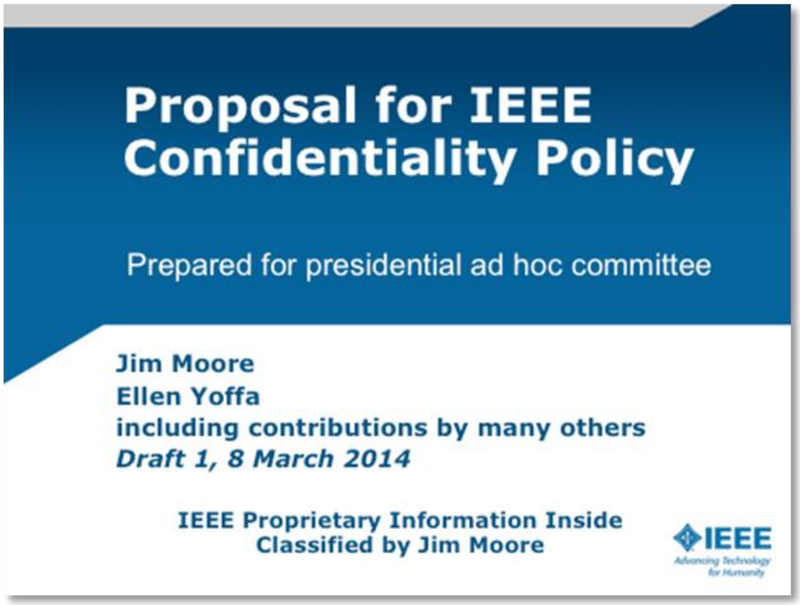
8 How do I create a confidential document?

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 members 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.

Each page of a classified document must be marked with a level appropriate for the information contained in that page. In addition, the cover of the document must show the highest level of any page contained within the document.

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.

For any classified document, that is, IEEE Proprietary or above, the originator must also identify himself or herself on the cover page as the person who selected the classification level. Here's an example cover page for an IEEE Proprietary document.



Proposal for IEEE Confidentiality Policy

Prepared for presidential ad hoc committee

Jim Moore
Ellen Yoffa
including contributions by many others
Draft 1, 8 March 2014

IEEE Proprietary Information Inside
Classified by Jim Moore

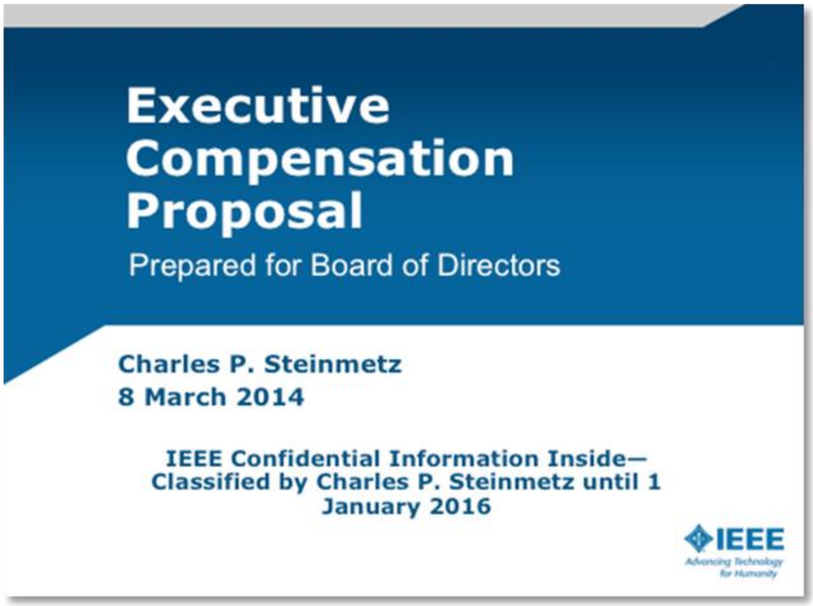
Electronic file names must be prefixed with a confidentiality indicator, e.g. "[IEEEP]", "[IEEEC]", and "[IEEECCD]".

If the document is classified IEEE Confidential or above, the cover page must 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 must include a declassification date and 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."

It is permitted to number copies, apply watermarks, or use steganographic techniques to enforce distribution limitations.

Here's an example cover page for an IEEE Confidential document.



Executive Compensation Proposal

Prepared for Board of Directors

Charles P. Steinmetz
8 March 2014

IEEE Confidential Information Inside—Classified by Charles P. Steinmetz until 1 January 2016

IEEE
Advancing Technology for Humanity

9 What level of classification should I assign?

In determining the classification of a document, one must 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.

9.1 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.
Product Evolution Strategies	IEEE Confidential	The period of the strategy plus two years	

A document containing this type of data…	**… might be classified at this level …**	**… for this duration.**	**Notes**
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.	

9.2 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	

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 Confidential	The period of time plus two years	
Executive performance plans	IEEE Confidential—Controlled Distribution	The period of time plus two years	

9.3 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.

9.4 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**
Partnership and alliance proposals	.		There may be antitrust considerations. Consult IEEE counsel.
Mergers and acquisitions			There are considerations of insider trading. Consult IEEE counsel.

9.5 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

Implementation note: Those who hold copies of Executive Session minutes or materials related to the consideration of candidates for awards or offices should securely dispose of these documents promptly when they are no longer useful. For legal reasons, the Governance Committee may retain an archival copy of the document in accordance with IEEE policies on records retention.

9.6 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.
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.

9.7 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 department.

10 Who is an Authorized Volunteer Leader (AVL)?

An IEEE member becomes an Authorized Volunteer Leader by completing an online course and executing a non-disclosure agreement. The non-disclosure agreement binds the individual in perpetuity. However, because each confidential document has a declassification date or a requirement to destroy when no longer useful, one can discharge the responsibility by destroying all classified documents in a secure manner or by waiting for their classification to expire.

A list of AVLs will be provided 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)
- 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 & Technical Program Chairs
- Conference Treasurers (Financial Interest)
- Annual Election Candidates
- TAB/PSPB PSC
- Editors-in-Chief
- Designated persons in non-US offices of IEEE
- Any other positions, boards, or committees designated by OUs

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

11 May an OU or other sub-organization create its own policy?

The information disclosure policy and the procedures implementing that policy apply to all of IEEE. Sub-organizations of IEEE are not permitted to create their own policies and/or markings. The terms “Confidential” and “Proprietary” may not be used for organization-specific markings. For example, it is not permissible to mark an item as “Shiny Toys Society Confidential”.

Keep in mind that IEEE’s information disclosure policy is legally enforceable. That’s why it must be distinguished from measures that rely on simple peer pressure for enforcement.

Nevertheless, it is understood that situations arise where IEEE societies or OUs are engaged in a friendly competition and 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”. That restriction might be enforced by peer pressure but would have no legal basis for enforcement.