Policy Number TA 2-100

Application: Worldwide Strategic Business Units and Subsidiaries

SUBJECT: PROTECTION OF COMPANY INFORMATION

GENERAL

The purpose of this policy statement is to ensure the protection of proprietary and confidential Company information from loss, misuse or misappropriation. The terms, proprietary and confidential, refer to certain information which if lost or misused could adversely affect Company operations, employees, customers or stockholders. Such information may contain financial, commercial or technical data, or may relate to payroll, benefits or personnel records, etc.

POLICY

Proprietary and confidential information may be found in various forms of Company data; therefore, all personnel are responsible for exercising appropriate care, custody and control of Company correspondence, reports, files, drawings, photographs, films, and electronically recorded data or images.

The management of Tenneco and each of its strategic business units and subsidiary companies is responsible for establishing and maintaining written guidelines for the appropriate degree of care, custody and control of printed, photographic or electronically recorded information, whether Company-owned or owned by others who have entrusted their information to the Company.

PROCEDURE

The Tenneco Protection of Confidential Information policy/procedure is included below. In the absence of a strategic business unit or subsidiary procedure implementing more stringent protection, or designed to facilitate information security in a unique operating environment, the Tenneco Protection of Confidential Information policy/procedure serves as the minimum level of information protection required at each of the Company’s strategic business units and subsidiaries.
TENNECO PROTECTION OF CONFIDENTIAL INFORMATION

GENERAL

Company information includes all information concerning Tenneco’s affairs which is not in the public domain and has not been approved by Tenneco for release outside the Company. It includes information developed by employees and may include information received from sources outside the Company.

This policy/procedure establishes a confidential classification for all forms of Company information; however, the procedures below address the handling of such information only when it is in document form.

NOTE: For information concerning computer-based data, electronic media, personal computers, personal computer software and EDP workstations, see the Electronic Media section of this manual. Further policy guidance regarding the handling or use of electronic data also is set forth in the IT Policy Manual. That manual may be accessed through the Lotus Notes menu by clicking on the IT Policy Manual icon.

Confidential information is proprietary or sensitive information pertaining to personnel matters, salaries, or benefits; financial, strategic commercial or technical data; employees, customers or stockholders; information owned by others who have entrusted their information to the Company; or any other information which if lost or misused would adversely affect the Company or others.

Confidential information should be made available only to individuals who have the need to know.

Company information which requires special protection is to be classified as confidential. Such classification of Company information is the responsibility of its originator. The originator should exercise good judgment in designating information as confidential, since overuse of this classification may destroy its effectiveness. **Confidential envelopes should be used only for transmitting confidential information.**

Company information which is not confidential is unclassified. Unclassified information is not particularly sensitive, covered by a secrecy agreement or required to be legally reported by the Company as confidential.

PROCEDURE

Use

Confidential information should only be used for the benefit of the Company. Confidential information of a third party and which has been
disclosed to the Company should be treated in the same manner as the Company’s own confidential information and should only be used for purposes permitted by the third party.

**Transmission**

Confidential documents, when transmitted outside of controlled access office areas or secured plant facilities, are to be put in envelopes marked confidential and transmitted to the addressee, for opening only by the addressee, or his or her designee.

The sender of a confidential envelope must be sure the envelope bears the originator’s name.

**Receipt**

Confidential envelopes are to be opened only by the addressee, or his or her designee.

If the addressee (or his or her designee) to whom an envelope marked confidential is not available within a reasonable time to open the envelope, and no other individual has been given authorization to open the addressee’s confidential correspondence, the envelope should be returned to the originator, with an explanation of the reason it is being returned.

**Safekeeping**

Confidential information should be kept in locked desks, file cabinets or offices, except when in use; or kept in office areas or secured plant facilities where access is granted only to the specific individual(s) who have the need to know the information.

Caution should be exercised to avoid such document being visible to others unless those others have a need to know the contents of such documents.

Copies of confidential information should be minimized and treated as confidentially as the original of the document.

**Disposal**

Confidential documents are to be destroyed by hand or machine shredding, when the document quantity is small. When the document quantity is large, contact the Law Department regarding disposal.

**Reporting**
Any unauthorized use or disclosure of confidential information should be reported to the Law Department.