| | | | |
|---|---|---|---|
| **Section Name:** | CORPORATE POLICICES – LAW | **Date:** | 04/12 |
| **Section No:** | 7 | **Supersedes:** | 08/98 |
| **Policy No:** | 7.13 | | |
| **Subject** | PROTECTION OF CONFIDENTIAL AND PROPRIETARY INFORMATION | | |

It is critically important to the Company's continued success that all reasonable precautions be taken to maintain the security of Company confidential information, as well as that of others which the Company has accepted in confidence. The value of such information depends upon the degree to which we are successful in maintaining its secrecy.

Confidential information encompasses both technical and non-technical trade secrets, including any non-public information of potential use or value to a competitor, customer or supplier. Such information, including financial information concerning individual Company units, divisions or groups, shall not be disclosed outside the Company except in accordance with the procedure described below.

## PROCEDURE

1. No Company unit or employee shall disclose or permit a third party to obtain access to Company confidential information, nor shall any Company unit or employee accept, or agree to accept, any information from any third party which that third party asserts is confidential or proprietary to himself or itself or which the Company unit or employee reasonably believes is confidential or proprietary to any third party, without a written agreement between the Company and such third party in a form approved by the Law Department.
2. Unit managers shall:
   - Implement adequate procedures to protect confidential information (see Exhibit 7.13, paragraph A).
   - Adopt appropriate physical security measures (see Exhibit 7.13, paragraph B).
   - Adopt appropriate general security measures in order to protect confidential information (see Exhibit 7.13, paragraph C).
   - Adopt employee security measures (see Exhibit 7.13, paragraph D).
   - Enforce access control practices and procedures designed and implemented by the Company's Information Technology Department.
3. The Company's Information Technology Department shall design, implement and maintain access control practices and procedures to safeguard electronically stored information.
4. From time to time, units, divisions and groups are requested to supply certain individuals, government agencies or other organizations with financial statements or other financial information for their respective units, divisions, or groups (see also Corporate Policy No. 7.8, Response to Government Investigations). Since the public (including competitors, customers, suppliers, other government offices, etc.) may be able to access such information through "freedom of information" legislation, such disclosures may not be in the Company's best interest. Accordingly, the Company only provides the requesting parties with consolidated financial statements (e.g., Annual and Quarterly Reports). Any exceptions must be approved by the Law Department.

5. New products and products in development represent a particularly vulnerable area for the Company, and disclosure of information concerning new products should be especially carefully protected. Unit managers shall observe the following precautions in dealing with new product secrets :

   - Obtain in advance a written confidentiality agreement in a form approved by the Law Department from those attending the demonstration or exhibition of a product or device that is still being developed.
   - Delay any public disclosure or offer for sale until any proprietary technology has been protected, if appropriate, by a patent filing.
   - Conduct all field trials on a "not-for-sale" basis, under the protection of a confidential, field-test agreement in a form approved by the Law Department.
   - Control all information on a confidential ("need-to-know") basis.

**Updates:**
Risk Management & Corporate Compliance
Law Department

**References:**
*Safeguarding Our Confidential Information* brochure & *Information Security Checklist* (available from the Law Department) and database
*Protecting Our Trade Secrets* brochure (available from the Law Department)
Corporate Principle:
1.2, Employee Responsibility Concerning Assets
Corporate Policies:
2.14, Agreements - U.S. Employees
3.4, Internal Controls
4.3, Protection of Company Property and Operations
5.4, Information Systems Controls
6.3, Financial Public Relations and Disclosure
7.2, Contract Review, Approval and Signature
7.4, Protecting Communications with Counsel
7.8, Response to Government Investigations
7.14, Access to Data Management and Communication Systems
7.16, Patents
7.19, Records Retention and Protection

## EXHIBIT NUMBER 7.13

Protection of Confidential and Proprietary Information
(Reference: Paragraph 2 of Policy 7.13)

A. Procedures to protect confidential information :

- Undertake an "information audit" to determine what information should be protected (see the Protecting Our Trade Secrets brochure available from Risk Management/Corporate Compliance department).
- Identify where such information is located (i.e., its physical and geographic location and the identity of persons who have such information or access to it (physically and electronically)).
- Establish employee education and controls to prevent unauthorized access to, dissemination or use of such confidential information.

- Ensure that financial and other employees refer to the Chief Financial Officer any requests from outside the Company for unit, division or group financial statements or other financial information (see Corporate Policy 6.3, Financial Public Relations and Disclosure).
- Enforce access control practices and procedures designed and implemented by the Company's Information Technology Department.

B. Physical security measures:

- Fences, gates, or other physical restraints to prevent unauthorized entry
- Guards or electronic controls restricting entry to sensitive areas, and keeping a record of persons entering and exiting the premises
- Physical barriers around secret devices or processes to prevent viewing by customers, suppliers, the public, and other employees who do not have a "need to know"
- Keep confidential data and documents in locked files, restrict access to those files to employees with a "need to know," place the files in supervised areas, require that files be used in a protected area, or require that they be signed out before removal.

C. Electronic security measures.

- The Company's Information Technology Department shall design, implement and maintain access control practices and procedures to safeguard electronically stored information. Such practices and procedures shall include measures effective to prevent third party access to Company systems and electronically stored information and to ensure that users with access to systems and information have access only to information they have a "need to know."

D. General security measures:

- Identify what is confidential and what may not be used or disclosed by placing confidentiality stamps and/or notices on documents containing confidential information. Signs should also be used in the vicinity of proprietary devices or processes.
- Require signed confidentiality agreements of all visitors.
- Escort visitors through Company premises.
- Control disposition of all confidential documents -- e.g., by onsite shredding.
- Lock up notebooks, data and other manuals at night, limiting the distribution and number of copies of those documents, and restricting physical access to research materials and instruments.
- Ensure that confidentiality agreements are obtained from all third parties who are provided with access to confidential information.
- Physically disperse the steps in a proprietary process (so that few individuals are aware of the entire process).
- Ensure that any documentation relating to Company trade secrets (e.g., operating or training manuals) which is licensed or loaned to the customer, is distributed with appropriate legal restrictions on use or disclosure.
- When traveling, never place confidential documents or laptop computers in checked baggage on airlines, and always place laptops and company documents in the trunk/boot of your vehicle if you must keep such items in the vehicle when parked.

E. Employee security measures:

- Ensure that all employees sign the applicable employment agreements.
- Advise employees what is considered confidential upon commencement of employment, and update this education annually. Distribute the Safeguarding Our Confidential Information brochure and Information Security Checklist (available from Risk Management/Corporate Compliance department) to employees with this training.
- Restrict employee access to areas where sensitive processes or information is located.
- Require employees to document R&D development.
- Require that technical staff advise sales and marketing personnel of restrictions on communication of confidential product information.
- Direct employees to report attempts by any unauthorized person to obtain proprietary information.
- Exclude disaffected or terminating employees from access to sensitive or proprietary or confidential information, or any materials that may be of use to a competitor.

**Related Topics**

| Section Name | Policy No | Subject |
|---|---|---|
| CORPORATE POLICIES – COMMUNICATIONS | 6.3 | Financial Public Relations and Disclosure |
| CORPORATE POLICIES – EMPLOYEES | 2.14 | Agreements – U.S. Employees |
| CORPORATE POLICIES – FINANCE | 5.4 | Information Systems Controls |
| CORPORATE POLICIES – LAW | 7.14 | Data Management and Communications Systems |
| CORPORATE POLICIES – LAW | 7.21 | Records Retention and Protection |
| CORPORATE POLICIES – LAW | 7.2 | Contract Review, Approval and Signature |
| CORPORATE POLICIES – LAW | 7.4 | Protecting Communications with Counsel |
| CORPORATE POLICIES – LAW | 7.8 | Response to Government Investigations |
| CORPORATE POLICIES – MANAGEMENT | 3.4 | Internal Control |
| CORPORATE POLICIES – OPERATIONS | 4.3 | Protection of Company Property and Operations |
| CORPORATE PRINCIPLES | 1.2 | Employee Responsibility Concerning Assets |