NELSON SLOSBERGAS P.A.

1110 BRICKELL AVENUE, SUITE 310
MIAMI, FLORIDA 33131
E-MAIL ADDRESS: NELSON@MIAMI-INTL-LAW.COM
WWW.MIAMI-INTL-LAW.COM

(305) 374-0030
FAX: (305) 374-2855

INTERNAL STEPS TO PRESERVE CONFIDENTIALITY, TRADE SECRETS, AND OWNERSHIP RIGHTS TO WORK PRODUCTS

A number of safeguards can be implemented to protect trade secrets. Some are computer-based, and others take the form of company policies and employment practices. While the combination of steps necessary to meet the Act's standard of reasonableness will necessarily vary with the circumstances of particular businesses, many recent cases suggest that a simple confidentiality agreement, by itself, is insufficient. A combination of some or all of the following procedures is advisable:

* Trade secret acknowledgment and non-disclosure agreements signed by all new employees when hired. Such agreements should refer to specific categories of trade secrets rather than to confidential information generally; specific categories may include customer lists, formulas, technical drawings and plans, and security process and methods.

* Non-competition covenants and Assignment of Inventions agreements signed by employees.

* Preparation of a Statement of Trade Secret Security Program and circulation to all employees, with written acknowledgment of receipt.

* Requirement of preservation and non-disclosure of trade secrets in employee manual or handbook.

* Creation and regular updating of a trade secret register.

* Access to trade secrets given only on a need-to-know basis.

* Labeling of all materials containing trade secrets.

* Internal transmission of confidential materials only in sealed envelope marked "Confidential," or in property labeled envelope within another envelope bearing no special legend.

* External transmission in envelope that is addressed and sealed but not marked "Confidential" in any way.

* Electronic transmission, internally or externally, only across secure pathways.

* Issuance of computer passwords or identification codes to restrict access by unauthorized personnel and prohibition of leaving computer terminal or desktop computer unattended while signed on to any database or program.

* Storage of confidential data and materials in suitable locked cabinets, desks or rooms; nighttime security checks for materials left unsecured.

* Where appropriate, use of identification badges, security guards or closed circuit television monitors.

* Document or computer tape/disk destruction policy, including prohibition on discarding confidential material in open waste containers.

* Exit interviews with terminating employees to emphasize non-disclosure of confidential information, and signing of additional non-disclosure form.