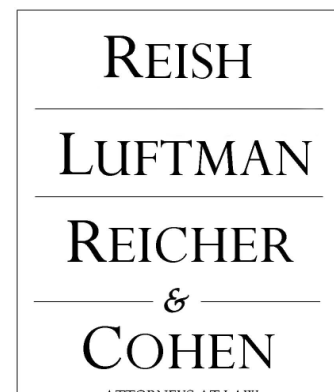


**MARK E. TERMAN, ESQ.**

MarkTerman@Reish.com



**Technology and Privacy in  
Today's Workplace: Protecting  
Confidentiality and Trade Secrets**

**PRESENTED TO**

**UCLA Extension Class  
Information Systems and Network Security**

**November 29, 2005 – Los Angeles, California**

**Copyright 2005  
Reish Luftman Reicher & Cohen**

**Mark Terman** is a partner with Reish Luftman Reicher & Cohen where he heads the firm’s Employment Law Practice Group. He counsels employers in claim prevention, hiring, policy, crisis, and discipline and termination matters, and represents them in federal and state court, arbitration and government proceedings. Mr. Terman’s employment litigation experience extends to wrongful termination, discrimination and sexual harassment, trade secret, fraud and other business torts. He is general counsel for the UCLA Alumni Association and is a member of its Board of Directors, and a former member of the Board of Directors of the Children’s Nature Institute.

Mr. Terman served as a Superior Court appointed arbitrator in some 25 cases. His peers selected him as a 2004, 2005, and 2006 California “Super Lawyer”, in which some 65,000 California lawyers were polled for each year. Mr. Terman speaks to and writes for client and industry groups on litigation avoidance and management, wage and hour issues, trade secret protection, and avoiding sexual harassment, among other employment law topics.

Mr. Terman earned his juris doctorate in 1983 from Loyola Law School, where he served on the Law Review. In August 1986, he attended Hasting College of Law as an attorney for jury trial training. He earned his bachelor’s degree in 1979 from University of California at Los Angeles.

Please see [www.reish.com](http://www.reish.com).

## Contents

I. Technology and Privacy in the Workplace .....	3
II. Competition and Trade Secrets .....	10
III. Appendix.....	13

## **I. Technology and Privacy in the Workplace**

### **A. How We Work Today vs. 5 or 10 Years Ago.**

1. Computers, e-mail, Internet, voice-mail are essential business tools.

### **B. Challenges for Employers**

1. Right to manage workplace.
2. Protect property and information of employer and its clients.
3. Protect employees.
4. Aid employer investigations.
5. Employee productivity.
6. Evidence.

### **C. Employer Monitoring of Employee Communications.**

1. American Management Association 2005 Electronic Monitoring and Surveillance Survey. See, <http://www.amanet.org/research/>
  - a. 526 U.S. companies responded (22% with more than 5000 employees; 7% with 2,501 to 5,000; 13% with 1,001 to 2,500; 10% with 501 to 101; and 25% with 100 or less).
  - b. Employer monitoring of employees' telephone calls, e-mail, internet connections, and/or computer files is about twice as much as reported in AMA's 1997 survey.
  - c. (X) What is monitored? (Y) Written policies inform employees?

	(X)	(Y)
i. Website connections/surfing	76%	89%
ii. E-mail	55%	34%
iii. Video for security	51%	80%
iv. Video for performance	10%	85%
v. Keystrokes, content, time	36%	80%
vi. Computer files	50%	82%
vii. Phone time phone/numbers	51%	78%
viii. Record calls (selected positions	19%	86%
ix. Voice-mail	15%	76%
x. GPS phones	5%	
xi. GPS vehicles	8%	
xii. GPS ID/Smart cards	8%	

- d. Monitoring purposes include: security, violence, legal risk management, productivity, performance reviews and training, legal compliance.
  - e. 65% use software to block connections to inappropriate websites.
  - f. 26% have terminated employees for misuse of the Internet; 25% have terminated employees for e-mail misuse.
  - g. 20% have been ordered by a court or regulatory body to produce e-mail vs. 9% in 2001.
2. American Society for Industrial Security Survey (325 U.S. based companies responding).
- a. Known/reported information piracy jumped 323% between 1992 and 1995.
  - b. Estimated loss to U.S. industry at \$2 billion a month from corporate security breaches.
  - c. Three-fourths of the incidents involved company insiders -- insiders are not just officers and employees. Insiders also include independent contractors, vendors and consultants.

**D. Legal Framework -- Employee Privacy Rights Balanced Against Employer's Need to Know.**

- 1. Constitutional Law.
  - a. Federal Constitution -- Only government employees have a reasonable expectation of privacy at work.
  - b. California Constitution -- All employees have a right to privacy; however, the courts must balance:
    - i. The employee's reasonable expectation of privacy at work against the employer's need to regulate the conduct of its employees and protect them at work; and
    - ii. Whether less intrusive means can accomplish the employer's legitimate objectives.
- 2. Common Law Privacy Rights. -- E.g., unreasonable intrusion upon seclusion, public disclosure of private facts, false light privacy, appropriation of name and likeness.
- 3. Contracts. -- Employer policies that certain information will be kept confidential or used for limited purposes. E.g., Employment agreements,

non-disclosure and confidentiality agreements, collective bargaining agreements, and employee handbooks.

4. Statutes. -- Transit vs. Storage.

- a. *California Privacy Act (Cal. Penal Code § 631, et. seq.)* prohibits eavesdropping and recording of confidential communications by means of an electronic amplifying or recording device.
  - i. Prohibits listening in on a phone call unless all parties consent.
  - ii. Has not been held to by the court to restrict employer access to gather information recorded on its own computers, e-mail, voice mail systems.
- b. *Federal Electronic Communications Privacy Act (18 USC § 2510, et seq.)*. Employers who provide the communications service (i.e., computers and phones) are exempt from the Act's prohibition of unauthorized access to or retrieval of electronic communication while it is in storage.
- c. The federal *Wiretap Act* and *Patriot Act* do not prevent the employer from access to stored email, data and voicemail either.

**E. How the Courts are Balancing Competing Employer and Employee Interests.**

1. Legitimate work related reasons for monitoring or search.
2. Employers need to know increases with severity of alleged misconduct.
3. Employer's published policies will usually defeat an employee's expectation of privacy.

**F. Employer's Written Technology and Internet Policy.**

1. Why employers should have one.
  - a. Not required by law; but, probably will be soon.
  - b. Deterrence of misconduct.
  - c. Public relations with employees.
  - d. Will give employer the best defense against a claim of invasion of privacy.

2. Key elements.

- a. The computers and everything on the system - files and software are the employer's property.
- b. Use is permitted for work purposes only or personal use is limited purposes/times.
- c. Employer's right to inspect and monitor at any time and employee's passwords do not ensure privacy and employers can override the passwords.
- d. No reasonable expectation of privacy when using employer owned equipment.
- e. The policy against discrimination and sexual harassment applies – no defamatory, profane, obscene, discriminatory or harassing materials are to be sent or received.
- f. Treat e-mail as if it is a permanent record – think about the contents before it is sent.
- g. Confidential, proprietary or trade secret information should not be sent unless necessary to carry out the employer's business.
- h. Violation of policy will lead to serious discipline up to and including termination
- i. See *TBG Ins. Services Corp. v. Superior Court*, 96 Cal.App.4th 443 (2002) (upholding employer's right to terminate employee for using employer-supplied home computer for access to pornographic websites. Employee had signed employer's "electronic and telephone equipment policy statement" which diminished the employee's expectation of privacy).

The employers' policy stated explicitly:

- The company's computers are to be used solely for company business;
- The company reserves the right to monitor the employee's use of company computers, including but not limited to the employee's use of the Internet and e-mail;
- The company keeps copies of all computer passwords and the existence of such passwords does not guarantee the confidentiality of any electronic communications;

- The transmission of any discriminatory, offensive or unprofessional messages is strictly prohibited;
- Access to any discriminatory or offensive Internet sites is strictly prohibited; and
- Employees are prohibited from using company equipment to post personal opinions on the Internet, especially if the opinion is discriminatory, political or offensive in nature.

*Id.* at 451-52.

3. Sample at Appendix 2.
4. Train management and employees.

**G. Electronic Data in Litigation**

1. Includes e-mail, voicemail, video mail, word processing, groupware systems, spreadsheets, databases, CAD, websites, and security systems.
2. Discovery of electronic evidence in litigation is becoming more common, not just in high-profile cases.
3. Some attributes of electronic evidence.
  - a. Much more of it than paper documents and files.
  - b. E-mail volume and candor.
  - c. More opportunity to find a “smoking gun.”
  - d. Prior consistent or inconsistent versions and drafts.
  - e. Date/time stamps versions, record creation, edit and access.
  - f. The delete button does not mean it’s gone forever.
    - i. Electronic information and versions are stored in multiple places inside and outside company walls.
    - ii. Information thought to be deleted or lost can often be retrieved by experts.
4. Shield and Sword – a litigant can oppress and be oppressed with the time and expense of electronic discovery.
5. Record Management.
  - a. Retention policies must include all forms of electronic information.

- b. Ensure that delete means delete in appropriate cases.
- c. Every business will be hit with a discovery request or subpoena that includes electronic records - be prepared.
- d. Litigation risks from not suspending routine record destruction policy when info is relevant to imminent or pending litigation.
  - i. *California Evidence Code* § 413 permits the trier of fact to consider a party's "willful suppression of evidence," when it determines "what inferences to draw from the evidence or facts in the case against a party."
  - ii. Standard "BAJI" jury instruction No. 2.03 (8th ed. 2001 Revision) permits the jury to "consider the fact that a party willfully suppressed, altered, damaged, concealed, or destroyed evidence to prevent its being presented in this trial when determining what inferences to draw from the evidence."
  - iii. Trial courts may adapt the instruction "to fit the circumstances of the case, including the egregiousness of the spoliation and the strength and nature of the inference arising from the spoliation" *Cedars-Sinai Med. Ctr. v. Superior Ct.* (1998) 18 Cal. 4th 1.12.
  - iv. *California Code of Civil Procedure* § 2023 (h) permits courts to impose various sanctions "against anyone engaging in conduct that is a misuse of the discovery process," including:
    - (1) A monetary sanction;
    - (2) An issue sanction ordering that designated facts shall be taken as established in the action in accordance with the adversely affected party's claim.
- e. Courts base decisions regarding the wrongfulness of evidence destruction on the "temporal proximity between the destruction and the litigation interference and the foreseeability of the harm to the nonspoliating litigant resulting from the destruction" *Willard v. Caterpillar, Inc.*, (1995) 40 Cal. App. 4th 892. 922-923.
- f. A party guilty of intentionally destroying relevant evidence can be subjected to criminal prosecution with maximum punishment of six months in jail and \$1,000 fine. *California Penal Code* § 135.

- g. The existence of a routine document retention policy can influence whether a court gives the jury an adverse inference instruction when a company destroys potentially relevant evidence pursuant to the policy. Several factors are relevant to that inquiry. *Willard v. Caterpillar, Inc.* (1995) 40 Cal. App. 4th 892, 922-923:
  - i. Whether the policy's retention times were reasonable, considering the facts and circumstances surrounding the relevant documents;
  - ii. Whether the policy was instituted in bad faith;
  - iii. Whether lawsuits concerning a complaint or related complaints have been filed; and
  - iv. The frequency and magnitude of such complaints.
- h. Document Retention Policies.
  - i. Actually involve the routine destruction of documents.
  - ii. Establish reasonable timetables for retaining documents before destruction based on legal and practical.
  - iii. Must be written, widely disseminated and known by employees, and regularly enforced.
  - iv. If properly followed, can shield a company from negative inferences or defaults due to destruction of documents.
  - v. If the party knows or should know that particular documents will become material at some point in the future, such documents should be preserved. (e.g., documents related to "complaints" should be retained for a longer period because of the potential for litigation, relevant to the documents).

## II. Competition and Trade Secrets

- A. **General Rule Re Covenants Not to Compete.** “Every contract by which anyone is restrained from engaging in a lawful trade or business of any kind is to that extent void.” *Cal. Bus. & Prof.Code* §16600.
- B. **Statutory Exceptions.**
1. Employee of a Corporation. Sale of goodwill of the business, all of the stockholder's stock, or substantially all assets of a corporation. *Cal. Bus.& Prof.Code* §16601.
  2. Employee of a Partnership. Sale of partnership interest or dissolution of the partnership. *Cal. Bus. & Prof. Code* §16602.
  3. Must be reasonable under the circumstances of each case. Geographic scope, duration of covenant, and activities precluded.
  4. Covenant is strictly construed. Courts will not enforce “sham covenants.”
- C. **Case Law Exceptions.** Partial restraints which limit, but do not preclude competitive activities or employment, may be enforceable. Employer generally cannot preclude employee from working for a competitor, but may limit how that employee may compete.
1. Confidentiality agreements prohibiting unauthorized disclosure or use of confidential and proprietary information or trade secrets.
    - a. Public policy protects:
      - i. Legitimate trade secrets of the employer.
      - ii. Employee's right to earn a living in his or her business, trade or profession.
    - b. Important provisions: (1) an identification, at least by category, of the information the company claims to be confidential and proprietary; and (2) the employee's acknowledgment of the company's designation of its trade secrets, the employer's effort to assemble the information, and the economic value of ensuring that the information is not known outside the company.
    - c. California's enactment of the Uniform Trade Secrets Act defines a “trade secret” as: Information, including a formula, pattern, compilation, program, device, method, technique or process that: (a) Derives actual or potential economic value from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. *Cal. Civil Code* §3426, et seq.

- d. Examples of confidential and proprietary information that may be a trade secret: research and development of new products, marketing and business plans, customer lists, pricing research and strategies, sales sources and other data, and manufacturing processes. This work product may not yet be developed fully enough to warrant patent or copyright protection.
  - e. Customer list cases are among the most common.
  - f. Trade secret protection programs.
2. Covenants prohibiting solicitation of customers. [But note, mailing announcements of new employment or business affiliation without asking for business is permissible because it is not a “solicitation.”]
  3. Covenants prohibiting “employee raiding.”
  4. Covenants limiting employee's preparations for a competing business while still employed. Similar to employee's fiduciary duty of loyalty to employer.
  5. Covenants prohibiting only a limited or small part of a business, trade or profession, but not all business activities.
  6. Why use agreements if the unfair competition and other laws may already provide a remedy for such conduct?
    - a. Deterrence before the conduct occurs.
    - b. Evidence after the conduct occurs.
  7. Should be signed as a condition of initial employment. Post employment issues - consideration.
  8. Do not include a covenant not to compete in agreements with non-owner employees – it may invalidate the entire agreement.
  9. Stock Option Agreements:
    - a. “bad boy” clause
    - b. non-compete provisions -- federal or state court?
  10. Personal Service Contracts.
    - a. Special, unique, unusual, extraordinary or intellectual character that gives the employee “peculiar value”.
    - b. Generally limited to “one-of-a-kind” entertainers.

11. Post-termination consulting agreements.

**D. Key Steps to Develop a Trade Secret Protection Program.**

1. Identify “real” trade secrets and their value.
  - a. Evaluate confidential and proprietary information and answer two questions: (1) What information, if taken by a competitor, could damage or destroy your business? and (2) How much money has or will the company spend to develop this information?
2. Identify and place legend key documents.
  - a. Mark key documents containing trade secrets with legend: “TRADE SECRET. This document contains confidential and proprietary information of QRS, Inc. Do not copy or circulate.”
  - b. Avoid dilution of protection and loss of credibility by stamping as “confidential” documents that are clearly not confidential.
3. Pre-hire investigation of criminal and employment history and other information, subject to applicable law governing such inquiry.
4. Use confidentiality/trade secret agreements with every employee whose duties bring them into contact with trade secrets. (See, Appendix 3).
5. Restrict access to those who need to know.
6. Update the employee handbook. (See, Appendix 1-2).
  - a. State company policy and deterrence; grounds for termination of employment, civil action and criminal prosecution.
  - b. Limit employees' expectation of privacy in their use of the company's telephones, computers, and work areas.
7. Update computer security. Use a computer consultant who first signs a confidentiality agreement.
8. Document controls. Examples: locked and/or guarded single depository, sign-in and sign-out procedure, access limited to those who need to know, limit or restrict photocopies, shred discarded confidential documents, limit faxes.
9. Consider other security measures. Examples: security guards, logbook of all persons entering or leaving the company's premises, briefcases and handbags subject to inspection by exit guards.
10. Effective exit interview procedures to remind departing employees of confidentiality. (See, Appendix 4).

- a. Consider use of acknowledgment of prior and continuing confidentiality obligations; a severance benefit may be useful to obtain employee's signature.
  - b. Require return of company equipment and documents.
11. Include independent contractors and other outsiders as part of the program.
12. Sue to enforce employer's confidentiality rights. Deterrence and credibility issues.

### **III. Appendix**

#### **APPENDIX 1 – SAMPLE CONFIDENTIALITY POLICY**

##### **CONFIDENTIALITY**

Information about [Company Name], its Employees, customers, suppliers, and vendors is to be kept confidential and divulged only to individuals within the Company with both a need to receive and authorization to receive the information. If in doubt as to whether information should be divulged, err in favor of not divulging information and discuss the situation with your Manager.

All records and files maintained by the Company are confidential and remain the property of the Company. Records and files are not to be disclosed to any outside party without the express permission of the [appropriate management]. Confidential information includes, but is in no way limited to: financial records; business, marketing, and strategic plans; personnel and payroll records regarding current and former Employees; the identity of, contact information for, and any other account information on customers, vendors, and suppliers; inventions, programs, trade secrets, formulas, techniques, and processes; and any other documents or information regarding the Company's operations, procedures, or practices. Confidential information may not be removed from Company premises without express authorization.

Confidential information obtained during or through employment with the Company may not be used by any Employee for the purpose of furthering current or future outside employment or activities or for obtaining personal gain or profit. The Company reserves the right to avail itself of all legal or equitable remedies to prevent impermissible use of confidential information or to recover damages incurred as a result of the impermissible use of confidential information.

Employees may be required to enter into written confidentiality agreements confirming their understanding of the Company's confidentiality policies.

## **APPENDIX 2 – SAMPLE TECHNOLOGY/INTERNET POLICY**

### **USE OF TECHNOLOGY AND THE INTERNET**

The Company's technical resources--including desktop and portable computer systems, fax machines, voice mail, electronic mail (e-mail), Internet and World Wide Web access, electronic bulletin boards, and its intranet--enable Employees quickly and efficiently to access and exchange information throughout the Company and around the world. When used properly, we believe these resources greatly enhance Employee productivity and knowledge. In many respects, these new tools are similar to other Company tools, such as stationery, file cabinets, photocopiers, and telephones. Because these technologies are both new and rapidly changing, it is important to explain how they fit within the Company and within your responsibilities as an Employee.

This policy applies to all technical resources that are owned or leased by the Company, that are used on or accessed from Company premises, or that are used on Company business. This policy also applies to all activities using any Company-paid accounts, subscriptions, or other technical services, such as Internet and World Wide Web access, voice mail, and e-mail, whether or not the activities are conducted from Company premises.

NOTE: As you use the Company's technical resources, it is important to remember the nature of the information created and stored there. Because they seem informal, e-mail messages are sometimes offhand, like a conversation, and not as carefully thought out as a letter or memorandum. Like any other document, an e-mail message or other computer information can later be used to indicate what an Employee knew or felt. You should keep this in mind when creating e-mail messages and other documents. Even after you delete an e-mail message or close a computer session, it may still be recoverable and may even remain on the system.

#### **1. Acceptable Uses**

The Company's technical resources are provided for the benefit of the Company and its customers, vendors, and suppliers. These resources are provided for use in the pursuit of Company business and are to be reviewed, monitored, and used only in that pursuit, except as otherwise provided in this policy.

Employees are otherwise permitted to use the Company's technical resources for occasional, non-work purposes with permission from their direct Manager. Nevertheless, Employees have no right of privacy as to any information or file maintained in or on the Company's property or transmitted or stored through the Company's computer, voice mail, e-mail, or telephone systems.

#### **2. Unacceptable Uses**

The Company's technical resources should not be used for personal gain or the advancement of individual views. Employees who wish to express personal opinions on the Internet are encouraged to obtain a personal account with a commercial Internet service provider and to access the Internet without using Company resources.

Solicitation for any non-Company business or activities using Company resources is strictly prohibited. Your use of the Company's technical resources must not interfere with your

productivity, the productivity of any other Employee, or the operation of the Company's technical resources. Employees may not play games on the Company's technical resources.

You should not send e-mail or other communications that either mask your identity or indicate that they were sent by someone else. You should never access any technical resources using another Employee's password. Similarly, you should only access the libraries, files, data, programs, and directories that are related to your work duties. Unauthorized review, duplication, dissemination, removal, installation, damage, or alteration of files, passwords, computer systems or programs, or other property of the Company, or improper use of information obtained by unauthorized means, is prohibited.

Sending, saving, or viewing offensive material is prohibited. Messages stored and/or transmitted by computer, voice mail, e-mail, or telephone systems must not contain content that may reasonably be considered offensive to any Employee. Offensive material includes, but is not limited to, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend someone on the basis of his or her race, color, creed, sex, age, national origin or ancestry, physical or mental disability, veteran status, marital status, medical condition, sexual orientation, as well as any other category protected by federal, state, or local laws. Any use of the Company's technical resources to harass or discriminate is unlawful and strictly prohibited by the Company. Violators will be subject to discipline, up to and including discharge.

[Company Name] does not consider conduct in violation of this policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, the Company reserves the right not to provide a defense or pay damages assessed against Employees for conduct in violation of this policy.

### **3. Access to Information**

The Company asks you to keep in mind that when you are using the Company's computers you are creating Company documents using a Company asset. The Company respects the individual privacy of its Employees. However, that privacy does not extend to an Employee's work-related conduct or to the use of Company-provided technical resources or supplies.

The Company's computer, voice mail, e-mail, or telephone systems, and the data stored on them are and remain at all times the property of the Company. As a result, computer data, voice mail messages, e-mail messages, and other data are readily available to numerous persons. If, during the course of your employment, you perform or transmit work on the Company's computer system and other technical resources, your work may be subject to the investigation, search, and review of others in accordance with this policy.

All information, including e-mail messages and files, that is created, sent, or retrieved over the Company's technical resources is the property of the Company, and should not be considered private or confidential. Employees have no right to privacy as to any information or file transmitted or stored through the Company's computer, voice mail, e-mail, or telephone systems. Any electronically stored information that you create, send to, or receive from others may be retrieved and reviewed when doing so serves the legitimate business interests and obligations of

the Company. Employees should also be aware that, even when a file or message is erased or a visit to an Internet or Web site is closed, it is still possible to recreate the message or locate the Web site. The Company reserves the right to monitor your use of its technical resources at any time. All information including text and images may be disclosed to law enforcement or to other third parties without prior consent of the sender or the receiver.

#### **4. Copyrighted Materials**

You should not copy and distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, and downloaded information) through the e-mail system or by any other means unless you have confirmed in advance from appropriate sources that the Company has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by the Company as well as legal action by the copyright owner. Any questions concerning these rights should be directed to your Manager.

#### **5. Confidential Information**

E-mail and Internet/Web access are not entirely secure. Others outside the Company may also be able to monitor your e-mail and Internet/Web access. For example, Internet sites maintain logs of visits from users; these logs identify which company, and even which particular person, accessed the service. If your work using these resources requires a higher level of security, please ask your Manager or the MIS Department for guidance on securely exchanging e-mail or gathering information from sources such as the Internet or World Wide Web.

All Employees should safeguard the Company's confidential information, as well as that of customers and others, from disclosure. Do not access new voice mail or e-mail messages with others present. Messages containing confidential information should not be left visible while you are away from your work area.

E-mail messages containing confidential information should include the following statement, in all capital letters, at the top of the message: **CONFIDENTIAL: UNAUTHORIZED USE OR DISCLOSURE IS STRICTLY PROHIBITED.**

#### **6. Security of Information**

Although you may have passwords to access computer, voice mail, and e-mail systems, these technical resources belong to the Company, are to be accessible at all times by the Company, and are subject to inspections by the Company with or without notice. The Company may override any applicable passwords or codes to inspect, investigate, or search an Employee's files and messages. All passwords must be made available to the MIS Department upon request. You should not provide a password to other Employees or to anyone outside the Company and should never access any technical resources using another Employee's password.

In order to facilitate the Company's access to information on its technical resources, you may not encrypt or encode any voice mail or e-mail communication or any other files or data stored or exchanged on Company systems without the express prior written permission from the MIS Department and your Manager. As part of this approval, the MIS Department will indicate a procedure for you to deposit any password, encryption key or code, or software with the MIS Department so that the encrypted or encoded information can be accessed in your absence.

#### **7. [Company Name]'s Software Policy**

If you want to install software on Company computers, you must contact the MIS Department and request to have the software installed. Employees are prohibited from installing any software on any Company technical resource without the express prior written permission from the MIS Department.

Involving the MIS Department ensures that the Company can manage the software on Company systems, prevent the introduction of computer viruses, and meet its obligations under any applicable software licenses and copyright laws. Computer software is protected from unauthorized copying and use by federal and state law; unauthorized copying or use of computer software exposes the Company and the individual Employee to substantial fines and exposes the individual Employee to imprisonment. Therefore, Employees may not load personal software onto the Company's computer system and may not copy software from the Company for personal use.

#### **8. Your Responsibilities**

Each Employee is responsible for the content of all text, audio, or images that they place or send over the Company's technical resources. Employees may access only files or programs, whether computerized or not, that they have permission to enter.

Violations of any guidelines in this policy may result in disciplinary action up to and including termination. In addition, the Company may advise appropriate legal officials of any illegal violations.

### **APPENDIX 3 – SUMMARY OF KEY PROVISIONS TO CONFIDENTIALITY AND NON-SOLICITATION AGREEMENT WITH NON-OWNER EMPLOYEE**

#### **RECITALS**

Recitals include that: the Company has developed and will continue to develop proprietary and confidential information and Trade Secrets; Employee would not be given access to this information if not employed; the Employee's execution of the Agreement is a condition of employment; and that it is not intended to unfairly restrict Employee's ability to earn a living after the employment ends.

#### **AGREEMENT**

Proprietary and Confidential Information and Trade Secrets. Definition of "Trade Secrets" for purposes of this Agreement to include information which derives independent economic value for not being generally known in the industry and for which the Company takes reasonable efforts to maintain secrecy. Include multiple examples of Company Trade Secrets. Acknowledgment that these items constitute Trade Secrets which are the sole and exclusive property of the Company.

Nondisclosure. Strict non-disclosure provisions that apply both during and after employment ends.

Employee's Further Obligation. No copying or removal of Trade Secrets and confidential information. Take reasonable precautions to prevent unauthorized use by others. Disclose and transfer to Company any improvements, discoveries and inventions developed during employment. No personal financial gain using Company Trade Secrets and confidential information. Must show a copy of this Agreement to any future employers.

Prior Knowledge and Relationships. Acknowledgment that Employee has not taken and will not use any Trade Secrets belonging to any prior employer.

Noncompetition During Employment. Employee will not directly or indirectly compete against Company while employed by Company.

Non-Solicitation of Employees. Prohibition on soliciting or pirating Employees and consultants away from Company.

Non-Solicitation of Clients. For a period after employment ends, prohibition on soliciting clients or customers away from Company.

Ownership of Copyrights and Inventions. Acknowledgment that anything created by Employee during the scope of employment is a “work made for hire” that belongs to the Company. Requirement that Employee assist Company in securing patents copyrights or similar protections of such works. Written notification to Employee required by the California Labor Code regarding Employee Inventions.

Term of Agreement. Usually beyond the end of employment.

Default; Cumulative Remedies. Company may seek injunctive and other relief against Employee in addition to money damages in the event of a breach.

Entire Agreement. Acknowledgment that this Agreement contains everything regarding the subject matter and supersedes any prior agreements or discussions. Provision that nothing in this Agreement is intended to vary or modify the “at will” nature of Employee’s employment with Company.

Amendment. Any changes need to be in writing.

Applicable Law and Jurisdiction. Agreement to submit to personal jurisdiction in California and selection of specific court geographic venue within California for any lawsuit.

Benefit and Burden. The Agreement is binding on the respective successors and assigns.

Waiver. No party can waive the requirements/protections of the Agreement unless it is in writing.

Severability. If a court finds certain provisions of the Agreement to be unenforceable, the court and enforce the balance of the Agreement.

Interpretation. Guidance for interpretation of the Agreement.

**APPENDIX 4 – SAMPLE TERMINATION CERTIFICATION**

**XYZ Company**  
**TERMINATION CERTIFICATION**

This is to certify that I do not have in my possession nor have I failed to return any devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, materials, equipment, or any other documents or property or any reproductions of any aforementioned items belonging to the Company, its subsidiaries, affiliates, successors or assigns (together, the “Company”).

I further certify that I have complied with all the terms of the Company’s Employment, Confidential Information, Invention Assignment and Arbitration Agreements signed by me, including the reporting of any inventions and original works of authorship (as defined therein), conceived or made by me (solely or jointly with others) covered by that agreement.

I further agree that, in compliance with the Employment, Confidential Information, Invention Assignment, and Arbitration Agreement, I will preserve as confidential all trade secrets, confidential knowledge, data or other proprietary information relating to products, processes, know-how, designs, formulas, developmental or experimental work, computer programs, data bases, other original works of authorship, customer lists, business plans, financial information or other subject matter pertaining to any business of the Company or any of its employees, clients, consultants or licensees.

I further agree that for twelve (12) months from this date I will not hire any employees of the Company and I will not solicit, induce, recruit or encourage any of the Company’s employees to leave their employment.

Date:

\_\_\_\_\_  
(Employee’s Signature)

\_\_\_\_\_  
(Type/Print Employee’s Name)

\*\*\*\*\*

**THESE MATERIALS ARE INTENDED FOR INFORMATIONAL PURPOSES ONLY, AND ARE NOT INTENDED AS LEGAL ADVICE. DUE TO PAGE AND TIME CONSTRAINTS, THE MATERIALS ARE AN OVERVIEW AND SUMMARY ONLY, AND THEY DO NOT CONTAIN AN EXHAUSTIVE EXPLANATION OF THE LAW AND ITS MANY EXCEPTIONS. LEGAL COUNSEL SHOULD BE CONSULTED IF YOU HAVE SPECIFIC QUESTIONS.**