Business Counsel Update

WEST®

Prudent Governance Practices in Troubled Times*

*by Alan S. Gutterman***

The directors, as well as the senior officers, of every corporation have specific duties with respect to identifying and managing the risks associated with the business activities of the corporation. Under state corporation laws, for example, directors and officers must satisfy their fiduciary duties of care and loyalty and this generally means that they are required and expected to exercise reasonable judgment in overseeing the activities of the corporation by, among other things, developing internal reporting and monitoring systems that will allow them to keep abreast of material risks. Once a material risk has been identified the directors and officers must exercise their good faith business judgment to manage those risks in an informed and disinterested manner. In addition, §404 of the Sarbanes-Oxley Act places explicit burdens on the leaders of public companies to regularly assess the effectiveness of their internal controls and stock exchange requirements, such as those mandated by the New York Stock Exchange, require that members of the audit committee of any listed company must discuss the company's policies with respect to risk assessment and management as well as the company's major financial risk exposures and the steps management has taken to monitor and control such exposures. It should be noted that the NYSE rules include a comment that the actions of the audit committee should not replace other mechanisms used by listed companies to manage and assess their risks and that the CEO and other members of the senior management team are expected to take the lead in this area. Finally, any actual or perceived failure with respect to risk management will likely expose the company and its directors and officers to intense scrutiny by the media and the financial community that may substantially damage the reputation of the company, impair its ability to obtain additional capital and trigger inquiries from regulators.

When a corporation runs into trouble based on what appears to be, in the perfect light of hindsight, a failure to anticipate and manage a material risk the directors are themselves vulnerable to a claim that they breached their duty of loyalty by failing to act in good faith in taking steps to identify and manage risks and/or consciously disregarding

* *This material is adapted from Business Transactions Solution's April 2009 online newsletter, Business Counsel Update (available on Westlaw, database identifier: BTS).*

** **Alan Gutterman** *is a partner at the San Francisco and Silicon Valley offices of The General Counsel (http://www.thegeneralcounsel.net/), a provider of interim in-house general counsel and attorney recruitment services. Mr. Gutterman has over two decades of experience as a partner and senior counsel with internationally recognized law firms counseling small and large business enterprises in the areas of general corporate and securities matters, venture capital, mergers and acquisitions, international law and transactions, strategic business alliances, technology transfers and intellectual property, and has also held senior management positions with several technology-based businesses. Mr. Gutterman is also the author of several publications, including Business Transactions Solutions, California Transactions Forms, Corporate Counsel's Guide to Strategic Alliances, Corporate Counsel's Guide to Technology Management and Transactions, and Going Global: A Guide to Building an International Business.*

April 2009

IN THIS ISSUE:

TO CONTACT US:

Customer Service 1-800-328-4880
Product Info & Sales 1-800-344-5009

west.thomson.com

warning signs that suddenly appear to be so clear once the damage has occurred. The business judgment rule can provide directors with a "safe harbor" absent a showing of a breach of fiduciary duties; however, in order for the rule to be of value to directors they must establish in advance a record that they have acted in good faith and in the honest belief that their decisions were in the best interests of the corporation and its shareholders. Given the volatility of business and financial markets, which means that a new and apparently unforeseeable crisis can arise at any moment, it is imperative for directors and senior officers to act immediately to review and shore up their risk assessment and management policies and procedures. This advice applies even to those corporations that believe they have already done enough (since any failure to explicitly and formally acknowledge the tremendous uncertainty in the environment might in and of itself be viewed as a questionable governance practice). Another complicating factor for corporations that fall into dire financial condition—referred to as the "zone of insolvency"—is the additional fiduciary duties to creditors as well as shareholders.

Every industry has its own unique array of risks and no advice can cover all situations; however, given general economic conditions, and particularly the problems in the financial and credit markets, directors and senior officers should begin by regularly and carefully monitoring risks that might impact the ability of the company to maintain liquidity and access to capital needed for the business to survive and hopefully expand in the future. Directors and senior officers should anticipate that is highly likely, even for the best companies, that cash flow will be slowing down and that for the foreseeable future debt and equity capital will be unavailable or available only on terms that are prohibitively expensive. As such, it is recommended that directors and officers should review and update the company's operating and business plans, establish performance monitoring procedures, analyze the availability of short- and long-term capital, evaluate the condition and prospects of key business partners, analyze and upgrade disclosure and communications practices and procedures and evaluate and improve corporate governance practices.

1. Operating and Business Plans

The first thing that the directors should do is order the CEO and the other members of senior management team to immediately conduct a thorough review and analysis of the company's near-term operating and business plans—covering the next 12 to 36 months—to identify potential issues relating to liquidity and capital requirements. The analysis should be based on the most current data and all assumptions should be rigorously tested so that several possible scenarios are placed in front of the directors for discussion. This is the time for the senior officers to be creative and brutally honest with themselves about adverse events that might occur within their specific functional area of responsibility. For example, the CFO needs to consider what might happen if credit rating agencies suddenly downgrade the company's rating and the senior officer in charge of sales should look and see how economic conditions are likely to impact the buying behavior of major customers (or groups of customers). Companies that have direct and indirect exposure to so-called "toxic" financial instruments need to determine how developments in this area will impact their balance sheets. All departments and business units need to look at how systematic liquidity issues might impact their operations—will key vendors provide revolving credit arrangements, will the company need to adjust payment terms for large customers, what options are available for accessing short-term credit and/or investing excess cash? Given the rise of globalization it is likely that economic conditions in many foreign countries will also need to be evaluated since companies now regularly sell into foreign markets and rely on foreign business partners for raw materials, components and outsourced business services.

It is likely that the operating and business plan review will uncover areas where revisions are necessary. The CEO and other senior officers should highlight specific issues that are of the greatest concern and propose changes to the plan that can mitigate the foreseeable material risks confronting the company. Among the options that should always be considered, although not necessarily implemented in each case, are cash preservation and cost reduction programs; classification of proposed capital expenditure programs into "essential" and "discretionary" and reallocation of scarce resources in accordance with those classifications (i.e., discretionary spending will be deferred and resources related to those programs will be channeled to other areas or, in the case of personnel, laid off); and identification of alternative sources of supply for key goods and services if there is a concern that current vendors may not be able to meet the anticipated requirements of the company. The decisions that must be made can be difficult and priorities must be set and honored by the directors and senior officers. For example, while it may be tempting to use available cash to repurchase company stock at what have become "bargain prices," that capital may be better used as a war chest that can accessed if credit markets continue to struggle beyond the danger period assumed in the plan. Senior officers must also set aside their personal interest in additional compensation to save cash and avoid unnecessary negative publicity.

2. Performance Monitoring Procedures

Once the operating and business plan review has been completed, and appropriate changes have been made to the plan, the directors should direct the CEO and the other senior officers to establish programs and procedures for continuous monitoring the performance of the company using the most current information possible. The monitoring program should extend beyond internal performance indicators to include all relevant factors in the company's business environment including general economic conditions, financing and credit markets and the health of the business activities of the company's key business partners and competitors. Provision should be made for regular and prompt reporting of material developments, particularly substantial and unforeseen variances from the plan, to the directors (or a specific sub-group of directors designated by the entire board) along with a description of the potential consequences and the various steps that the management team is considering in order to mitigate any new risks to the business activities of the company. Monitoring cannot be confined to developments in the domestic market and must include all key foreign markets. For example, if major manufacturers in Asia announce plant shutdowns the impact of these developments should be considered not only from the supply side, if applicable, but also in relation to dampened demand for the company's products in Asian markets.

3. Availability of Short- and Long-Term Capital

While liquidity issues are an important part of the above-described review of the company's operating and business plan a separate analysis should be done on the projected availability of short- and long-term capital to execute the plan and strategies should be developed for seeking and obtaining alternative sources of capital. One of the first things that should be done is a review of the company's current debt and credit agreements to identify any potential compliance issues with respect to covenants and payment obligations. Particular attention should be paid to provisions that allow lenders to adjust credit terms, suspend additional borrowings or even terminate the agreement - can call the loan for immediate repayment. The CFO should carefully evaluate the company's ability to meet its obligations under these agreements. A similar process should be followed with any other agreements that include the extension of credit to or by the company including contracts with suppliers that have traditionally allowed the company to pay for goods and services 30, 60 or even 90 days after taking delivery. If actual or potential problems are discovered, the company should consider contacting lenders (including other lenders that might have the right to call their loans under cross-default provisions) as soon as possible to amicably negotiate some form of workout. If that is necessary, the revised operating and business plan that should have been developed by the senior management team will be a useful tool in persuading lenders that the company has a good handle on managing its financial situation. Even if the company does not have an immediate compliance issue under its existing credit arrangements the CFO should identify and communicate with other potential capital providers since there is no guarantee that the company's existing lenders will continue extending credit even to their best customers.

4. Business Partner Evaluation

The operating and business plan review discussed above should include the collection and evaluation of information on each of the company's key business partners in order to assess whether they are in a position to continue their current and projected volume of business with the company during the planning period. As part of that assessment a review should be performed of the existing contractual arrangements with those partners to confirm the duties and responsibilities of both parties and identify any specific milestones or performance conditions that might be at risk of being defaulted upon by either party. For example, if the company has appointed another party as an exclusive distributor of the company's products in an important territorial market a review should be made to determine whether the distributor will be able to satisfy any minimum sales requirements that should have been imposed as a condition to exclusivity. If it appears that the distributor will have problems fulfilling its obligations, plans must be made for identifying and establishing new distribution channels in that market. Joint venture arrangements should also be reviewed to determine whether partners can continue to fill their obligations. In many cases the governance provisions in the joint venture agreement will permit a shift in voting rights or allow one of the parties to terminate the venture and put their equity interest to the other party.

5. Disclosure and Communications Practices

All companies, particularly listed companies, must seriously consider disclosure and communications practices and procedures as they go through their plan review process and make adjustments to accommodate turbulent business and financial conditions. For listed companies this means understanding and complying with the detailed disclosure requirements under the federal securities laws with respect to risk assessment and management in general and liquidity and capital resources specifically. When filing their annual and quarterly reports with the SEC, listed companies must include a detailed discussion of liquidity and capital resources in the management discussion and analysis (MD&A) section and interim changes in the company's liquidity profile need to be disclosed in Form 8-K filings. SEC requirements regarding the MD&A should be carefully reviewed and followed and particular attention should be paid to changes that may have been made in forecasts that the company may have issued in previous reporting periods. Stock exchange regulations and state laws should also be

consulted to determine if they create additional disclosure obligations. While the entire board, and the audit committee in particular, should be carefully monitoring the company's public disclosures increased vigilance is necessary in a time when external changes are occurring on an almost daily basis and additional resources should be assigned to collecting and evaluating the information that would serve as the basis for the required disclosures.

Compliance with SEC and exchange reporting requirements is just one element of the company's overall communications strategy and it is essential for the company to develop and implement a comprehensive plan for communicating with its key stakeholders including customers, vendors, investors, regulators, the general public and, perhaps most importantly, employees. With respect to the investment community, one of the main concerns is that unfounded rumors regarding the business and financial condition of the company will play havoc with the company's stock price. Certainly the disclosures made to investors should be accurate and bad news should not be withheld when the circumstances warrant disclosure; however, special care should be taken to keep analysts fully informed and monitor all news sources to identify and remedy misinformation regarding the company. In addition, the CEO and senior officers of each of the key functional departments and business units should reach agreement on a common communications message that can be used in discussing the company's condition and prospects with interested parties. Meetings should be held with employees to update them on company affairs and answer any questions they might have about business strategy and plans relating to personnel, including layoffs and reduction in compensation and/or benefits. Discussions should also be initiated with key customers and vendors about possible restructuring of contractual arrangements and procedures should be implemented to ensure that each side remains informed about new events. This is the time when a professional communications advisory firm might be used to assist company representatives in dealing with the unfamiliar issues that arise in times when the company enters a crisis situation.

6. Corporate Governance Practices

Directors and senior officers should launch a thorough review of the company's corporate governance practices including internal controls and risk assessment/management processes. The review should be done in conjunction with outside professional experts from the legal and accounting areas and should include refreshed training for the directors and senior officers regarding their fiduciary obligations and the need for them to think and act responsibility in their formal deliberations and in their communications with interested stakeholders. Specific consideration should be given to whether or not the directors and senior officers are meeting frequently enough to evaluate information and engage in face-to-face dialogue regarding the strategic and legal issues that might be confronting the company. Failure to regularly deliberate on these matters might later be construed as a breach of the duty of due care and expose the directors to potential liability from shareholder actions. Experienced legal counsel should be asked to provide guidance on the processes that the directors should follow and the particular issues that need to be addressed. In particular, directors should be sure that they have access to all relevant information and that the records of their deliberations clearly document that the directors acted prudently and had a good basis for all of their decisions in order to preserve the protections of the business judgment rule. Finally, directors should also be made aware of limitations of exculpatory provisions in the company's charter documents and the scope of available protection under the company's directors' and officers' liability insurance coverage.

Challenges of the Internet for In-House Counsel—Drafting Effective Policies and Procedures Relating to E-Mail Use and Internet Access

The Internet, and related developments in communications technology in general, has transformed the workplace and created significant benefits and opportunities for businesses of all sizes; however, engaging in activities on the Internet also carries the potential for extraordinary liability in a wide range of areas including infringement of intellectual property rights, unfair competition, defamation, sexual harassment, wrongful termination, fraud, and invasion of privacy. In addition, connecting its computer system to the Internet, or allowing dial-in access, can expose a company to computer hackers, viruses, and industrial espionage. It is, therefore, sound practice for every company, regardless of its size or the line of business in which it is engaged, to develop, implement, and enforce policies on the use of company-supplied communications tools, including e-mail accounts and Internet access facilities of all types.

Before drafting and implementing any new policies in this area management must evaluate and assess the specific need for limitations and restrictions on the use of Internet technology. There are a number of preliminary questions that management should address including:

- Which employees will have access to the Internet technology and how will they be identified?
- What steps can, and should, be taken to prevent unauthorized access or sabotage to the Internet site by employees or outside parties?
- What steps should be taken to prevent employees from using the Internet technology for illegal or illicit purposes, such as harassment, discrimination, or libel?
- What rules should be implemented to protect confidential or sensitive information that might be included, or transmitted, over the Internet?

- What steps should the company take with respect to monitoring or accessing information which is stored or transmitted by employees?
- Should employees be required to sign written authorizations that permit the company to monitor employees' use of the Internet?

One way the evaluation and assessment process can be accomplished is to put together a technology team made up of employees from various departments within the company. The technology team can be responsible for a variety of tasks, including providing management with recommendations regarding Internet technological needs; assisting in the often delicate and time-consuming process of implementing the Internet technology; adapting the company's existing policies and programs to the new Internet tools; and communicating the company's overall technological goals to the workforce. In cases where all or a portion of the company's employees are members of a union, union representatives may need to be consulted if the Internet technology will have a material effect on working conditions.

The form and content of the company's Internet and e-mail policies may vary depending on the circumstances, particularly the laws that might apply to the activities of the company's personnel in a given location. In general, the company policy should identify acceptable uses, and prohibited misuses, of the company's communications tools. The policy should concern itself with limiting access to the company computers and Internet access facilities to employees and other authorized persons, including some limited access for family members of an employee. Ideally, use of company communications tools should be restricted to necessary communications with coworkers, customers, consultants, vendors, and other business partners of the company; however, many policies do permit some personal use of communications tools, so long as such use does not interfere with company business or result in unwarranted company expense or consumption of company resources.

Companies can use a variety of strategies in drafting appropriate policies. As the company begins to integrate the new technologies into the workplace, it might adopt a simple and basic policy regarding computer use. *(**See page 5**)* As the company becomes more dependent on Internet access, policies should extend beyond computer use to address specific risks associated with the Web. When the company is small and activities are somewhat informal, the policy can be relatively short and focus on general "common sense" guidelines. *(**See page 6**)* As the company grows, however, the policy should be more comprehensive and include issues such as infringement and obscene materials. *(**See page 7**)* Many firms adopt a more comprehensive policy covering all aspects of the business-related uses of the Internet as well as the company's in-house computers and networks. *(**See page 9**)*

Broader policies are often supplemented by additional policies on specific areas of concern. For example, Internet users should be cautioned against inadvertently disclosing any copyrighted materials of the company in ways that might facilitate unauthorized and uncompensated use by third parties and this can be reinforced through the development of a company policy on the use of copyrighted materials. *(**See page 10**)* Many companies create policies regarding the form and content of business communications made through the use of e-mail. *(**See page 11**)*

While all of the issues listed above are important and generally apply to almost every type of business, the policy or guidelines should always be customized to any specific requirements and risks of the particular company or firm. For example, law firm guidelines for Internet usage should reinforce the need to preserve high professional standards, particularly in situations where the user is communicating with clients and commenting in online forums where the user's affiliation with the firm is disclosed to the public. *(**See page 12**)*

Computer Use Policy

[This form presents a simple and basic computer use policy, which can be tailored to a company's specific needs. Some companies may be reticent to adopt a full-blown computer use policy for fear of an employee backlash. This is a particular concern in the educational environment where students and faculty generally oppose restrictions on computer use. In such cases, a simple, one-page policy like this can address most of the major concerns surrounding the use of computer and telecommunications equipment and resources. As a company's use of technology grows, its policy can be expanded.]

This document describes the policies and guidelines for use of the computer and telecommunications resources of [name of company] (the "Company"). All computer users employed by the Company have the responsibility to use these resources in a professional, ethical and lawful manner.

The computers and computer accounts provided to employees by the Company are to assist them in the performance of their jobs. The computer and telecommunications system belongs to the Company and may only be used for authorized business purposes.

Employees waive their right of privacy in anything they create, store, send, or receive on the Company's computer or telecommunications system. Employees consent to management or supervisory personnel of the Company accessing and reviewing all material employees create, store, send, or receive on the computer or telecommunications system.

Use of the Company's computer or telecommunications system for any of the following activities is strictly prohibited:

(1) Sending, receiving, displaying, printing, or otherwise disseminating material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, or defamatory.

(2) Sending, receiving, displaying, printing, or otherwise disseminating confidential, proprietary business information or trade secrets in violation of company policy or proprietary agreements.

(3) Transmitting, storing, or otherwise disseminating commercial or personal advertisements, solicitations, promotions, destructive programs (for example, viruses or self-replicating code), or political material.

(4) Violating any state, federal, or international law governing intellectual property (for example, copyright, trademark, and patent laws) and online activities.

(5) Violating any license governing the use of software.

Violations of this policy may result in disciplinary action, including possible termination of employment, legal action, and criminal liability.

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of the Company's computer and telecommunications equipment and services.

Dated: [date]

[signature of employee]

[name of employee]

[employee's computer account]

Guidelines for Internet Usage

[This form is a simple version of guidelines for Internet usage that is appropriate for implementation by smaller businesses that limit their information assets to company-owned desktop computers. The guidelines emphasize the need for employees and contractors to exercise good judgment and common sense when accessing the Internet and to refrain from accessing information that is inappropriate and not aligned with a legitimate business purpose. Particular concerns addressed in the guidelines include unauthorized dissemination of proprietary company information and downloading of software on to the company's information assets. This form includes a short-form statement of the company's rights to monitor Internet usage and reminds employees and contractors that they should not have any expectation of privacy.]

These guidelines are intended to provide you with some basic tips regarding Internet usage while you are engaged in activities on behalf of [name of company] (the "Company"). These guidelines are not intended to be comprehensive and do not contain all of the "do's" and "don'ts" of Internet usage. While these guidelines provide examples of improper usage, it is essential that you use good judgment and common sense in determining whether you are using the Internet appropriately and what steps you should be taking to protect the resources of the Company. While these guidelines are primarily intended for employees of the Company they also apply to contractors of the Company who are using the Internet for business purposes in order to discharge their contracted responsibility to the Company and contractors are expected to adhere to these guidelines.

General Principles

Your first obligation as a user is to protect the Company's information assets. The assets that are part of the Company's information systems network, including computers and other devices that permit access to the Internet, are business assets and should not be considered to be your personal assets. The following general principles should be understood and followed with respect to your use of the Internet solely for the business purposes of the Company:

- Material that would be considered inappropriate, offensive or disrespectful to others should not be accessed or stored;
- Any software downloaded or installed on the Company's assets must comply with applicable licensing agreements and copyrights;
- You should only use network services for which you have authorization to access;
- Material classified for internal use only should not be sent via the Internet; and
- The Internet should not be used for personal gain or profit, to represent yourself as someone else, to

provide information about employees to persons or businesses not authorized to possess that information, when it interferes with your job or the jobs of other employees, or when it interferes with the operation of the Internet for other users.

You should always consult with your manager whenever you have doubts about your use of the Internet and the application of the principles outlined above.

Data Classification

Personnel records and financial information that is stored on the Company's network is considered information for internal use only. This information, along with other proprietary information will not be sent via the Internet. Managers can make exceptions for sending the Company's internal-use-only material when appropriate encryption is used.

External Communications

Electronic mail or e-mail is the most commonly used form of communication on the Internet and you should expect to engage in business communications on behalf of the Company using e-mail; however, when communicating with parties outside of the Company using e-mail the following rules should be kept in mind:

- No form of chain letter should be sent using Company assets;
- Do not send e-mail so that it appears to have come from someone else; and
- Do not automatically forward your e-mail to a non-Company e-mail address.

Additional Matters

You may not remotely access the Company's network without prior written authorization by your managers and any such remote access should be done only using the protocols established by the Company's network systems department. Unless you have prior authorization, do not run port or vulnerability discovery programs or try to get into open ports.

When downloading software for use on Company assets, you must comply with the Company's procedures for the importation of software, even if it's "public domain." As a courtesy to others, try to do large file transfers during off hours.

The Company reserves the right to monitor your use of Company assets and you should have no expectation of privacy with regard to your use of such assets.

If you have any questions regarding Internet usage, contact your manager.

Internet Access Policy Guidelines

[This form is an example of a policy guidelines relating to employee use of company-supplied Internet access facilities. While the style and content of Internet policies may vary among companies, it is important for the employer to make it clear that personal use of its computers and other communications tools will be carefully monitored and that employees should not have an expectation of privacy in that area. In addition, the policy should make it clear that Internet use raises issues of defamation and copyright infringement, as well as the possibility that widespread use of Internet tools to access sex cites on the World Wide Web might create a hostile environment that increases the risk of sexual harassment claims against the company. In order for this type of policy to be effective, particularly in light of the restrictions on employees' privacy rights, it should be widely disseminated in personnel handbooks and as part of the company's own internal electronic library. Some policies also include rules relating to e-mail etiquette, including content, sending and responding to messages within the company, forwarding messages, and sending unsolicited messages to outsiders.]

These guidelines address the appropriate use of various electronic communications tools that the company regularly makes available to its employees, including company-supplied computers and company-supplied network tools like browsers and Internet access facilities. Certainly we all understand that the Internet and the information available through it is a tremendous resource for the company and that it can be very important to employees as they carry out their duties for the company. However, it should not be forgotten that careless use of electronic communications tools can be quite harmful to the company, its customers, and its employees. Accordingly, your use of these electronic communications tools should always follow the rules and policies set forth herein, all of which are designed to protect the company's interests and prevent exposure to unnecessary liabilities.

1. Business Purpose Requirements

Access to company communications tools is provided to you in conjunction with the company's business and to assist you in carrying out your duties with the company. We anticipate that you will be using these tools to communicate internally with your coworkers

or externally with customers, consultants, vendors, and other business associates. Also, we hope that Internet access will enhance your productivity by allowing you to access information that you can use in your work. Please remember, however, that the communications tools are intended primarily for business use. Some incidental personal use of company communications tools is permitted so long as it does not interfere with the performance of your job, consume significant resources, give rise to more than additional costs, or interfere with the activities of other employees.

2. Sexually Oriented, Defamatory, or Obscene Materials

In no event is any company computer to be used in any way to access or download material from any site where the principal content of the material is sexually oriented, or where employees have reason to believe the information being accessed may be defamatory or irresponsible. Also, no employee should ever use a company communications tool to transmit any defamatory or obscene material. Use of the communications tools in any way which is sexually offensive or harassing is expressly prohibited.

3. Infringing Materials

You may not use any company communications tools in connection with any infringement of another person's intellectual property rights (e.g., copyrights). For example, downloading material from an Internet source might be considered a copy of it under the copyright laws and, therefore, if the material is copyrighted, that would be an infringement. If there is any doubt as to whether or not something can be downloaded, you should contact the network manager or a member of the company's legal staff in advance.

4. Company Monitoring and Auditing

You should know that, in order to make these policies effective, Internet access using the company's communications tools will need to be monitored and/or audited from time to time. You should have no expectation that any information transmitted over company facilities or stored on company-owned computers is or will remain private. Any personal use that you might make of the company's communications tools is based on the express understanding that the company reserves the right (for its business purposes or as may be required by law) to review employee use of, and to inspect all material created by or stored on, these communications tools.

YOUR USE OF THE COMPANY'S COMMUNICATIONS TOOLS CONSTITUTES YOUR PERMISSION FOR THE COMPANY TO MONITOR YOUR COMMUNICATIONS AND TO ACCESS FILES THAT ARE MADE 0N OR WITH THE TOOLS.

5. Reporting Violations

If you become aware of any violations of this policy, you are encouraged to report such violations to [name] or call [phone number] which is the company's hot line for reporting improper conduct on a confidential basis.

6. Policy Changes and Posting

Questions regarding this policy may be directed to [name] and or members of the company's legal staff. While the company intends to generally follow the rules set out in this policy, it also reserves the right to change the policy at any time without any prior notice to employees. The company will make reasonable efforts to ensure that the latest version of this policy is kept available through postings on the company's web page at [address].

Computer Use and Internet Policy

Purpose

The purpose of this policy is to ensure the proper use of the computer and telecommunication resources and services of [name of company] (the "Company ") by its employees, independent contractors, and other computer users. All computer users have the responsibility to use the Company's computer resources in a professional, ethical, and lawful manner.

The following policies, rules, and conditions apply to all users of computer and telecommunication resources and services, wherever they are located within the Company. Violations of this policy may result in disciplinary action, including possible termination of employment, legal action, and criminal liability.

Policy

The Company's computer and telecommunication resources include, but are not limited to, the following: host computers, file servers, application servers, mail servers, fax servers, communications servers, workstations, standalone-computers, laptops, software, and internal or external computer and communications networks (including Electronic Data Interchange networks, Internet, commercial online services, bulletin board systems, and e-mail systems) that are accessed directly or indirectly from the Company's computer facilities.

The term "Users," as used in this policy, refers to all employees, independent contractors, and other persons or entities accessing or using the Company's computer and telecommunications resources and services.

The Company has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites visited by Users on the Internet, monitoring chat groups and news groups, reviewing material downloaded or uploaded by Users, and reviewing e-mail sent and received by Users.

The computers and computer accounts given to Users are to assist them in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on the Company's computer or telecommunications system. The computer and telecommunications system belongs to the Company and may only be used for business purposes.

Users are governed by the following provisions, which apply to all uses of the Company's computer and telecommunications resources and services:

1. **Compliance With Applicable Laws and Licenses**

   Users must comply with all software licenses and copyrights, and with all state, federal, and international laws governing intellectual property and online activities.

2. **Prohibited Activities**

   Fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or other unlawful or inappropriate material may not be sent by e-mail or other forms of electronic communication (such as chat groups, bulletin boards, or news groups) or displayed on or stored in the Company's computers. Users encountering or receiving such material should immediately report the incident to their supervisor.

3 **Prohibited Uses**

   Without prior written permission, the computer and telecommunications resources and services of the Company may not be used for the transmission or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political material, or any other unauthorized use.

4. **Communicating Information**

   Content of all communications should be accurate. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may, and likely will, be reviewed by others.

5. **Communication of Trade Secrets**

   Unless expressly authorized by the User's supervisor, sending, receiving, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the Company is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties.

6. **Installation of Software; Virus Detection**

   Users may not install software onto their individual computers or the network without first receiving express authorization to do so from the system manager.

   Users may not install or use encryption software on any of the Company's computers without the express written consent of their supervisor. Users may not use passwords or encryption keys that are unknown to their supervisors.

   All material stored on floppy disk or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to the Company MUST be scanned for viruses and other destructive programs before being placed onto the Company's computer system.

7. **Forwarding E-Mail**

   Users may not forward e-mail to any other person or entity without the express permission of the sender.

8. **Communications with Attorneys**

   E-mail from or to in-house counsel or an attorney representing the company must include a header identifying the message as an attorney-client communication.

9. **Accessing Other Users' Files**

   Users should not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. The ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file.

10. **Responsibility for Passwords**

    Users are responsible for safeguarding their passwords for the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system using another User's password or account. Users may not disguise their identities while using the computer system.

11. **Export Restrictions**

Because of export restrictions, programs or files containing encryption technology are not to be placed on the Internet or transmitted in any way outside the United States without prior written authorization from [name].

12. Waiver of Privacy

Users waive any right to privacy in anything they create, store, send, or receive on the Company's computers or the Internet. Users consent to personnel of the Company accessing and reviewing all material Users create, store, send, or receive on the Company's computers or the Internet.

13. Other Policies Applicable

Users shall observe and comply with all other policies and guidelines of the Company, including, but not limited to,[set forth additional policies].

14. Disclaimer of Liability for Actions by Users

The Company is not responsible for the actions of individual Users in using the equipment and resources that are the subject of this policy.

15. Disclaimer of Liability for Use of Internet

The Company is not responsible for material viewed or downloaded by Users from the Internet. Users are cautioned that the Internet is a worldwide network of computers that contains millions of pages of information. Many of these pages include offensive, sexually explicit, and inappropriate material. Users accessing the Internet do so at their own risk.

16. Amendments and Revision

This policy may be amended or revised from time to time as the need arises.

I have read, understand, and agree to comply with the foregoing policy, rules, and conditions governing the use of the Company's computer and telecommunications resources and services. I understand that a violation of this policy may result in disciplinary action, including possible termination of employment, legal action, and criminal liability.

Dated: [date]

[signature of employee]

[printed name of employee]

[employee's computer account]

Policy on Copyrighted Materials

[This form is an example of a policy on the use of copyrighted materials that may be adopted by a company to ensure that its employees do not engage in activities that may result in an infringement of the company's valuable copyrights. The policy begins with a brief overview of copyright protection including actions that may result in infringement. Whenever possible the policy should include a list of works typically produced or used by the company that are eligible for copyright protection so that employees understand what documents and databases are in need of protection. The policy then sets out several guidelines that should be followed in order to avoid infringement and then provides information on steps that can be taken to obtain appropriate authorization of use or transfer of copyright material in order to avoid violations of the policy.]

[NAME OF COMPANY] POLICY ON COPYRIGHTED MATERIALS

I. Introduction

[Name of company] (the "Company") continually invests significant resources to create software, text, and other materials. The majority of these materials are protected under copyright laws of the United States and of other countries worldwide. To protect its investment, the Company diligently guards against infringement of its copyrighted materials. This policy outlines certain conduct that violates the Company's copyrights. This policy is subject to change at any time and without notice.

II. Copyright

Copyright protects original works of authorship fixed in a tangible medium of expression. Copyright infringement occurs when any one or more of the following rights is violated: (1) reproduction; (2) adaptation; (3) distribution to the public; (4) performance in public; or (5) display in public. Copyright infringement issues can also arise when a new work or a modification of an existing work, known as a derivative work, is created from a copyrighted work. A derivative work is based upon a pre-existing work in which the pre-existing work is changed, condensed, recast, transformed, adapted, or embellished. If the pre-existing or underlying work is a protected work under copyright law, one who wishes to exploit the derivative work must obtain a license from the owner of the copyright in the underlying work or works. Thus, modification of the Company's copyrighted materials without explicit permission for commercial use constitutes infringement. Without written permission from the Company, you may not make any unauthorized reproduction or engage in distribution of the Company's copyrighted materials, which include, but are not limited to, materials such as books, publications, computer software (including object code and source code), online curricula, Web content, diagrams, photos, testing materials, exams, text, images, and graphics published by

the Company in any format. It is Company policy to enforce its copyrights against any third party who infringes on its copyright. To ensure that you do not infringe on any of the Company's copyrighted materials:

(1) Do not directly or indirectly copy, reproduce, or distribute any of the Company's materials (including Web pages) or any part of the text or graphics from those materials.

(2) Do not directly or indirectly modify or create derivative works of any of the Company's materials.

(3) Do not copy, reproduce, or modify source code or object code of any of the Company's products.

(4) Do not create an emulator or simulator of a Company product in a manner that is likely to confuse the public about the source of the emulator or simulator.

(5) Do not create materials that look as though they originated from or are endorsed by the Company.

(6) Do not imitate the color or visual appearance of the Company's materials and/or products.

(7) Do not use the Company's icons as graphical design elements in your materials.

(8) Do not distribute the Company's work by sale, rental, or other disposition.

III. Copyright Permission Requests

To request permission to use the Company's copyrighted material, please use our online Request Tool at [address of Web site].

IV. Additional Guidelines

General policies about the Company's trademarks and web usage are found at [address of Web site].

DISCLAIMER

This policy document is not intended to serve as legal advice. Should you have questions regarding your legal rights or duties, please consult your own attorney. Should you have further questions regarding the Company's policy for its copyrighted materials, please contact [name of entity] at [address of Web site].

Business Email Communications Policy

[This form is an example of business email communications policy that can be used by companies to educate their employees regarding the preferred methods for professional and efficient electronic communications with outside business partners and within the company. Guidelines are provided for sending new emails and replying to emails and covers content, subject fields, signatures, timing of responses, tone and forwarding. These guidelines should be used with an overall email use policy that addresses other topics including monitoring of employee email communications.]

I. Purpose

To provide rules and tips for professional and efficient business email communication by all employees of [name of company]

II. Policies

A. Sending out New Emails

(1) Content: Keep messages brief and to the point. Try to restrict yourself to one subject per message; sending multiple messages if you have multiple subjects. This helps recipients to use the "subject" field to manage the messages they have received.

(2) Subject field: Make sure that the "subject" field of your email message is meaningful. Do not put questions into subject field.

(3) Signature: Have proper name, title and contact information in your email signature, including phone number and Company websites.

B. Replying to Emails

(1) Reply promptly: Respond to outside emails (customers, vendors, etc.) within 24 hours. Also reply to any customer or vendor related interdepartmental email issues within 24 hours. Address all other interdepartmental emails within 48 hours. Always reply, even if a brief acknowledgment is all you can manage. There is still sufficient unreliability about email transmissions to create doubt in the mind of the sender that you ever received it.

(2) Ask for more information: If not enough information is provided, immediately ask for more in a polite tone. Something like "can you tell me more about …" or "I am sorry I did not understand the question …"

(3) Reply To all: Reply to all in most cases (especially email sent to the support groups), but always be aware not everyone might need or be privileged to the information. If you are uncertain about what you are sending, check with your supervisor or manager first.

(4) Don't type angry: Be very careful how you express yourself, especially if you feel heated about the subject. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression. If you

meant something in jest, use a "smiley" [:-)] to convey that.

C. Additional Tips

(1) Don't send frivolous, abusive or defamatory messages. Apart from being discourteous or offensive, they may break the law.

(2) Verify all information very carefully. Our number one job (after being polite) is to be accurate! Also verify spelling and grammar to the best of your ability.

(3) CC (copy) your emails to the correct Company employees, such as your supervisor, or anyone else that is directly involved. However do not add unnecessary people to email chain.

(4) Use standard spelling, punctuation, and capitalization. Do not use all caps. THERE'S NOTHING WORSE THAN AN EMAIL SCREAMING A MESSAGE IN ALL CAPS.

(5) Use the OUTLOOK Follow Up & Reminder features to remember important emails that require follow up.

(6) Attachments: Avoid unnecessarily large file sizes. Try to reduce the size of pictures, and send links to a downloadable file instead of the file itself. Describe the link and tell them exactly what to expect.

(7) Do not expect the people you are communicating with to remember other email chains or phone conversations that occurred many days or weeks ago.

(8) Do not assume the other person understands the technologies or components involved as well as you do. You have to assume our customer only has a basic knowledge unless they have already demonstrated otherwise.

(9) Emails are essentially public communications. Remember that people other than the person to whom it's addressed may see your message; i.e. recognize that anyone along the chain of distribution could get to see what you have said, and it might even end up in someone else's hands by being forwarded to a third party.

(10) Set your Out of Office in Outlook if you will be gone more than four hours from your desk (half a day or more).

Law Firm Guidelines for Internet Usage

[This form is an example of guidelines for Internet usage suitable for implementation by a professional services business such as a law firm. The guidelines define the types of Internet access services to which the policies and procedures will apply and then outline the appropriate uses of the Internet access services. A separate section on confidentiality considerations should be included given the sensitive nature of the information collected and used by employees of the firm, particularly attorneys, in providing professional services to the firm's clients. In all cases the users of the firm's Internet access services should be admonished to maintain standards of professional responsibility with respect to communications made to outsiders and others within the firm. The last section of the guidelines addresses in detail the firm's policies with respect to privacy in relation to monitoring Internet usage and the firm reserves broad rights to track how its Internet access services are being used].

I. Internet Access Services

[name of law firm] (the "Firm") provides access to the Internet from the desktop, from computers in the library and from laptop computers and other mobile devices that allow users to access the Internet. This policy statement sets forth the Firm's policies with respect to acceptable use of any Firm-provided Internet access resources including computers and any other Internet-access devices, browser software and communications lines to the Internet. If and when Internet is used for the purpose of sending and/or receiving e-mail (or other electronic communications such as instant messaging), reference should also be made to the Firm's policies and procedures relating to the use of e-mail and other electronic communications.

II. Appropriate Use of Internet Access Services

A. Business Use

The Firm's Internet access resources are, like other resources of the Firm, first and foremost made available for Firm-related business. They can be used for work on client matters, practice and business development, associated research and other Firm matters.

B. Personal Use

The Firm recognizes that use of the Firm's Internet access resources for personal use may be necessary, just as personal telephone calls from the office may be necessary, and may be more efficient than using the telephone or leaving the office to conduct personal business. Personal use of the Firm's Internet access resources is permitted subject to this policy. The capacity of the Firm's communications lines to the Internet is not unlimited and, therefore, Firm-related uses have priority at all times.

C. Permitted Uses

1. Downloading of Text and Other Non-Executable Files

For Firm-related business, users, in their discretion, may download text and other non-executable files. Users are encouraged, where possible, to download large files (whether for Firm-uses and always for personal uses) during off-peak periods (e.g., evening hours), when there is likely to be less congestion on the Firm's communications lines to the Internet. For personal use, users should attempt, where possible, to determine the size of a file before downloading and avoid downloading audio, video or graphics files, or any other files that are in excess of twenty pages; only print out a downloaded file when, having checked with other users, there are no other competing Firm-related needs for the printer; and not print out very large files.

2. Interactive Sites

Users of the Internet may need to access Web sites or other Internet locations that require user registration or for which a charge is imposed. Users also may need to access or upload information to other interactive sites, such as bulletin boards or private or public chat rooms. Subject to the Firm's Policy Relating to Use of E-Mail (which prohibits subscribing to personal listservs at the Firm, limits personal use to short messages and asks that users try to limit the receipt of lengthy personal messages from correspondents), access to such sites and locations is permitted in accordance with the following:

- Registration using a Firm e-mail address is permitted.
- Whenever the user registers using a Firm e-mail address, participates in a listserv, enters a chat room, sends or otherwise uploads information, the inclusion of the domain name "lawfirm.com" indicates that the user is affiliated with the Firm. Users should be sensitive to any such affiliation (whether implicit or express) and, for uses that are obviously Firm-related, they must be authorized to engage in interactions or upload information that identifies their relationship to the Firm.
- If a Web site or other Internet location charges for access or to obtain relevant information, users should charge, or authorize another to charge, such fees to their Firm-issued or personal credit cards. Where such charges are required for access in connection with Firm-related matters, they are reimbursable in accordance with usual Firm policies and procedures.
- Participation in interactive games or in other similar interactive sites is not permitted for personal use.

D. Prohibited Uses

Internet access from the Firm is prohibited for objectionable activity and the following activities are expressly prohibited:

- Accessing (including browsing) any sexually-oriented or other similar "adult" Web sites, news groups or other Internet locations. Users are forbidden from undertaking any other activity that is intended to cause sexually-oriented or other "adult" materials to be downloaded to, or to be otherwise associated with, the Firm.
- Accessing (including browsing) any other Web sites, news groups or other Internet locations for purposes of gambling or engaging in any illegal activity.
- Downloading executable programs (e.g., self-extracting zip files) or program modules (i.e., software applications or applets), or installing executable attachments to e-mail, except as authorized by the Information Services Department, to protect the Firm's computer systems from viruses and to prevent incompatibility with Firm-provided software.
- Conducting any ongoing non-Firm business activity.

III. Confidentiality Considerations

Disclosure of user information is inherent in Internet usage. Users should be aware that they may be inadvertently disclosing confidential information about themselves and the Firm to Web site operators or third parties.

Particularly when Internet usage is undertaken in connection with client-related matters, users should be aware that Web sites and other Internet locations are capable of monitoring and tracking user-specific and Firm usage, the frequency and length of user visits, any items searched and any information that was retrieved and downloaded.

When Web sites and other Internet locations require information about the Firm or its resources as a condition of registration or access, users should not disclose sensitive or proprietary information. Providing public information about the Firm is permissible, but users should clear any disclosure of proprietary information with the Information Services Department.

Many Web sites use "cookies," which are files that are sent to a user's hard drive and allow Internet servers to keep track of specific user information. In the interests of maintaining user privacy and the confidentiality of information about the Firm, its users and their usage patterns, the Firm's Internet browser has been modified to require the express consent of the user before a Web site is allowed to install a cookie on a user's personal computer. In most cases, Web sites remain fully accessible even when a user declines to permit the cookie to be installed.

IV. Privacy

Consistent with the tradition of the Firm, we respect the privacy of all users of the Firm's Internet access resources. Personnel at the Firm do not routinely monitor users in their Internet-related activities. Nevertheless, all users are put on notice that the Firm tracks Internet usage and is aware of which sites (including the Web, news groups and other Internet locations) are visited by which users. It uses computer programs to check for and log patterns of activity, routing information and length of Internet access to particular sites and locations, and has the capability to monitor the contents of uploads and downloads.

Accordingly, no user of the Firm's Internet access resources has (or should expect to have) any expectation of privacy. (The Firm will, of course, respect its professional and legal obligations not to disclose client confidences.) Whether for the purposes of managing those resources and traffic flow, assuring system security, verifying and ensuring compliance of all persons with Firm policies or applicable law, or for any other reason, the Firm specifically reserves the right (from time-to-time or at any time), to intercept, divert, discard, access or review any Internet communication, other electronic communications or file, or any contents of such communication, or any other information created on, transmitted over or stored in Firm or service provider facilities, whether incoming or outbound, and whether at the time of transit or thereafter.

The Firm also reserves the right to disclose to other persons or otherwise use the contents of any Internet communication or any other electronic communications or file for any of the foregoing purposes, as well as for the purposes of complying with or assisting law enforcement officials or legal authorities who may, by subpoena, search warrant or otherwise, seek review of such communications, or for the purposes of litigation or other legal proceedings.

The only persons authorized by the Firm to intercept, divert, access, disclose or review any Internet communication, other electronic communications or file, or any contents of such communication, without the consent of the sender or recipient, is the Director of the Firm's Information Services Department.