PANNONE
LOPES
DEVEREAUX &
WEST LLC

counselors at law

Best Practices Series
Document Retention and Best Practices

1. Sarbanes Oxley Act provides guidance to businesses

Sections 802 and 1102 of SOX make it a crime to alter, cover up, falsify, or destroy any document or tangible object in order to prevent its use in any official proceeding. The act or attempt to alter, conceal or destroy records with intent to impair use in an official proceeding may be found to be obstruction of justice under SOX. Those responsible for the preservation of records in the business setting should note that the definition of documents includes electronic information and communications. A violation of the above noted sections may result in extensive fines and/or imprisonment for up to 20 years.

2. "Best Practices" relating to the retention and destruction of documents

In the financial setting, SEC Rule 210.2-06 requires accountants and audit committees to keep all records, work papers, and other documents including memoranda, correspondence, and communications for a period of 7 years. In all circumstances in which a company is notified of an official proceeding or investigation company policy should dictate the immediate termination of actions involving the destruction of documents.

It is imperative that all businesses maintain an up to date internal policy regarding document destruction. A comprehensive policy must be strictly enforced in order to ensure the requisite protections against what may be considered an illegal activity. The document retention/destruction policy must be clearly written, effectively communicated to staff with the goal of strict adherence. It is prudent for business to incorporate the essence of SEC rule 210.2-06 which is strictly applicable to accountants when dealing with all important financial documents, contracts, and other important documents. Adherence to a Best Practices model dictates that in those circumstances in which the course of action is unclear, document retention is prudent.

3. How do the SOX rules apply to electronic documents, emails, voicemail, instant messages and other electronically stored media?

It is important to note that the application of the SOX rules are universal as it relates to the retention and destruction of electronic files and communications. A prudent document retention policy will include back-up procedures, archiving, and other systematic fail safe mechanisms to retention. It is generally prudent for the retention of important documents and communications for a period of at least 7 years depending upon the industry standard and specific circumstances. This policy would also apply to email, voicemail, and instant message logs must also be retained.

The treatment of instant messaging requires a policy decision that is consistent with the company's overall

retention procedures. In general, if a company permits instant messaging as a means of communication, instant message logs should also be retained in accordance with applicable policy.

The Federal Rules of Civil Procedure have recently been modified to address the discovery of electronic documents and information. In order to comply with the modifications in the procedural rule changes businesses are required to develop and implement retention policies regarding electronic data. It is equally important for companies to develop and implement programmatic changes that will result in efficient methods by which to access and search for data when required under the rules in order for compliance to be an economic exercise. Deleted data, meta data, voicemail, temporary files, all forms of e-mail, backup tapes and other forms of electronic information have been found admissible and discoverable under the new discovery rules. It is also important to note that that storage media found in PDAs, Blackberries and laptops have been found discoverable.

The importance of developing retention policies and procedures for electronic data is learned from the level of fines and sanctions imposed upon corporations found to be in violation of discovery rules. Examples are as follows:

§ $10 million fine by the SEC against Bank of America;

§ $SEC upon 5 differenimposed by the

8.25 million fine

t financial firms;

§ $Districtmillion fineAltria; andby US 2.75 Court on imposed

§ $Morgan Stanley for electronic 1

billion judgment against

preventing economic sanctions during litigation procedures.

4. Imprisonment is sometimes the sanction of non-compliance

Unauthorized destruction of documents relating to any official government proceeding may result in imprisonment if the violation is severe. The actions by courts and federal agencies have certainly been noted by accountants when courts issue ten year prison sentences to a colleague for non-compliance with retention rules. If the document destruction is found to be in bad faith rather than inadvertent, the Federal Sentencing Guidelines permit judges to increase fines and sentences. The incentive to develop and adhere to strict document retention policies is learned from the sanctions and fines levied for violation of Rules 34 and 26 of the Federal Rules of Civil Procedure.

5. How do companies and individuals protect against severe fines and penalties?

A. Review and Revise - The first step is a complete review and revision of internal policies addressing document retention and destruction. The nature and scope of the policies required regarding document retention and destruction based should incorporate industry standards and use SOX as a best practices standard. Make certain that the policy must be concise and comprehensive.

B. Electronic Information - Document retention and destruction policies should clearly address electronic information which include retention and overwriting backup tapes, retention of email and voicemail files, and effective searchable backup of all important discovery related issues.

Best Practices dictates that a written retention policy is essential to

electronic information.

C. Monitoring activities - Strict adherence in the areas of internal and external policies. Inconsistencies inretention and destruction policies and procedures may evidence bad faith.

D. STOP Destruction of documents and data as early as possible - All destruction procedures should be halted as soon as the company is aware of possible legal proceeding or issue is discovered. Heavy sanctions have been levied upon firms who destroyed data and documents relevant to official proceedings, even where mere negligence or failure to inform all the necessary individuals led to destruction of relevant information.

E. Educate Staff - Communicate routinely the importance of compliance with document management, retention, and destruction policies. Ensuring that documents and data are stored and managed according to policy saves time and money when this information must be searched at a later date. Education as to the importance of adherence to policies will help to prevent accidental destruction of relevant information. Staff should understand that information is discoverable, even deleted electronic information, and may be asserted against the company.

6. What are the basic elements of a document management, retention, and destruction policy look like?

A. Statement of Purpose - Explain the reasoning behind the policy and list purposes such as compliance with relevant law, ensuring that valuable documents are available when needed, and the proper disposal of documents that are no longer necessary.

B. Applicable Documents - The company must distinguish between documents that are essential documents and those that are non-essential. Essential documents should include:

1. those necessary to meet government retention, reporting and compliance requirements; 2.
contracts;
3. insurance policies;
4. human resource and personnel files;
5. financial and audit information;
6. intellectual property;
7. official correspondence;
8. policies and procedures; and 9. any other essential business documents used in the course of business and its governance.

C. Non-Essential Documents - There are also a large number of documents for which retention serves little purpose and may expose the company to additional costs and legal liability. These include personal email and correspondence, document drafts, and many others. Such non-essential documents should be destroyed according to a written retention policy, *with the exception of documents relevant to or discoverable in potential official proceedings.* Important correspondence such as email or voicemail should be saved to a designated backup source and destroyed according to the same principles as the above documents.

D. Length of Retention - Companies should use the SEC standard for 7 years for all important documents unless there is a superseding industry standard. If there is no specific legal requirement a company should weigh the costs and benefits of retention and destruction.

E. Have a Clear Procedure for Halting Destruction - When an official proceeding such as a lawsuit is even reasonably foreseeable all destruction should be stopped. Establish a chain of command that establishes responsibility for ensuring that all potential proceedings are communicated to the necessary individuals and that the policy is complied with.

This update is a summary for general Information and discussion only. It is not a complete analysis and may not be relied upon as legal advice. Please contact Gary R. Pannone, Esquire for further consultation at 401-824-5115 or send an email to him at gpannone@pldw.com