INTERIORVAULT
SECURE DOCUMENT STORAGE & DESTRUCTION

INFORMATION DISPOSAL & RISK MANAGEMENT

1. Every Business Has Information That Requires Destruction

All businesses have occasion to discard confidential data. Customers lists, price lists, sales statistics, drafts of bids and correspondence, and even memos, contain information about business activity which would interest any competitor. Every business is also entrusted with information that must be kept private. Employers and customers have the legal right to ensure, and have this data protected.

Without the proper safeguards, information ends up in the dumpster where it is readily and legally, available to anybody. The trash is considered by business espionage professionals as the single most available source of competitive and private information from the average business. Any establishment that discards private and proprietary data without the benefit of destruction, exposes itself to the risk of criminal and civil prosecution, as well as the costly loss of business.

2. Stored Records Should Be Destroyed On A Regular Schedule

The period of time that business records are stored should be determined by a retention schedule that takes into consideration their useful value to the business and the governing legal requirements. No record should be kept longer than this retention period.
By not adhering to a program of routinely destroying stored records, a company exhibits suspicious disposal practices that could be negatively construed in the event of litigation or audit. Also, new Privacy Act legislation requires that, in the event of a law suit, each party provide all relevant records to the opposing counsel within 60 days of the defendants initial response. If either of the litigants does not fulfill this obligation, it will result in a summary finding against them. By destroying records according to a set schedule, a company appropriately limits the amount of materials it must search through to comply with this law.

From a risk management perspective, the only acceptable method of discarding stored records is to destroy them by a method that ensures that the information is obliterated. Documenting the exact date that a record is destroyed is a prudent and recommended legal precaution.

3. Incidental Business Records Discarded On A Daily Basis Should Be Protected

Without a program to control it, the daily trash of every business contains information that could be harmful. This information is especially useful to competitors because it contains the details of current activities. Discarded daily records include phone messages, memos, emails and address's, misprinted forms, drafts of bids and drafts of correspondence.

INTERIOR VAULT | 661 W. Athabasca Street, Kamloops, BC V2H 1C5
Local: (250) 372-1897 | Fax: (250) 434-7487 | Toll Free Number: 1-866-772-9154
records.admin@interiorvault.com | www.interiorvault.com

All businesses suffer potential exposure due to the need to discard these incidental business records. The only means of minimizing this exposure is to make sure such information is securely collected and destroyed. Today, personal information starts with; a name, phone number and email address – it's that simple.

4. Recycling Is Not An Adequate Alternative For Information Destruction.
To extract the scrap value from office paper, recycling companies use unscreened, minimum wage workers, to extensively sort the paper under unsecured conditions. The "acceptable" paper is stored for indefinite periods of time until there is enough of a particular type to sell. The sorted paper, still intact, is then baled and sold to the highest bidder, often overseas, where it may be stored again for weeks or even months until it is finally used to make new products.

There is no fiduciary responsibility inherent in the recycling scenario. Paper is given away or sold and, by doing so, a company gives up the right say in how it is handled. There is, also, no practical means of establishing the exact date that a record is destroyed. In the event of an audit or litigation, this could be a legal necessity. And, further, if something of a private nature does surface, the selection of this unsecured process could be interpreted as negligent. For all these reasons, the choice of recycling as a means of information destruction is undesirable from a risk management perspective.

If environmental responsibility is a concern, materials may be recycled after they are destroyed or a firm can contract a service that will destroy the materials under secure conditions before recycling them. Any recycling company that minimizes the need for security has its own interests in mind and should be avoided.

5. A Certificate Of Destruction Does Not Relieve A Company From Its Obligation To Keep Information Confidential
Any company contracting an information destruction service should require that it provide them with a signed testimonial, documenting the date that the materials were destroyed. The "certificate of destruction", as it is commonly referred, is an important legal record of compliance with a retention schedule. It does not, however, effectively transfer the responsibility to maintain the confidentiality of the materials to the contractor.

If private information surfaces after the vendor accepts it, the court is bound to question the process by which the particular contractor was selected. Any company not showing due diligence in their selection of a contractor that is capable of providing the necessary security could be found negligent. Be sure your contractor is is a member in good standing with Naid Canada.

And, from a practical standpoint, if proprietary or private information is lost or leaked by the fraud or negligence of a vendor, the obligations of that vendor are irrelevant.

The firm whose information falls into the wrong hands stands to lose the most, either from loss of business, prosecution or unfavourable publicity.

Since a business cannot transfer its responsibility to maintain confidentiality, it must be certain that it is dealing with a reputable company with superior security procedures. Unfortunately, there are those information destruction services that provide certificates of destruction while having no semblance of security and, in some cases, no destruction process available to them. Anyone interested in contracting a data destruction service is advised to thoroughly review their policies and procedures, conduct an initial site audit and conduct subsequent unannounced audits.

6. Most Records Storage Companies Do Not Have The Equipment To Provide Shredding Services

Many commercial records storage facilities offer records destruction as a service to their customers. However, in a survey conducted by the National Association for Information Destruction, a majority of the commercial storage firms were found lacking the equipment necessary to provide the service themselves. It is a common practice in that industry to subcontract the destruction of the records. In some cases, disreputable storage firms were found misleading their customers by charging for secure records destruction, while the materials were being sold to a recycling company for scrap.

Any business using a commercial records storage firm should inquire as to the nature of the destruction services that are available. It is an unacceptable risk to permit a storage firm to select a subcontractor to provide the records destruction service. The owner of the records is ultimately responsible for their security and, therefore, should be selecting the vendor directly.

7. Internal Personnel Should Not be Responsible To Destroy Certain Information

Common sense dictates that payroll information and materials that involve labour relations or legal affairs, should not be entrusted to lower level employees for destruction. But, beyond that, competition sensitive information is best protected from them as well. It has been established, time and again, that employees are the most likely to realize the value of certain information to competitors. Lower wage employees often have the economic incentive to capitalize on their access to it. The only acceptable alternatives are to have the materials destroyed under the supervision of upper management or by a carefully selected, high security service.

8. Information Protection Is A Vital Issue To Senior Management.

In a survey conducted by the Conference Board, top executives from 300 companies ranked the security of company records as one of the top five critical issues facing business. When asked which issues required immediate attention and policy development, the security of company records ranked second only to employee health screening.