Summary Statement of Principles
Regarding the Development of Guidelines
Respecting Destruction and Disposal of Information and Protection of Privacy

Introduction

As the national association representing companies that specialize in secure information and document destruction, NAID Canada believes:

- Every organization should be legally obligated to appropriately safeguard personal information;
- Organizations need to be as careful in the destruction of documents as they are in protecting them on their premises;
- There is a significant risk to reputation and competitive position for organizations that do not use secure document destruction techniques; and
- Protection of sensitive discarded information is a matter of national (economic) security

Guidelines for the Destruction and Disposal of Information and Protection of Privacy

In recognition and support of the aforementioned beliefs, NAID Canada recommends consideration of the following principles, as the basis for development and implementation of efficient and effective guidelines respecting destruction and disposal of information and protection of privacy in support of Bill 38, *The Personal Information Protection Act*.

Principle: Why should we destroy and dispose of information and protect privacy?

Because information is only as secure as the weakest link in its lifecycle

To protect privacy, any standards for the proper collection and management of information must include requirements for proper disposal and destruction of this same information. The reality is that identity theft and information-based fraud are among the fastest growing crimes – and they are growing because of improper disposal and destruction. Dumpsters and garbage receptacles are recognized as a primary source for personal and corporate information theft. Failure to adequately address the disposal and destruction of information contributes to the growth in these criminal activities and jeopardizes protection of privacy for consumers and businesses alike.

- In order to comply with legislation and regulations;
- In recognition of the fact that recycling is not an adequate alternative for information destruction. Information can and should be recycled, but only after it has been properly destroyed; and
- To help protect against identity theft, a rapidly growing crime that is currently costing Canadians millions of dollars a year. Identity thieves will migrate to those jurisdictions with lesser controls and sub-standard protection of privacy.

Principle: What should be destroyed and disposed of?

Every organization has information that requires destruction and disposal

All organizations with employees and/or customers have occasion to discard confidential data. Customers lists, price lists, sales statistics, drafts of bids, correspondence and even memos, contain information about activities which may interest competitors or other unauthorized parties. Every organization is also entrusted with information that must be kept private. Employees and customers have the legal right to have this data protected. Without the proper safeguards, information ends up in a dumpster where it is readily, and legally, available to anybody. 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 modern destruction methods exposes itself to the risk of prosecution, as well as costly loss of business and reputation.

- *Customer* and/or *employee* records containing *personal* or *identifying* information (e.g.s. name, phone number, address, social insurance number, etc.); and
- Protection of information should include *incidental business records* which are discarded on a daily basis (examples of discarded daily records include phone messages, memos, forms, drafts of bids, invoices and correspondence).

Principle: Who should be responsible for destruction and disposal of information?

Internal personnel should not be responsible for destroying certain information

Common sense dictates that certain information and materials including payroll, labour relations, legal affairs and medical information, by way of illustration, should not be entrusted to employees for destruction. But, beyond that, competition sensitive information is best protected as well. Unfortunately, it has been established that employees are the most likely to realize the value of certain information to competitors. And, lower wage employees may 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.

- Ensure that *employees* who are charged with the disposal and destruction of information are *limited in their access to appropriate information; and*
- *Screen/select external vendors* based on consideration of a number of criteria including *licensing, insurance, bonding, safeguards, security and volume of information they can handle*

Principle: Where should the information be destroyed and disposed of?

Information can be destroyed and disposed of in three (3) ways:

1. I*n-house* – done on the premises by employees using a proper site-based shredder;
2. *Mobile* – a vendor brings a destruction vehicle that, at a minimum, provides physical security from unauthorized access before information is destroyed and that materials remain in the immediate custody of the authorized vendor until the mobile shredding equipment destroys them; or
3. *Plant-based* – information is picked up and taken to a facility where it is destroyed and disposed of in accordance with NAID certification standards including:

    - Requiring non-employees entering the facility to sign in and out of the facility;
    - Providing a secure area within the facility devoted only to destroying media;
    - Preventing unauthorized access to the designated secure destruction area;
    - Ensuring that materials are always attended by a company employee or physically secured from unauthorized access while in the custody of the destruction contractor before they are destroyed;
    - All materials are securely contained during transfer from the customer's custody to transportation vehicle to prevent loss from wind or other atmospheric conditions;
    - There is an alarm system in place and utilized when the secure destruction facility is unoccupied;
    - There is a closed circuit internal video monitoring all access points and processing activities in the secure destruction facility;
    - All vehicles used to transfer client records will have applicable government inspection for road worthiness; and
    - All vehicles used for the transfer of client records have lockable/securable cabs and lockable/securable fully enclosed boxes

Principle: When should information be destroyed and disposed of?

Stored records should be destroyed on a regular schedule

The period of time that records are stored should be determined by a retention schedule that takes into consideration their useful value 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, an organization exhibits suspicious disposal practices that could be negatively construed in the event of litigation or audit. 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 precaution.

- *Incidental business records* should be destroyed and disposed of on a timely basis
- *Discarded records stored on-site* must be securely contained between the time of collection and final destruction

Principle: How should information be destroyed and disposed of?

Paper media can be destroyed in one of four (4) ways, in accordance with the NAID specifications outlined below:

1. *Continuous Shred* – indefinite length and a cutter width of 5/8 inch (1.59 cm) or less;
2. *Cross Cut/Pierce and Tear* – maximum cutter width of shortest dimension is 1 inch (2.54 cm) with the maximum length of the cut strip of 2.5 inches (6.35 cm);
3. *Pulverized* (equipment with screens) – uses screen with 2-inch (5.08 cm) diameter holes; or
4. *Pulping and incineration*

- Equipment or processes used to destroy *micro-media* must produce a particle size of 1/8 inch (.32 cm) maximum;
- Standard operating practice dictates that all client records are *destroyed within 72 hours* of transfer from the client. Exceptions include acts of God, breakdowns or client instructions (or permission) to retain the media for a longer period;
- Destroyed materials must be disposed (sold, gifted or discarded) in a responsible manner; and

Upon completion of the destruction process, a signed *Certificate of Destruction* should be provided by the vendor to the client, confirming that the records transferred from the client to the vendor have been destroyed.

General Provisions Respecting the Destruction and Disposal of Information and Protection of Privacy

In addition to the specific principles identified above, NAID Canada believes, that at a minimum, guidelines developed in support of Bill 38, The *Personal Information Protection Act* should:

1. Include the following definitions:

   Record…an item of information that can be stored in any medium;
   Discard…casting aside information once the record is no longer required;
   Disposal…the time period between discarding and physical destruction of records;
   Destruction…physical destruction of records to ensure reconstruction of the information (or parts thereof) is not possible;
   Identifying information… data or information pertaining to an individual, organization or business that could result in damage, harm or loss, if used for purposes other than intended;
   Personal Information…any information that could identify a business, organization or individual that is recorded in any form;
   Recycling…material that has not been adequately destroyed and could allow for reconstruction of information (note: recycling and reuse of material is acceptable after it has been obliterated through shredding or alternative methods)

2. Outline the conditions under which records containing personal and private information may be discarded by organizations, including, but not limited to:

   - requiring shredding of customers records before they are discarded;
   - requiring that personal information contained in customers records be erased before they are discarded;
   - requiring that personal information contained in customers records be made unreadable before they are discarded; and
   - taking (reasonable) actions to ensure that no unauthorized persons will gain access to personal information contained in customers records between the time of disposal and destruction

3. Specify that any organization with customers and/or employees be required to take reasonable steps to effectively dispose of information that requires destruction consistent with the definitions to be included in the Act;

4. Assign responsibility for compliance to individuals in each organization or entity to ensure accountability; and

5. Highlight what sanctions or penalties an organization could face if they fail to demonstrate that they have used due diligence in their attempt to properly discard and dispose of records containing personal information

Conclusion

Organizations need to be as careful in the disposal and destruction of documents and records as they are in collecting and maintaining them. Failure to deploy secure destruction procedures will come at the expense of unassuming individuals who were not afforded the privacy protection they deserve and are entitled to.

British Columbia's new *Personal Information Protection Act* should ensure that personal information is appropriately safeguarded up to and including the point of destruction by incorporating provisions for disposal and destruction in the Act's supporting guidelines.

NAID Canada would like to thank the Ministry of Management Services for the opportunity to provide input into the guidelines that are currently in development. It is our understanding that there will be additional opportunities to provide input as you move forward. We welcome the opportunity to participate in this process.