

Commentary on Sample Policy on Destruction of Personal Information

1. **Effective date:** Act 136 (SB 2292), which requires businesses to securely dispose of personal information, is effective January 1, 2007.
2. **Required written policy:** Act 136 requires businesses to take “reasonable measures” to protect against unauthorized access of personal information in connection with disposal of documents and records, which include “[d]escribing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity.” The written policy may (but need not be) included in the company’s employee handbook. The policy must describe the procedures used by the business with respect to destruction and disposal of records.
3. **Designation of responsible employee:** The sample policy designates a “document destruction officer” who is responsible for oversight of the business’s destruction policies. Nothing in Act 136 requires such a designation. However, it is suggested that employers assign a manager or committee to oversee and coordinate document destruction throughout the enterprise. Centralized control of destruction policies and procedures should result in more efficient and comprehensive destruction practices.

The responsible employee or committee should determine the types of documents or records containing personal information which are handled by your company, the approximate volume of such documents and records, and should identify all employees responsible for handling documents and records containing personal information. After this assessment is concluded, your Company will be better able to determine what training should be conducted, what further destruction equipment (such as shredders or data destruction software) may be necessary, and whether outsourcing document destruction to a third party is cost-effective.

4. **Training for employees:** Although training is not specifically mandated by the statute, it seems obvious that reasonable compliance measures must include educating and training those employees who handle and dispose of personal information.
5. **Electronic/Optical storage:** Because large amounts of data containing personal information can be stored on hard drives, thumb drives, memory cards, cds, dvds, and other optical or electronic storage media, particular care should be taken when disposing of computer hardware, software, cds, dvds, and personal computing devices such as Palm Pilots, Blackberrys, etc. If you are utilizing a software destruction program, use a program which meets the standards of U.S. Department of Defense (“DOD”) directive 5220.22-M. See
5. **Technological advances may require future modification:** As technology advances, more and more devices are capable of storing data containing personal information, and identity thieves are becoming more adept at stealing that information. Your company should attempt to insure that its destruction policies keep up with advancements in technology.

Sample Policy On Destruction Of Personal Information

[DISCLAIMER: This material is being provided by the Hawaii Employers Council for illustrative and informational purposes only, is not intended to constitute legal advice, and should not be interpreted as legal advice. Prior to adopting this or any other document destruction policy, your business should consult with a competent attorney or information destruction consultant.]

The following describes the Company's official policy relating to the proper disposal of documents, electronic media, and other non-paper media containing "personal information." It applies to all employees who, in the course of their employment, dispose of or transfer paper documents, electronic media, or other media containing personal information. All disposal by Company employees of documents, electronic media, or non-paper media containing "personal information" generated or received in the course of business shall conform to this policy.

1. **Definitions**

- a. For purposes of this policy, "**personal information**" means either (1) a person's first name and last name, or (2) first initial and last name, or (3) a person's first name, as **well as any one of the following**:

- the person's social security number (unless redacted to the last four digits), or
- the person's driver's license number,
- the person's Hawaii identification card number; or
- any account number for a financial account, such as a bank account, checking account, pension account, 401(k) account, brokerage account, etc.

Examples of the types of documents and items which may include personal information are documents regarding health benefits, insurance, 401(k) accounts, pension accounts, IRA accounts, brokerage accounts, direct deposit of wages, pay slips, tax records, W-2 forms, I-9 forms, medical records, invoices, personal checks, charge card records, identification cards, insurance cards, etc. Many different types of documents have the potential to include personal information as defined by this policy.

- b. For purposes of this policy, "**electronic and other media**" shall include any non-paper material or media on which information can be stored or preserved, including, but not limited to, computer hard drives, zip drives, "thumb" drives, floppy disks, USB flash drives, memory sticks, magnetic tape, or other electromagnetic or electromechanical means of storing data, and includes optical storage media such as cds or dvds. It shall also include items such as identification cards, credit cards, or other non-paper material containing personal information.

2. **Oversight:** [The Company's IT Manager/HR Manager/Office Manager] has been designated as the document destruction officer generally responsible for oversight of the Company's destruction of personal information. He/she is responsible for questions regarding this policy, and should be contacted by any employee with questions regarding this policy. In addition, the document destruction officer shall be responsible for:

- identifying employees who handle and dispose of documents or electronic or other media containing personal information
- providing training for employees regarding the requirements of this policy and the procedures for the secure destruction of documents and electronic or other media containing personal information
- monitoring the purchase and proper maintenance of any equipment used for secure destruction (such as shredders and secure destruction software)
- conducting due diligence on any destruction services provided by a third party
- monitoring the Company's compliance with this policy and applicable law regarding secure disposal of personal information

3. **Review of documents or electronic and other media prior to disposal:** Prior to disposing of documents or electronic and other media by any non-secure method, all employees who dispose of documents or electronic and other media containing personal information must review the document or media to ensure that it does not contain personal information as defined by this policy.

4. **Destruction procedures for paper documents:** All employees disposing of paper documents, microfilm, photographs, negatives, and similar media which contain personal information must do so by one of the following methods:

- a. **Disposal of paper documents by the employee:** Employees who are disposing of documents containing personal information through shredding or pulverizing should check the document after destruction to determine whether the information contained therein can be read. If, after shredding or pulverizing, the information contained in a document can still be read, the document should be re-shredded, cross-shredded, or re-pulverized, and checked again. If an employee cannot shred or pulverize a document so as to make its contents unreadable, the document should be set aside for burning or other destruction methods. Contact the document destruction officer for further instructions.

- b. Documents to be destroyed by service provider : The company may contract with a third party for document destruction services. Disposal of documents containing personal information may be accomplished by placing the documents in secure disposal containers for disposal by the destruction service provider. The document destruction officer shall be responsible for determining the number and location of disposal containers and notifying employees of those locations.

5. **Destruction procedures for electronic media and other media**: An employee disposing of electronic media, or non-paper and non-electronic media containing personal information shall do so by one of the following methods:

- a. Computers, servers, and portable digital assistant (“PDA”) devices:

Before any computer, PDA, or other computing device containing personal information on its hard drive is sold, leased, donated, recycled, or otherwise transferred to a third party for further use, the hard drive(s) shall be erased and reformatted using a software program designed to ensure the secure destruction of personal information. Employees must only use software programs designated by the document destruction officer. If personal information cannot be securely erased from the device, the hard drive or other component containing the personal information shall be securely destroyed.

If any computer, server, PDA, or other computing device containing personal information is to be disposed of, rather than transferred to a third party for further use, the hard drive(s) of the device and any recording or memory unit of the device containing personal information shall either be physically removed and destroyed by breaking the drive, or the drive or unit must be wiped by a suitable degaussing magnet.

[*Optional*: Disposal may also be accomplished by providing the computer or computing device to a third-party destruction service provider designated by the document destruction officer.]

- b. Zip drives, floppy disks, etc. and optical storage media:

Prior to disposal, all electronic data storage media such as external hard drives, zip drives, tape drives, floppy disks, memory cards, memory sticks, USB flash drives, or other electronic storage media containing personal information shall have the data contained in the item destroyed by either wiping the media with a degaussing magnet, or by physically destroying the media through shredding or similar physical destruction.

CD's, DVD's, and other optical storage media must be disposed of by physical destruction of the media, such as by shredding.

Disposal may also be accomplished by providing the electronic storage media or optical storage media to a third-party destruction service designated by the document destruction officer.

c. Non-paper and non-electronic media:

Personal information may be recorded on non-paper and non-electronic media such as plastic identification cards, credit cards, celluloid film, etc. If such media consists of material (such as plastic credit cards) suitable for shredding or pulverizing, disposal should be accomplished in the same manner as paper documents. If such media is not suitable for shredding or pulverizing, an employee disposing of such media must contact the document destruction officer for disposal instructions. If in doubt as to the proper method of disposal, contact the document destruction officer.

6. **Reports of violations:** Employees should immediately notify the document destruction officer or their supervisor of any violation of this policy, or of any concerns they may have regarding the secure disposal or destruction of personal information.