

---

---

# A BILL FOR AN ACT

RELATING TO PERSONAL INFORMATION.

**BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:**

1 PART I

2 SECTION 1. The purpose of this Act is to implement the  
3 recommendations of the December 2007 report of the Hawaii  
4 identity theft task force to protect the security of personal  
5 information collected and maintained by state and county  
6 government agencies.

7 PART II

8 SECTION 2. Chapter 487J, Hawaii Revised Statutes, is  
9 amended by adding a new section to be appropriately designated  
10 and to read as follows:

11 "§487J-A Policy and oversight responsibility. (a) By  
12 September 1, 2009, each government agency shall designate an  
13 agency employee to have policy and oversight responsibilities  
14 for the protection of personal information.

15 (b) The designated agency employee shall:

16 (1) Ensure and coordinate agency compliance with this  
17 chapter, chapter 487N, and chapter 487R;



- 1       (2) Assist individuals who have identity theft and other  
2           privacy-related concerns;
- 3       (3) Provide education and information to agency staff on  
4           privacy and security issues;
- 5       (4) Coordinate with state, county, and federal law  
6           enforcement agencies on identity theft investigations;  
7           and
- 8       (5) Recommend policies and practices to protect individual  
9           privacy rights relating to the individual's personal  
10           information."

11       SECTION 3. Section 487J-1, Hawaii Revised Statutes, is  
12 amended by adding a new definition to be appropriately inserted  
13 and to read as follows:

14       "Personal information" has the same meaning as in section  
15 487N-1."

16       SECTION 4. Chapter 487N, Hawaii Revised Statutes, is  
17 amended by adding three new sections to be appropriately  
18 designated and to read as follows:

19       "§487N-A Information privacy and security council;  
20 established; duties; reports. (a) There is established an  
21 information privacy and security council within the department  
22 of the attorney general for administrative purposes only.



1 Members of the council shall be appointed no later than  
2 September 1, 2008, by the governor without regard to section  
3 26-34 and shall be composed of representatives of state and  
4 county agencies.

5 (b) By January 1, 2009, the council shall submit to the  
6 legislature a report of the council's assessment and  
7 recommendations on initiatives to mitigate the negative impacts  
8 of identity theft incidents on individuals. The report shall  
9 emphasize assessing the merits of identity theft passport and  
10 identity theft registry initiatives that have been implemented  
11 in other states.

12 (c) No later than June 30, 2009, the council shall develop  
13 guidelines to be considered by government agencies in deciding  
14 whether, how, and when a government agency shall inform affected  
15 individuals of the loss, disclosure, or security breach of  
16 personal information that can contribute to identify theft. The  
17 guidelines shall provide a standardized, risk-based notification  
18 process in the instance of a security breach.

19 (d) The council shall review the individual annual reports  
20 submitted by government agencies, pursuant to section 487N-C and  
21 submit a summary report to the legislature no later than twenty  
22 days prior to the convening of the regular session of 2010 and



1 each year thereafter. The summary report shall include the  
2 council's findings, significant trends, and recommendations to  
3 protect personal information used by government agencies.

4 The initial report to the legislature shall also include  
5 proposed legislation to amend section 487N-2 or any other law  
6 that the council deems necessary to conform to the guidelines  
7 established under subsection (c).

8 **§487N-B Personal information security; best practices;**  
9 **websites.** (a) The council shall identify best practices to  
10 assist government agencies in improving security and privacy  
11 programs relating to personal information. No later than March  
12 31, 2009, the council shall identify best practices relating to:

13 (1) Automated tools;

14 (2) Training;

15 (3) Processes; and

16 (4) Applicable standards.

17 (b) No later than July 31, 2009, the best practices  
18 identified by the council shall be posted on each government  
19 agency's website in a manner that is readily accessible by  
20 employees of the government agency.

21 **§487N-C Personal information system; government agencies;**  
22 **annual report.** (a) Effective January 1, 2009, any government



1 agency that maintains one or more personal information systems  
2 shall submit to the council an annual report on the existence  
3 and character of each personal information system added or  
4 eliminated since the agency's previous annual report. The  
5 annual report shall be submitted no later than September 30 of  
6 each year.

7 (b) The annual report shall include:

8 (1) The name or descriptive title of the personal  
9 information system and its location;

10 (2) The nature and purpose of the personal information  
11 system and the statutory or administrative authority  
12 for its establishment;

13 (3) The categories of individuals on whom personal  
14 information is maintained, including:

15 (A) The approximate number of all individuals on whom  
16 personal information is maintained; and

17 (B) The categories of personal information generally  
18 maintained in the system, including

19 identification of records that are:

20 (i) Stored in computer accessible records; or

21 (ii) Maintained manually;

22 (4) All confidentiality requirements relating to:



- 1           (A) Personal information systems or parts thereof
- 2                   that are confidential pursuant to statute, rule,
- 3                   or contractual obligation; and
- 4           (B) Personal information systems maintained on an
- 5                   unrestricted basis;
- 6       (5) Detailed justification of the need for statutory or
- 7                   regulatory authority to maintain any personal
- 8                   information system or part thereof on a confidential
- 9                   basis for all personal information systems or parts
- 10                   thereof that are required by law or rule;
- 11       (6) The categories of sources of personal information;
- 12       (7) The agency's policies and practices regarding personal
- 13                   information storage, duration of retention of
- 14                   information, and elimination of information from the
- 15                   system;
- 16       (8) The uses made by the agency of personal information
- 17                   contained in any personal information system;
- 18       (9) The identity of agency personnel, by job
- 19                   classification, and other agencies, persons, or
- 20                   categories to whom disclosures of personal information
- 21                   are made or to whom access to the personal information
- 22                   system may be granted, including the purposes of



1           access and any restrictions on disclosure, access, and  
2           redisclosure;

3       (10) A list identifying all forms used by the agency in the  
4           collection of personal information; and

5       (11) The name, title, business address, and telephone  
6           number of the individual immediately responsible for  
7           complying with this section.

8       (c) For purposes of this section:

9           "Personal information system" means any manual or automated  
10          recordkeeping process that contains personal information and the  
11          name, personal number, or other identifying particulars of a  
12          data subject."

13           SECTION 5. Section 487N-1, Hawaii Revised Statutes, is  
14          amended by adding a new definition to be appropriately inserted  
15          and to read as follows:

16           "Council" means the information privacy and security  
17          council established under section 487N-A."

18           SECTION 6. There is appropriated out of the general  
19          revenues of the State of Hawaii the sum of \$                or so  
20          much thereof as may be necessary for fiscal year 2008-2009 for  
21          three staff analyst positions to support the work of the



1 information privacy and security council established pursuant to  
2 this Act.

3 The sum appropriated shall be expended by the department of  
4 the attorney general for purposes of this part.

5 PART III

6 SECTION 7. Act 137, Session Laws of Hawaii 2006, as  
7 amended by Act 183, Session Laws of Hawaii 2007, section 11, is  
8 amended by amending section 3 to read as follows:

9 "SECTION 3. This Act shall take effect on July 1, [~~2008-~~  
10 2009."]

11 PART IV

12 SECTION 8. Practices and procedures relating to security  
13 of laptops, removable data storage devices, and communication  
14 devices. By December 31, 2008, the information privacy and  
15 security council established under section 487N-A, Hawaii  
16 Revised Statutes, in consultation with the information and  
17 communication services division of the department of accounting  
18 and general services, and the information technology divisions  
19 of the respective counties, shall develop recommended practices  
20 and procedures to provide guidance to information technology  
21 managers in all government agencies relating to the security of  
22 laptops, removable data storage devices, and communication





1 devices used to remotely access applications installed on state  
2 or county networks. The council shall include recommendations  
3 on best practices and standards for protecting personal  
4 information that may be used with, stored on, or transmitted by  
5 the foregoing devices.

6 PART V

7 SECTION 9. Third party personal information use  
8 contractual provisions. Effective September 1, 2008, any  
9 government agency that contracts with third parties to provide  
10 support services on behalf of the agency shall include, in all  
11 new or renewed contracts, provisions to protect the use and  
12 disclosure of personal information administered by the agency.

13 Provisions relating to personal information protection in  
14 contractual agreements with third parties shall require:

- 15 (1) Implementation of technological safeguards acceptable  
16 to the government agency to reduce exposure to  
17 unauthorized access to personal information;
- 18 (2) Mandatory training on security awareness topics  
19 relating to personal information protection for  
20 employees of the third party;
- 21 (3) Confidentiality agreements to be signed by third party  
22 employees acknowledging that:



- 1 (A) The personal information collected, used, or  
2 maintained by the government agency is  
3 confidential;
- 4 (B) Access to the personal information is restricted  
5 to the minimum necessary; and
- 6 (C) Use of the personal information is restricted to  
7 uses consistent with the services subject to the  
8 contractual agreement;
- 9 (4) Clarification that no personal information shall be  
10 retained or used for a purpose other than that for  
11 which it was originally collected by the third party  
12 and all copies of personal information records shall  
13 be destroyed by the third party at the conclusion of  
14 the contract;
- 15 (5) Prompt and complete disclosure of security breaches;  
16 and
- 17 (6) A complete log of disclosures made of the government  
18 agency personal information.

19 As used in this section, "technological safeguards" means  
20 the technology and the policy and procedures for use of the  
21 technology to protect and control access to personal  
22 information.



## PART VI

1  
2 SECTION 10. (a) Guidance on recommended human resources  
3 practices to protect personal information. No later than  
4 January 1, 2009, the lead state and county government agencies  
5 that have primary responsibility for human resource functions  
6 shall develop and distribute to the appropriate government  
7 agencies written guidelines detailing recommended practices to  
8 minimize unauthorized access to personal information and  
9 personal information systems relating to personnel recruitment,  
10 background checks, testing, employee retirement and health  
11 benefits, and time-reporting and payroll issues. The  
12 recommended practices shall address, at a minimum:

- 13 (1) Physical safeguards for paper and electronic records  
14 stored onsite and offsite, as well as for removable  
15 storage media that includes laptop computers, USB  
16 storage devices, compact discs, and tapes;
- 17 (2) Administrative safeguards to control and monitor  
18 access to human resources personal information  
19 systems; and
- 20 (3) Technological safeguards to ensure the confidentiality  
21 and integrity of information transmitted over computer



1 networks, laptop computers, and removable storage  
2 devices.

3 (b) Definitions. For the purpose of this part:

4 "Administrative safeguards" means administrative actions,  
5 policies, and procedures to manage the selection, development,  
6 implementation, and maintenance of security measures to protect  
7 personal information and to manage the conduct of the workforce  
8 in relation to the protection of personal information.

9 "Physical safeguards" means physical measures, policies,  
10 and procedures to protect personal information systems and  
11 related buildings and equipment from natural and environmental  
12 hazards and unauthorized intrusion.

13 PART VII

14 SECTION 11. (a) Security breach notification policy. No  
15 later than September 1, 2009, all government agencies shall  
16 develop a written agency policy relating to notification of any  
17 security breach of personal information. The policy shall  
18 ensure appropriate safeguards to protect personal information  
19 and shall apply to electronic system and paper document records  
20 that contain personal information.

21 The security breach notification policy for government  
22 agencies shall consider guidelines established by the



1 information privacy and security council under section 487N-A  
2 Hawaii Revised Statutes, and shall include provisions to  
3 determine:

- 4 (1) Whether security breach notification is required;
- 5 (2) The timeliness of the notification;
- 6 (3) The source of the notification;
- 7 (4) The contents of the notification;
- 8 (5) The manner in which notification shall be provided;
- 9 and
- 10 (6) Recipients of notification.

11 (b) Security breach notification policy review and  
12 amendment. No later than September 1, 2009, all government  
13 agencies shall submit their security breach notification policy  
14 to the attorney general, appropriate corporation counsel, or  
15 county attorney for review and comment. A government agency's  
16 security breach notification policy shall be promptly amended to  
17 incorporate revisions recommended by the attorney general,  
18 corporation counsel, or county attorney after review of the  
19 security breach notification policy.

20 Beginning December 31, 2010, government agencies shall  
21 review their security breach notification policies by December  
22 31 annually and make amendments as necessary. Information



1 relating to a government agency's security breach notification  
2 policy, including any amendments, shall be disseminated to the  
3 appropriate employees in each government agency.

4 PART VIII

5 SECTION 12. Definitions. For purposes of this Act:

6 "Government agency" has the same meaning as in section  
7 487N-1, Hawaii Revised Statutes.

8 "Personal information" has the same meaning as in section  
9 487N-1, Hawaii Revised Statutes.

10 "Personal information system" means any manual or automated  
11 recordkeeping process that contains personal information and the  
12 name, personal number, or other identifying particulars of a  
13 data subject.

14 "Records" has the same meaning as in section 487N-1, Hawaii  
15 Revised Statutes.

16 "Security breach" has the same meaning as in section  
17 487N-1, Hawaii Revised Statutes.

18 SECTION 13. In codifying the new sections added by  
19 sections 2 and 4 of this Act, the revisor of statutes shall  
20 substitute appropriate section numbers for the letters used in  
21 designating the new sections in this Act.



1 PART IX

2 SECTION 14. Statutory material to be repealed is bracketed  
3 and stricken. New statutory material is underscored.

4 SECTION 15. This Act shall take effect on July 1, 2025.



**Report Title:**

Identity Theft; Personal Information; Government Agencies

**Description:**

Implements recommendations of the 12/2007 report of the Hawaii identity theft task force to protect the security of personal information collected and maintained by state and county government. (SB2803 HD1)

