**Information Privacy and Security Council**
**Meeting Agenda**
December 19, 2018
1:00 p.m.

**Videoconference Centers (VCC)**
Kalanimoku Bldg., 1151 Punchbowl St., Basement B10, Honolulu, HI 96813
Hilo State Office Bldg., 75 Aupuni St., Basement, Hilo, HI 96720
Wailuku State Office Bldg., 54 S. High St., 3rd Flr., Wailuku, HI 96793
Lihue State Office Bldg., 3060 Eiwa St., Basement, Lihue, HI 96766

I. Call to Order

II. Public Testimony on Agenda Items
*Interested persons may submit data or views to the Council: 1) in writing submitted in advance to Information Privacy and Security Council (IPSC), 1151 Punchbowl St., Room B-10, Honolulu, HI 96813; or 2) in person at any of the sites listed on this notice. Testimony must be related to an item on the agenda, and such person shall be required to identify the agenda item to be addressed by the testimony. Each individual or representative of an organization is allotted three minutes for testimony, or an amount of time otherwise designated in advance by the Chair.*

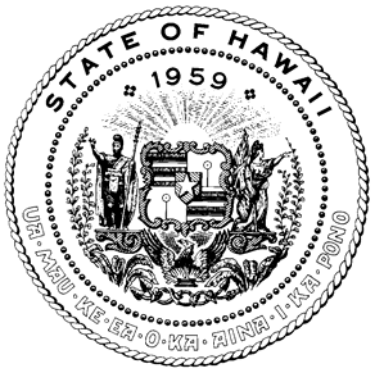
III. Annual Summary Report to the Legislature; Discussion and Appropriate Action

IV. Relating to Found Electronic Devices Legislation, Memo and Guideline; Discussion and Appropriate Action

V. Good of the Order
   a. Announcements
   b. Next meeting: February 20, 2019, 1:00 p.m.

VI. Adjournment

Individuals who require special needs accommodation are invited to call (808) 586-6000 at least three working days in advance of the meeting.




INFORMATION AND PRIVACY SECURITY COUNCIL

ANNUAL SUMMARY REPORT

DECEMBER XX, 2018

SUBMITTED TO

THE THIRTIETH STATE LEGISLATURE

**Information Privacy and Security Council**
**Annual Summary Report**
**December XX, 2018**

The Information Privacy and Security Council (IPSC) submits the following summary report on the existence and character of government agencies' personal information (PI) systems, pursuant to section 487N-5(d), Hawai‘i Revised Statutes (HRS).

The IPSC has received the individual annual reports submitted by government agencies of the State of Hawai‘i, City and County of Honolulu, Hawai‘i County, Maui County, and Kaua‘i County, in accordance with HRS section 487N-7. Enclosed are the council's findings and summary of recent legislation to protect PI handled by government agencies.

## BACKGROUND

Any State or local government agency that maintains one or more personal information systems is required under section 487N-7, Hawaii Revised Statute (HRS), to submit to the IPSC an annual report on the existence and character of each PI system added or eliminated since the agency's previous annual report.

The IPSC continued with the "paperless" method of reporting to all jurisdictions and departments. All agencies had the option of using the IPSC's Privacy Impact Assessment (PIA) Online Form or fillable PDF, accessible to agencies through the IPSC website (ipsc.hawaii.gov), to comply with their reporting requirement. Although use of the PIA Online Form was strongly encouraged, agencies still had the option to submit their reports by email or by mail, if they wished.

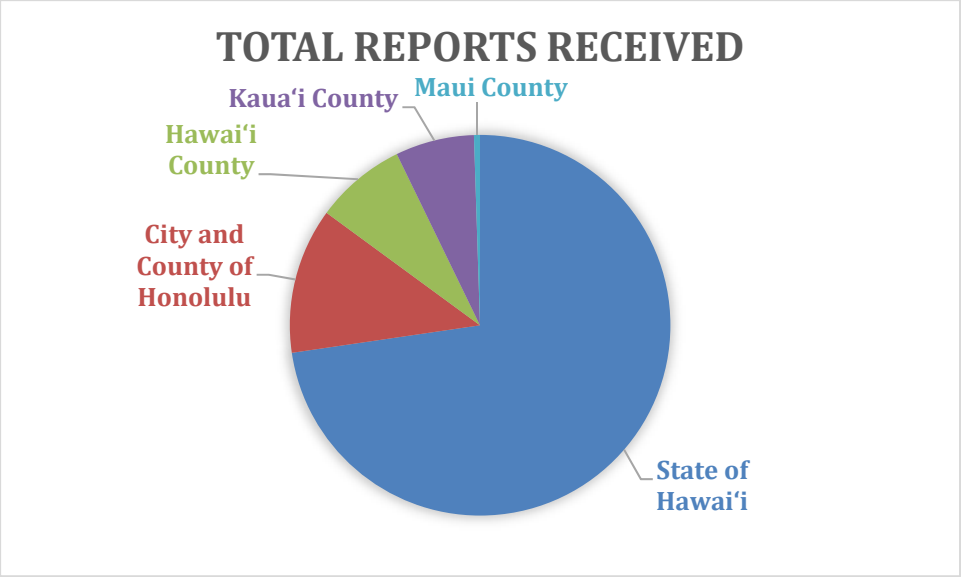
## LEGISLATION

### Relating to Found Electronic Devices

Under new legislation in the last session, new authority was given to state and county agencies allowing them to remove PI from lost electronic devices before returning to the finder.

## FINDINGS

The rate of reporting continues to improve since the enactment of section 487N-7, HRS, which established the reporting requirement. This year, the IPSC received reports from a total of 194 agencies (compared to 155 in 2017).




*Total Reports Received: 73% from the State of Hawai'i; 12% from the City and County of Honolulu; 8% from Hawai'i County; 7% from Kaua'i County; and 1% from Maui County.*

### General Statistics

| | |
|---|---|
| Total Reports Received in 2018 | 194 |
| Reports Submitted by State Agencies | 140 |
| Reports Submitted by City and County of Honolulu Agencies | 21 |
| Reports Submitted by Hawai'i County Agencies | 15 |
| Reports Submitted by Maui County Agencies | 1 |
| Reports Submitted by Kaua'i County Agencies | 13 |
| Total Agencies Reporting No Changes from Previous Year | 11 |
| Agencies Reporting Systems Collecting PI of General Public | 95 |
| Agencies Reporting Systems Collecting PI of Government Employees | 115 |

**MEMORANDUM**

[DATE]

**TO:** State & County Agencies

**FROM:** Information Privacy and Security Council, State of Hawai‘i

**SUBJECT:** Removing PII From Found Devices
HRS §52D-14 – Duty & Right of Finders Amendment for Electronic Media

---

A law that was made effective in July 2018, sections 52D-14 and 261-17, Hawaii Revised Statutes (HRS), now requires state and county agencies to remove PII from “found” electronic devices before returning them to the finder or destroy the devices, if not possible.

The law adds a new language to sections 52D-14 and 261-17, HRS, which is summarized here:

(c) Before an electronic device that allows for storage of personal information is returned to the finder or disposed of by public auction or other means, the device shall be sanitized in accordance with guidance provided by the information privacy and security council to ensure removal of personal information. If removal of personal information is not possible or cannot be verified without unreasonable expense, the device shall be destroyed in a manner sufficient to eliminate the information, and then disposed of or recycled. The chief of police shall make reasonable efforts to notify the finder that the device was destroyed and disposed of or recycled because personal information could not be removed.

For executive branch departments, the Office of Enterprise Technology Services (ETS) has provided guidelines at https://ets.hawaii.gov/policies to safely dispose of data and devices, and when appropriate, to comply with sections 52D-14 and 261-17, HRS, sanitizing requirements. Other jurisdictions may follow these guidelines or develop their own.

Should you have questions or request assistance, please contact Acting IPSC Chair Vincent Hoang, Chief Information Security Officer, ETS, at vincent.hoang@hawaii.gov or 587-1212.

This new law was a legislative initiative by the Information Privacy and Security Council.

# Device Sanitization Guideline

From the Office of Enterprise Technology Services (ETS)

**Policy Document:** 545.02.01
**Version:** 1.1
**Effective Date:** XX/XX/2018
**Data Classification:** Public

## STATEMENT

Data sanitization is the process of irreversibly removing or destroying data stored on a memory device (hard drives, flash memory / SSDs, mobile devices, CDs, and DVDs, etc.) or in hard copy form. It is important to use the proper technique to ensure that all data is purged. Guidance below is derived from NIST SP 800-88 Rev. 1 ("Guidelines for Media Sanitization").

## SCOPE

Protecting the confidentiality of information should be a concern for everyone, from federal agencies and businesses to home users. Recognizing that interconnections and information exchange are critical in the delivery of government services, this guide can be used to assist in deciding what processes to use for sanitization or disposal.

## CONTROLS

Per HRS §§ 52D-14 and 261-17.7, any unclaimed property may be turned over to finders if it is unclaimed after forty-five days. However, given that cell phones, computers, and other electronic devices may contain personal information such as:

(1) Social Security Number;
(2) Driver's license number or Hawaii identification card number; or
(3) Account number, credit or debit card number, access code, or password(s);

after the forty-five days have passed and before the electronic devices can be returned to the finder or disposed of, the device must be sanitized to ensure removal of any personal information. If the removal of personal information is not possible or cannot be verified, the device shall be destroyed to ensure the information is not accessible and then properly disposed of or recycled.

## Table 1. Device Sanitization Controls

| Control Number | Control Name | Control Detail |
|---|---|---|
| 1 | CLEAR | Manually delete all information, then perform a full manufacturer's reset to reset the mobile device to factory state. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results. |
| **2** | PURGE | See DESTROY.<br><br>Most Electronic devices only offer capabilities to Clear (and not Purge) the data contents. Devices may offer Purge capabilities, but these capabilities are specific to the hardware and software of the device and should be applied with caution. The device manufacturer should be referred to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. |
| **3** | DESTROY | - Shred<br>- Disintegrate<br>- Pulverize<br>- Incinerate by burning the device in a licensed/approved incinerator |
| **4** | **NOTES** | - Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as call history, browser history, files, photos, etc.) to verify that no personal information has been retained on the device.<br>- For both Clear and (if applicable) Purge, refer to the manufacturer for proper sanitization procedure.<br>- If device is locked via "Find my iPhone" for example and 45 days has passed, the device should be "Destroyed" as it will not be possible to verify that data has been purged. |

** Refer to NIST 800-88r1- Table 5-1 & Table A-3
for additional device sanitization procedures including specific devices such as iPhones & Android.

## RELATED RESOURCES

800-88 – NIST Guidelines for Media Sanitization – Revision
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf

IRS Media Sanitization Guidelines
https://www.irs.gov/privacy-disclosure/media-sanitization-guidelines

## GUIDELINE HISTORY

| Version | Description | Date |
|---|---|---|
| 1.1 | Initial Release: (ETS) > GD | 11/1/2018 |

## CONTACT INFORMATION

For questions about this guideline, please contact ETS at ets.policies@hawaii.gov

## APPROVING AUTHORITIES

**Vincent Hoang** **Date:**
**Chief Information Security Officer**
**State of Hawai'i**

**Todd Nacapuy** **Date:**
**Chief Information Officer**
**State of Hawai'i**