Information Privacy and Security Council
Meeting Agenda

February 20, 2019
1:00 p.m.

<u>Videoconference Centers (VCC)</u>
Kalanimoku Bldg., 1151 Punchbowl St., Basement B-10, 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. Review and Approval of the December 10, 2018 and December 19, 2018 Meeting Minutes

III. Public Testimony on Agenda Items

a. *Interested persons may submit testimony on any agenda item 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.*
b. *Each individual or representative of an organization is allotted three minutes for testimony.*

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

V. Relating to Geographic Information System Data and Title Records; Discussion and Appropriate Action

VI. Good of the Order
a. Announcements
b. Next meeting: April 17, 2019, 1:00 p.m.

VII. 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 Privacy and Security Council (IPSC)
Meeting Minutes - DRAFT
December 10, 2018

Videoconference Centers (VCC)

Kalanimoku Bldg., 1151 Punchbowl St., Rm. 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

Members Present

Vince Hoang, Acting Chair	Office of Enterprise Technology Services (ETS)
Lisa Tong (Designee)	Department of Commerce and Consumer Affairs
Jonathan Chee	Department of Education
Wilfredo Tungol (Designee)	Department of Health
David Keane	Department of Human Resources Development
Lim Yong	Department of Human Services
Carol Taniguchi	Legislature
Jodi Ito (Designee)	University of Hawaii
Jules Ung	County of Hawaii
Nyree Norman	County of Kauai

Members Absent

Kevin Thornton	Judiciary
Mark Wong	City & County of Honolulu
Karen Sherman	County of Maui

Other Attendees

William Monahan, CISO	Department of Human Services
Greg Dalin	ETS
Susan Bannister	ETS

I. Call to Order

Acting Chair Hoang called the meeting to order at 1:07 p.m. at which time quorum was established.

II. Review and Approval of September 19, 2018 Meeting Minutes

Member Keane made a motion to approve the September 19, 2018 meeting minutes, which was seconded by Member Yong. A vote was taken and the motion passed unanimously.

III. Public Testimony on Agenda Items

None.

IV. Annual Summary Report to the Legislature (Draft)

Hoang summarized the draft report noting that there were logistical issues with completing the online Sharepoint questionnaire. In the future, ETS will standardize the pdf, which seems easier to maintain. Agencies which don't have major changes to their report, would simply update the date of their submittal. The total number of reports received increased from previous years.

Hoang stated that there were discussions in the past on how to reduce the amount of personal information collected within each of the jurisdictions. As the amount of personal information collected increases, so do the risks. He asked if this could be a priority item for the next calendar year, i.e., to develop a joint effort of identifying where those records are and make strong efforts to reduce the overall collection of personal information.

Discussion ensued. Member Designee Ito reported that the University of Hawaii has put in its best practices not to retain sensitive personal information wherever possible. She noted that it is very difficult to do due to various units requiring it for business operations. Part of the best practices strongly encourages staff to delete any unneeded repository of sensitive information. Member Keane asked if there is any thought on aligning that effort with the data governance to a larger data governance. Hoang stated that ETS is making an effort in asking those types of questions during the Governance cycle. As ETS makes stronger progress with the ETS statewide policies, there will be a control statement explicitly having a goal of reducing that data. Following through on it will be the challenge. Member Designee Ito stated that as part of the UH data governance program, they have data classification categories and different technical requirements around those category lines so sensitive information must be encrypted.

Mr. Monahan suggested that the various jurisdictions communicate when they make individual progress rather than have an IPSC-led initiative with the risk of it failing. The IPSC can strongly recommend that the agencies move toward those models with the goal of reducing risk.

Member Yong stated that they have implemented and tested a new disaster recovery system and wondered if it should be reflected in the report. Hoang deferred the finalization of the report until the next meeting.

Member Designee Tungol entered the meeting at 1:15 p.m.

V. Enterprise Technology Services Statewide Security Policies and Standards

Hoang reported that the policies are in draft. The intent is to have some lean policy statements overarching information security with a control-based approach within the standards to be very prescriptive in how to do the implementation. He intends to share it with a broader audience within ETS in the future. Initial concerns are having controls that are unenforceable so want to define the minimum baselines for all of the departments. They are currently looking at three classifications so the control level would be dependent on the classification level.

VI. Good of the Order

a. Announcements

Hoang reported that the memo regarding data sanitization and the draft of the data sanitization guidelines will be discussed at the next meeting as they were not listed on the agenda. These topics will be on the next IPSC meeting agenda with the Annual Summary Report to finalize and approve.

b. Next meeting: December 19, 2018, 1:00 p.m.

VII. Adjournment

At 1:25 p.m., Member Yong made a motion to adjourn, which was seconded by Member Designee Tong. A vote was taken and the motion passed unanimously.

Recorded by: ______________________________
Susan Bannister
Office of Enterprise Technology Services

Information Privacy and Security Council (IPSC)
Meeting Minutes - DRAFT
December 19, 2018

Videoconference Centers (VCC)
Kalanimoku Bldg., 1151 Punchbowl St., Rm. 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

Members Present

Vince Hoang, Acting Chair	Office of Enterprise Technology Services (ETS)
Lisa Tong (Designee)	Department of Commerce and Consumer Affairs
Jonathan Chee	Department of Education
Wilfredo Tungol (Designee)	Department of Health
David Keane	Department of Human Resources Development
Lim Yong	Department of Human Services
Jodi Ito (Designee)	University of Hawaii
Jules Ung	County of Hawaii
Nyree Norman	County of Kauai

Members Absent

Kevin Thornton	Judiciary
Carol Taniguchi	Legislature
Mark Wong	City & County of Honolulu
Karen Sherman	County of Maui

Other Attendees

Kandis McIntosh	Department of Health
William Monahan, CISO	Department of Human Services
Valri Kunimoto	Department of the Attorney General
Susan Bannister	ETS

I. Call to Order

Acting Chair Hoang called the meeting to order at 1:04 p.m. at which time quorum was established.

II. Public Testimony on Agenda Items

None.

III. Annual Summary Report to the Legislature

There were no further discussions. Hoang reported that the draft report will be submitted as presented pending approval from the incoming Chief Information Officer (CIO).

IV. Relating to Found Electronic Devices Legislation, Memo and Guideline

Hoang reviewed the draft memorandum and Device Sanitization Guideline that will be sent to State and County Agencies pending approval from the incoming CIO. There were no further discussions.

V. Good of the Order

a. Announcements

Hoang announced that January 28 is International Data Privacy Day. ETS will have something on its website and will share it with other departments before then. The committee will not meet in January since it coincides with the 2019 Hawaii State Legislature opening day.

b. Next meeting: February 20, 2019, 1:00 p.m.

VII. Adjournment

At 1:10 p.m., Member Yong made a motion to adjourn, which was seconded by Member Chee. A vote was taken and the motion passed unanimously.

Recorded by: ______________________________
Susan Bannister
Office of Enterprise Technology Services

DAVID Y. IGE
GOVERNOR

DOUGLAS MURDOCK
CHIEF INFORMATION
OFFICER

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

P.O. BOX 119, HONOLULU, HI 96810-0119
Ph: (808) 586-6000 | Fax: (808) 586-1922
ETS.HAWAII.GOV

ETS 643

February 14, 2019

DRAFT

TO: Department Heads

FROM: Douglas Murdock, Chief Information Officer

SUBJECT: Removing PII From Found Devices As Required In Sections 52D-14 and 261-17, HRS

New language in Hawaii Revised Statutes (HRS), Sections 52D-14 and 261-17, effective July 1, 2018, requires state and county agencies to remove PII from "found" electronic devices before returning them to the finder or to destroy the devices if PII removal is not possible. The Information Privacy and Security Council initiated this statute change, as requested by State and County agencies. The new language in Sections 52D-14 and 261-17 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.

(d) 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 by the director or the director's agent 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 director or the director's agent 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) provides Device Sanitizing 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. Other jurisdictions may follow these guidelines or develop their own.

Should you have questions or need assistance, please contact Information Privacy and Security Council Chair Vincent Hoang, Chief Information Security Officer, ETS, at vincent.hoang@hawaii.gov or (808) 587-1212.

c: IT Coordinators

Device Sanitization Guideline

From the Office of Enterprise Technology Services (ETS)

Policy Document: 545.02.01
Version: 1.0
Effective Date: XX/XX/2019
Data Classification: Public

STATEMENT

Data sanitization in this section is the process of irreversibly removing or destroying data stored on a memory device (hard drive, flash memory / SSD, mobile device, CD, DVD, etc.). It is important to use the proper technique to ensure that all data is deleted and cannot be recovered. Guidance below is derived from NIST SP 800-88 Rev. 1 ("Guidelines for Media Sanitization").

SCOPE

Protecting the confidentiality of information should be everyone's concern, from state agencies and businesses to home users. Recognizing that interconnections and information exchanges are critical in delivering government services, use this guide to select the data sanitization method or disposal process.

CONTROLS

Cell phones, computers, and other electronic storage 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).

Devices containing information must be properly disposed of by erasing data from storage media so that data recovery is impossible:

- Electronic data must be adequately sanitized when repurposing storage media and equipment
- Storage media must be properly disposed of when end of life is reached

- Documentation is completed and retained in accordance with record retention requirements

Follow instructions in this section to properly clear, purge, and destroy such device. If the removal of personal information is not possible or removal cannot be verified, the device shall be destroyed to ensure the information is not accessible.

Table 1. Device Sanitization Methods

Method Number	Method Name	Control Detail
1	CLEAR	Manually delete all information, then perform a full manufacturer's reset to restore the mobile device to factory state.
2	PURGE	See DESTROY. 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 - Disintegrate - Pulverize - 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. - For both Clear and (if applicable) Purge, refer to the manufacturer for proper sanitization procedure.

** 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
1.0	Initial Release: (ETS) > GD	02/14/2019

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

Doug Murdock **Date:**
Chief Information Officer
State of Hawai‘i