Department of Hawaii

STANDARD OPERATING PROCEDURES (SOP)

FOR

ADMINISTRATION: PRIVACY

DEPARTMENT OF HAWAII
VETERANS OF FOREIGN WARS
OF THE UNITED STATES

Approved August 14, 2020

STANDARD OPERATING PROCEDURES (SOP)
FOR
DEPARTMENT OF HAWAII
VETERANS OF FOREIGN WARS OF THE UNITED STATES

ADMINISTRATIVE

PURPOSE

The State of Hawaii Veterans of Foreign Wars, Administration Manual contains guidelines for maintaining Department Personnel Privacy Information.

SECTION 1
Control and Administration

This Section of the SOP is maintained and administered by the State Adjutant. All employees, interns and volunteers with access to PII shall read and sign the Privacy Policy Acknowledgement.

SOP REVIEW

The SOP will be reviewed to ensure the following:

1. Contact information is accurate and up to date.
2. The SOP will be updated to ensure compliance with the National Bylaws, and applicable directives and regulations.
3. The Adjutant will report on all changes made to the SOP.

After an initial approval by the State Commander, This SOP will be reviewed annually. The Senior Vice Commander will review the SOP before the Department Convention. The State Adjutant will present the SOP at the first COA after the Department Convention for approval. After approval the SOP will become immediately effective. During the year any changes to the SOP will given to the Department Adjutant for distribution to voted on at the next COA.

SECTION 2
Personal Identifiable Information Collection Statement

Personally Identifiable Information We Collect

We collect Personally Identifiable Information when you provide it to us, such as when you join our organization, register for an event, request services, request information or otherwise communicate with us. Many of the services that we offer, including but not limited to events require your contact details as a condition of use, when you interact with us you are no longer anonymous. We may also receive information about you from other sources and add it to the information you have provided to us.
In General, we may collect and store any personally identifiable information you provide to us. Personally identifiable information is data that identifies you, or that can be combined with other information to identify you or to contact you, and includes (but is not limited to) your name, address, email address and telephone number.

SECTION 3
Summary of Applicable Hawaii Statues

It is a violation of Hawaii Revised Statutes 487N to transmit Personal Identifiable Information (PII) that is not encrypted and password protected.

All emails that contain sensitive information should be sent as a password protected, encrypted attachment, using applications such as WinZip or 7Zip (freeware), and provide the password separately (e.g., by phone, another email, or in person).
Hawaii Revised Statutes 487N defines PII as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
(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 that would permit access to an individual's financial account.

SECTION 4
PERSONAL IDENTIFIABLE INFORMATION (PII)

The Department of Hawaii, VFW collects, stores, and shares personal information every day.

It's crucial that you know whether any of the personal information you hold should be treated as "sensitive." If you have questions on what information you have is PII, Contact the State Adjutant.

Personally identifiable information (PII) is information that, when used alone or with other relevant data, can identify an individual. PII is defined as information that:

(i) That directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.

(ii) That indirectly identifies specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicators, and other descriptors).

(iii) Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information.

(iv) This information can be maintained in either paper, electronic or other media.

Department of Hawaii Veterans of Foreign Wars (VFW) personnel are reminded that safeguarding sensitive information is a critical responsibility that must be taken seriously at all times. Department of Hawaii, VFW policy specifies the following security policies for the protection of PII and other sensitive data:

1. It is the responsibility of employees, interns, volunteers and contractors to safeguard and protect data to which they have access. They shall respect the confidentiality of such information, and refrain from any conduct that would indicate a careless or negligent attitude toward such information.
2. The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. Because VFW employees and contractors may have access to personal identifiable information concerning individuals and other sensitive data, we have a special responsibility to protect that information from loss and misuse.

Sensitive vs. Non-Sensitive PII

Personally identifiable information (PII) can be sensitive or non-sensitive. Some personal information is objective. Some personal information is more sensitive than other types.

Sensitive personal information includes:

- Name, such as full name, maiden name, mother's maiden name, or alias
  Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number. Partial identifiers, such as the first few digits or the last few digits of SSNs, are also often considered PII because they are still nearly unique identifiers and are linked or linkable to a specific individual.
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well- defined group of people and Social media Handles.
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or thenumber and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, zip code, employment information, medical information, education information, financial information.

Subjective Data:

It's also possible to generate **subjective personal information** about someone. For example:

- An employee record or complaint file
- A set of notes from a meeting
- Emails between you and a customer or employee about another person

Non-Sensitive PII

Non-sensitive or indirect PII is easily accessible from public sources like phonebooks, the Internet, and corporate directories. Examples of non-sensitive or indirect PII include:

- Zip code
- Race
- Gender
- Date of birth
- Place of birth
- Religion

The above list contains quasi-identifiers and examples of non-sensitive information that can be released to the public. This type of information cannot be used alone to determine an individual's identity.

Non-sensitive information is linkable. This means that non-sensitive data, when used with other personal linkable information, can reveal the identity of an individual and should be store appropriately.

Safeguarding PII

The Department should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.

Data should be deleted if no longer needed for its stated purpose, and personal information should not be shared with sources that cannot guarantee its protection.

You must store PII securely. You must also securely store any key or additional information that could be used to link the data to an individual.

The likelihood of harm caused by a breach involving PII is greatly reduced if we minimize the amount of PII we use, collect, and store. Annual PII purging should be part of the Records Retention Program.

Breaches involving PII are hazardous to both individuals and organizations. In the event of a PII data breach immediately contact the State Commander and Sate Adjutant for further guidance.

SECTION 5
Fair Information Practices

- **Collection Limitation:** We will limit to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality:** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose Specification:** The purposes for which personal data are collected should be specified at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Use Limitation:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.

- **Security Safeguards:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- **Individual Participation:** An individual should have the right: (a) to obtain from the State Adjutant, confirmation of whether or not the VFW Department of Hawaii has data relating to them; (b) to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

- **Accountability:** State Adjutant shall be accountable for complying with measures which give effect to the principles stated above.

SECTION 7
LINKS

Links:

VFW National Links:

VFW National

Visit our VFW Youth Scholarships

VFW Department of Hawaii Links:

VFW Department of Hawai Website

Department of Hawaii on Facebook

APPENDIX

A. Privacy Policy Acknowledgement Form

Privacy Policy Acknowledgment

By signing below, I acknowledge that I have read and understand the Department of Hawaii privacy policy.

Date: _____

Signed: _____

Printed Name: _____