



STATE OF HAWAII
DEPARTMENT OF HUMAN RESOURCES
DEVELOPMENT
POLICIES AND PROCEDURES

POLICY NO. 103.001 DO/ISO	NO. of PAGES 13 1 Attachment
EFF. DATE 5/25/04	REV. NO./Date Rev. No. 2 02/15/12

TITLE: ACCEPTABLE USAGE OF INFORMATION
TECHNOLOGY RESOURCES

APPROVED

Barbara A. Kheg
Barbara A. Kheg, Interim Director

I. POLICY

The use of the State's Information Technology (IT) resources by its employees is a privilege and shall be used for furthering State business and in service to the citizens of Hawaii. Usage shall be limited to legal purposes only. Usage shall not be for illegal, dishonest, disruptive, threatening, damaging to the reputation of the State, inconsistent with the mission of the State, or likely to subject the State to legal liability.

The primary subject matter expert for IT and lead agency for IT systems in State government is the Department of Accounting and General Services ("DAGS"). DAGS participated in developing this policy and concurs with it, including its intent and the expectations placed on users of State IT resources.

II. RATIONALE

The State's IT resources are government property. As with other government property, employees are expected to limit usage of such resources to work-related activities and exercise care and caution when using this technology.

III. DEFINITIONS

"IT resources" means all hardware, software, documentation, programs, information, data, and other devices that are owned or provided by the State. These resources include those that enable remote and local communication such as hubs, switches, routers, and concentrators or access between various platforms and environments such as the mainframe, minicomputers, servers, Local Area Networks ("LANs"), Wide Area Networks ("WANs"), and personal computers.

"Users" mean all State employees in the executive branch who are authorized to use or access the State's IT resources.

"Personal Data" means 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:

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

- (1) Social Security Number;
- (2) Driver's license number or Hawaii identification card number;
- (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account;
- (4) Date of birth;
- (5) Home/cell/mobile phone and personal mail address.

Personal data also includes information described in Chapter 92F-14 of the Hawai'i Revised Statutes. Unencrypted e-mail is not secured transmission.

IV. SCOPE

This policy applies to all employees in the executive branch who are authorized to use or access the State's IT resources, excluding employees of the University of Hawai'i.

Departments that permit volunteers, contractors, vendors, and members of the general public to access the department's IT resources shall be responsible for supervising and monitoring their usage and conduct.

V. GENERAL PROVISIONS

A. PERMISSION AND ACCEPTANCE

The use of any of the State's IT resources implies that the User accepts and agrees to all the terms and conditions as contained in this policy.

B. STATE AS OWNER, CUSTODIAN AND LICENSEE

The State, and not the employee, is the sole owner, custodian, and in cases of software, the licensed user of all IT resources.

C. NO EXPECTATION OF PRIVACY

Users are on notice that there is no proprietary interest and no reasonable expectation of privacy while using any of the IT resources that are provided by the State. The State considers all information and data processed, transmitted, received, and stored on the State's IT resources, including but not limited to, processed documents,

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

electronic and voice mail, and Internet communications as owned by the State. The State may obtain access to any of its resources at any time. The State may disclose any of its IT resources to law enforcement or other third parties without prior consent of the Users.

D. MONITORING AND ENFORCEMENT

The State is the owner or custodian of data and information that is stored on, processed by, or transmitted through the State's IT resources. The State may at any time, and without prior notice, examine data and information such as electronic mail, individual file directories, and other information for purposes such as, but not limited to, ensuring compliance with applicable rules, regulations, policies and procedures, monitoring the performance of the IT resources, and conducting investigations.

The State has the right to monitor, review, audit, and/or disclose any and all of the aspects of the computing and networking resources including but not limited to, monitoring access by Users to the Internet sites that are visited, viewing the contents of electronic mail, documents, files, blog entries, chat groups, or news groups, and inspecting materials that are downloaded or uploaded by Users.

E. REVOCATION OF ACCESS TO IT RESOURCES

The State reserves the right, without advance notice to Users, to revoke access to IT resources, to override Users' passwords without notice, or to require Users to disclose passwords and/or codes to facilitate access to information that is processed and stored in the department's IT resources.

F. POLICY VIOLATION

Violation of this policy by Users may result in immediate revocation or curtailment of computer usage, disciplinary action that may include discharge from employment, and/or civil and criminal liability.

G. AMENDMENTS AND REVISIONS OF THIS POLICY

The State reserves the right to amend or revise this policy from time to time, as the need arises.

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

VI. RESPONSIBILITIES

A. DEPARTMENT OR AGENCY HEADS

1. Development of Acceptable Use Policies

Department or agency heads may choose to develop and enforce their own IT acceptable use policies to further define the use of IT resources within their own departments or agencies. A sample *Acceptable Usage of Information Technology Resources Acknowledgment Form* is set forth as Attachment A.

Should a conflict exist, this *Acceptable Usage of Information Technology Resources* policy shall take precedence over all policies and/or procedures that are developed by the departments or agencies.

2. Authorization and Supervision

Department or agency heads or their designees shall be responsible for:

- a. Authorizing the use of IT resources for specific employees;
- b. Disseminating this policy and any amendments hereto;
- c. Ensuring that Users of IT resources are familiar with the provisions of this policy and any amendments hereto, including developing procedures to ensure that all affected employees are aware of this policy and any amendments hereto;
- d. Supervising the use of IT resources, including taking reasonable precautions to safeguard the resources under their jurisdiction against unauthorized access, use, disclosure, modification, duplication or destruction;
- e. Ensuring that current and new Users are informed of appropriate uses of the State's IT resources;
- f. Enforcing this policy and any amendments hereto; and
- g. Taking appropriate corrective action for violations of this policy and any amendments hereto.

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

3. Periodic Review

Department and agency heads should conduct periodic reviews of IT policy documents with all employees to ensure that employees are kept up to date with regards to new and additional policy requirements and to restate existing policy requirements. These periodic reviews shall remind users of their responsibility in the proper use of the department's information technology resources and their obligation to protect confidential resources, information, and data. Users will be required to sign a new acknowledgment document once the periodic review has been completed.

B. USERS' RESPONSIBILITIES

1. Familiarity with Policies

All Users shall become familiar with this and other supporting and applicable IT resource policies. Questions related to the applicability of this policy may be directed to the User's departmental personnel office. Questions related to the technical aspects of the IT resources may be directed to the User's departmental IT coordinator and/or departmental designated office.

2. Duty Not to Waste IT Resources

It shall be the Users' responsibility to:

- a. Not deliberately perform acts that waste IT resources or unfairly monopolize resources to the exclusion of others. Such acts include, but are not limited to, printing multiple copies of documents, using the e-mail system for sending mass mailings or chain letters, spending excessive amounts of time (unless it is in the course of work), on the Internet, engaging in online chat groups, or otherwise creating unnecessary network traffic;
- b. Not copy and/or download audio, video, and picture files, unless they are work-related; and
- c. Routinely delete outdated or otherwise unnecessary electronic communication and computer files to free up IT resources and help to keep systems running more efficiently and smoothly. Users shall be aware that the deletion of

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

electronic communication and computer files may not fully eliminate the messages and files from the system. Users are directed to review the Department of Accounting and General Services "General Records Schedule" as well as any Department specific policy, which addresses deleting, erasing, discarding, or disposing of electronically stored information.

3. Duty to Act Lawfully, Ethically, Respectfully, and Responsibly

It shall be the Users' responsibility to:

- a. Act lawfully, ethically, respectfully, and responsibly in the use of the State's IT resources;
- b. Maintain the confidentiality of classified materials including personal data;
- c. Transmit or disclose classified and/or confidential information including personal data, through secured electronic communication media only to another party who is authorized to receive or view such information; and
- d. Immediately report an encounter or receipt of unlawful, unethical, or questionable materials to a supervisor or the department or agency head's designee.

4. Duty to Protect the State's IT Resources

It shall be the Users' responsibility to:

- a. Take all reasonable precautions to protect the State's IT resources from unauthorized access, use, disclosure, modification, duplication, and/or destruction;
- b. Employ access controls, and other security measures provided by the department or agency and take prudent and reasonable steps to limit unauthorized access to IT resources;
- c. Assist and cooperate in the protection of the IT resources and follow departmental or agency procedures in matters such as, but not limited to, logging off and powering down while away from the computer and at the end of each workday, scanning files obtained from external sources for

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

viruses or signs of other malicious codes prior to accessing the information, and making backup copies of files and data on the hard drives of their respective personal computers; and

- d. Not disclose passwords to any other individual as Users shall be held responsible for all computer transactions that are made with their user IDs and passwords. Passwords shall not be of the type that can be easily surmised, shall not be recorded where they may be easily obtained, and shall be changed immediately upon suspicion that an unauthorized person is aware of the User's password.

VII. PERSONAL USAGE

- A. Employees, in general, are permitted incidental and minimal personal usage of IT resources if such privilege does not adversely affect the program's operations or does not cause harm or embarrassment to the State.
- B. Personal use of IT resources by an employee shall not interfere with his/her job duties or the operations of the State.
- C. Good judgment shall be exercised in using the State's IT resources.
- D. An employee is not authorized personal use of IT resources that result in expenses or charges to the State and he/she shall not engage in the prohibited activities as described in Part VIII, *Prohibited Activities*, below. Employees shall be responsible for the payment of any charges and any additional cost that is incurred as a result of their personal use.
- E. Users who engage in personal use of the State's IT resources shall make it clear to all concerned that their activity or communication is not being sanctioned or used for official State business.

VIII. PROHIBITED ACTIVITIES

The State explicitly prohibits all activities that are in violation of any federal, State or other applicable laws, rules, regulations, and established policies and procedures. Such activities include, but are not limited to:

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

A. Unauthorized Access to Files and Directories

Users are strictly prohibited from:

1. Circumventing the security controls of the State's IT resources, including but not limited to, cracking other Users' passwords, decoding encrypted files, or using software application programs to secretly penetrate computer and information systems; and
2. Accessing directories and files of other Users in order to read, browse, modify, copy, or delete any data or information without the explicit approval of the individual User and/or the department or agency head or designee.

B. Unauthorized Use of Copyrighted or Proprietary Materials

Users are strictly prohibited from:

1. Illegally **copying** material that is protected under copyright law or from making such material available to others for copying;
2. Illegally **sending** (uploading) material that is protected under copyright law, including trade secrets, proprietary financial information, or similar materials without the express prior approval from the department or agency head or designee; and
3. Illegally **receiving** (downloading) material that is protected under copyright law, including trade secrets, proprietary financial information, or similar materials without the express prior approval from the department or agency head or designee.

Users who are unaware if the information is copyrighted, proprietary, or otherwise inappropriate for transfer, shall resolve all doubts in favor of not transferring the information and consult with their supervisor or the department or agency head or designee.

C. Use of Hardware and Software, whether or not provided by the State

1. Users are strictly prohibited from installing hardware such as, but not limited to, communication cards, memory boards and modems, and software such as commercial, shareware, and freeware, on any computer system without the express approval of the department or agency head or designee.

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

2. Users are strictly prohibited from using, connecting, removing, performing, distributing or otherwise operating IT devices, systems, or services such as, but not limited to the following without signing the Acceptable Usage of Information Technology Resources Acknowledgment Form (See Attachment A):
 - a. **Thumb/Flash/USB Portable Storage Devices**
Including portable storage devices that attach to the computer via a USB (Universal Serial Bus) connection or any other computer interface device or type
 - b. **Wireless Connectivity**
Including all computing devices utilizing radio frequency, microwave frequency, or infrared frequency communications methods and technologies
 - c. **Portable Computers**
Including Laptop, Sub-notebook, Tablet, or Portable Personal Computing devices or systems
 - d. **Internet**
Via commonly available browsers such as Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Opera
 - e. **Remote Terminal Access**
Either via dial-up, LAN/WAN or wireless based access methods and terminal emulation and session emulation software applications
 - f. **E-mail**
Including the State's Lotus Notes e-mail system, departmental e-mail and Internet e-mail accessed using State equipment
 - g. **Data Transfers and System Interfaces**
Including all data transfers and systems interfaces to and from state computer systems and storage devices
 - h. **Personal Data Assistants (PDA's) and cell phone hybrids**
Including all State owned and State authorized handheld access devices
 - i. **Magnetic Media**

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

Including disk, tape, cartridge, library, or disk/tape libraries or arrays

- j. Compact Disk (CD) and Digital Video Disk (DVD) media
Including all storage media utilizing laser encoding methods and techniques
- k. Hard Copy report output
Including all hardcopy report output, compilations, publications, assembled and unassembled reports, and other confidential paper based information generated by the State's computer systems
- l. Weblogs (aka "BLOGS")
Including all online weblogs (BLOGS), discussion boards, bulletin board systems, forums and FAQ columns
- m. Instant Messaging/Chat
Including Microsoft Instant Messaging and other online chat and messaging services

D. Use for Profit and Solicitation

Users are strictly prohibited from using the State's IT resources for any personal or private financial gain, commercial or profit-making activities, and political, religious, or other solicitations.

E. Unlawful and Unethical Conduct

1. Professional Communications

Users shall be responsible to:

- a. Behave in a professional manner and shall exercise courtesy when using any electronic communication media;
- b. Exercise the same degree of care, judgment, and responsibility in composing and transmitting electronic communications as would be done when composing and sending written communication;
- c. Strictly refrain from the usage of profanity and/vulgarity when using any IT resource; and

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

- d. Assume that an electronic message will be saved and reviewed by someone other than the intended recipients.
2. Discriminatory, Inappropriate and Offensive Communications
- a. Users are strictly prohibited from using the State's IT resources to intentionally access, download from the Internet, display, transmit, or store any information that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, pornographic, violent, intimidating, libelous, defamatory, or is otherwise unlawful, inappropriate, and offensive, including but not limited to, offensive material concerning gambling, sex, race, color, national origin, religion, age, disability, or other characteristics that are protected by law;
 - b. The Users' departmental policies such as the sexual harassment, workplace violence, and equal employment opportunity and affirmative action policies shall apply fully to the use of IT resources. Users are strictly prohibited from any actions that may violate such policies while using the State's IT resources; and
 - c. Users are strictly prohibited from making defamatory comments or taking actions such as forwarding of electronic mail that facilitate the publication or spread of such comments.
 - d. Users are strictly prohibited from sending, distributing or forwarding any and all e-mail via the State's electronic e-mail systems that the reasonable person would consider sexually explicit, profane, or offensive in any way, shape or form.

3. Attacking the System

Users shall not attempt, subvert, engage in, or contribute to any activity that would compromise the security of the State's IT resources. Activities that are expressly prohibited include, but are not limited to:

- a. Deliberately crashing, sabotaging, or damaging any computer system;

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

- b. Using software that is designed to destroy data, collect data, facilitate unauthorized access to information resources, or disrupt computing processes in any way; or
- c. Using invasive software that may cause viruses or other damage or expense.

4. Theft

Users are strictly prohibited from removing any hardware, software, attached peripherals, supplies, and documentation without the express approval of the department or agency head or designee.

Users are strictly prohibited from using diskettes, manuals, or other means as defined in section C.2 of this policy or by any other means to obtain restricted information.

5. Misrepresentation

Users are strictly prohibited from making unauthorized statements or commitments on behalf of the State or posting an unauthorized home page or similar web site.

IX. DISCLAIMER OF LIABILITY FOR INTERNET USE

Users who access the Internet do so at their own risk. The State shall not be responsible for material viewed or downloaded by Users from the Internet.

Users are cautioned that pages might contain offensive, sexually explicit, and inappropriate material.

X. AUTHORITIES AND REFERENCES

AUTHORITIES

Chapter 26, Hawaii Revised Statutes, *Executive and Administrative Departments*

Chapter 84, Hawai'i Revised Statutes, *Standards of Conduct*

Chapter 92F, Hawaii Revised Statutes, *Uniform Information Practices Act*

ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES

POLICY NO. 103.001 (Eff. 5/25/04; as rev. 02/15/12)

Chapter 94, Hawai'i Revised Statutes, *Public Archives; Disposal of Records*

REFERENCES

Comptroller's Memorandum 2002-30, dated July 31, 2002, *E-Mail Retention Schedule to Conserve Resources*

Department of Accounting and General Services, Information and Communication Services Division, *Statewide IT Standards*

Department of Accounting and General Services, Information and Communication Services Division, dated February 2, 1998, *Policy and Guidelines on the Use of the State of Hawai'i Electronic Mail System*

XI. ATTACHMENTS

Attachment A: Acceptable Usage of Information Technology Resources Acknowledgment Form



Policy 26.01
Version Number: 1

Initial Approved Date: December 15, 2006
Last Modification Date: December 15, 2006

TO

All Deputies, Division and Branch Chiefs, Staff Officers, District Health Officers, and Administrators of Attached Agencies

FROM

Director of Health

SUBJECT

Notification of Security Breaches.

PURPOSE

To decrease the risks of identity theft by establishing Department of Health ("DOH") security breach notification and reporting policies and guidelines requiring the notification of an individual(s) whenever the individual's personal information has been compromised by unauthorized disclosure, and to comply with the requirements of Hawaii Revised Statutes ("HRS") Chapter 487N.

DEFINITIONS

Encryption – means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

Personal information – means 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 name or data elements are not encrypted:

- (1) Social security number;
- (2) Driver 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.

Personal information – does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Records – means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

Redacted – means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

Security breach – means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident or unauthorized access to and acquisition of encrypted records or data containing personal information along with confidential process or key constitutes a security breach.

Workforce - Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DOH, is under the direct control of DOH, whether or not they are paid by DOH.

POLICY

It is Department policy that:

- DOH shall ensure that it provides notice to all individual(s) affected by a security breach immediately following discovery or notification of breach.
- Any and all instances of a security breach shall be immediately reported to the appropriate Office/Branch/Division Chief, Deputy Director, HIPAA Office, and the Director. The supervising Deputy Director and Director shall evaluate the incident and determine the appropriate response.
- This policy shall be effective January 1, 2007.

I. Ensure that personal information records are identified, minimized and properly secured.

- A. Inventory records.** Each DOH program shall identify and create an inventory of the records that it maintains or are maintained on its behalf that include personal information. The inventory should include the types of personal information maintained, the location of the record (whether on-site or off) and the employees or any third parties who are authorized to access the records. The inventory does not need to list each record or document, but should describe the types of records maintained and the respective purposes for which the personal information is permitted to be used and/or disclosed.

- B. **Minimize and eliminate.** Each DOH program shall review their data collection policies to determine whether they can minimize or eliminate the collection of personal information. Programs may consider collecting such information in redacted format (e.g., the last four digits of the Social Security numbers). In addition, programs shall consider whether existing records containing personal information are no longer needed. If not, they should be destroyed pursuant to DOH's Destruction of Personal Information Records policy.
- C. **Ensure security of information.** Each DOH program shall have written procedures that ensure the security of any records that contain personal information, whether maintained by the program or by third parties. Such procedures may require particular handling and storage techniques, including confidentiality agreements with third parties, and may limit access to the information to appropriate employees. Procedures should address, among other things, how and where such records are secured, who has access and how access is monitored (refer to the DOH intranet site for recommended security guidelines).

II. **Notification of security breaches.**

- A. DOH collects personal information for specific government purposes. Therefore, DOH shall provide notice that there has been a security breach to individual(s) affected by a security breach following discovery or notification of breach. The disclosure notification shall:
1. Be made without unreasonable delay, with the exception of law enforcement requests pursuant to subsection II.c;
 2. Be consistent with any measures necessary to:
 - a. Determine sufficient contact information;
 - b. Determine the scope of the breach; and
 - c. Restore the reasonable integrity, security and confidentiality of the data system.
- B. **Notification of owner or licensee of personal information affected by a security breach.** DOH maintains or possesses records or data containing personal information of residents of Hawaii. Therefore, DOH shall notify any owner or licensee of personal information involving any security breach that there has been a security breach immediately following the discovery or notification of breach, with the exception of law enforcement requests, pursuant to subsection II.c.
- C. **Law enforcement requests.** DOH shall notify the individual(s) of a security breach, consistent with the legitimate needs of law enforcement as provided as follows:

1. The notice required by this section shall be delayed if a law enforcement agency informs the DOH that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such a request is made in writing, or DOH documents the request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation.
2. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to DOH its determination that notice will no longer impede the investigation or jeopardize national security.

III. Description of the disclosure notice.

- A. The notice shall be clear and conspicuous.
- B. The notice shall include a description of the following:
 1. Incident in general terms;
 2. Type of personal information that was subject to the unauthorized access and acquisition;
 3. General steps taken by DOH to protect the personal information from further unauthorized access;
 4. Telephone number that the individual(s) may call for further information and assistance, if one exists; and
 5. Advice that directs the individual(s) to remain vigilant by reviewing account statements and monitoring free credit reports.

IV. Provision of the notice.

The notice to affected individual(s) may be provided by one of the following methods:

- A. **Written** notice to the last available address DOH has on record;
- B. **Electronic** mail notice, for those individual(s) for whom DOH has a valid electronic mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and

signatures for notices legally required to be in writing set forth in 15 U.S.C. Section 7001;

- C. **Telephonic** notice provided that contact is made directly with the affected individual(s);
- D. **Substitute** notice, if DOH demonstrates that the cost of providing notice would exceed \$100,000 or that the affected class of subject individuals to be notified exceeds two hundred thousand or if DOH does not have sufficient contact information or consent as described above, for only those affected individuals without sufficient contact information or consent, or if the DOH is unable to identify particular affected individuals, for only those unidentifiable affected individuals. Substitute notice shall consist of all the following:
 - 1. Electronic mail notice when DOH has an electronic mail address for the subject persons;
 - 2. Conspicuous posting of the notice on the DOH website; and
 - 3. Notification to major statewide media.

V. **Any waiver of the provisions of sections I-IV of this policy is contrary to public policy and is void and unenforceable.**

VI. **Reporting requirements.**

Any and all instances of a security breach defined in this policy shall be immediately reported as outlined below.

- A. **DOH program workforce member's responsibilities include, but are not limited to:**
 - 1. Notifying his/her respective Office/Branch/Division Chief immediately after he/she becomes aware that a security breach may have occurred;
 - 2. Immediately documenting all relevant facts and circumstances of the security breach or potential security breach and submitting all documentation to his/her Office/Branch/Division Chief.
- B. **Office/Branch/Division Chief's responsibilities include, but are not limited to:**
 - 1. Receiving the initial report from a workforce member(s) or others of a security breach (alleged or confirmed) from his/her program's workforce members or others;

2. Collecting and documenting relevant facts and circumstances of the reported security breach within two (2) working days. In addition, the chief shall complete a "Personal information security incident report form" (refer to the DOH intranet site for the standardized form);
3. Immediately contacting and forwarding all relevant facts and circumstances (including the "Personal information security incident report form") regarding any security breach to his/her supervising Deputy Director and the DOH HIPAA Office;
4. Being knowledgeable and familiar with this policy and the requirements and definitions;
5. Ensuring that his/her program's workforce member(s) are familiar with DOH security breach notification policies and that they understand the definition of "security breach" and "personal information" as defined therein.
6. Submitting a legislative report to the Director for approval and signature within ten (10) days of the security breach.

C. Supervising Deputy Director's responsibilities include, but are not limited to:

1. Receiving the initial report of a security breach (alleged or confirmed) from his/her Office/Branch/Division Chief;
2. Choosing to convene or consult with the following DOH components: Administration, Health Information Systems Office, Communications Office, HIPAA Office, specific DOH programs, and/or others, such as the Attorney General's Office, regarding the initial report of a security breach (alleged or confirmed);
3. Evaluating, assessing and determining if the initial incident/breach is defined as a security breach that is reasonably likely to or will actually result in illegal use of personal information and creates a risk of harm to the individual;
 - a. Evaluating and determining the appropriate response to the reported incident/breach which includes but is not limited to immediately contacting the Director and forwarding the relevant facts and circumstances regarding incident/breach to the Director.

D. Director's responsibilities include, but are not limited to:

1. Immediately informing the Governor's office of any security breaches. Such notice should be given to the Chief of Staff, the policy office and the communications office;
2. Initiating the notification process requirement for affected individual(s) of a security breach as defined in sections II-IV of this policy.
3. Reviewing and revising, if necessary, the written report to the legislature as provided by the Off/Branch/Division Chief. Assuming responsibility for the submittal of the required written report to the legislature regarding a security breach within 20 days of discovery as defined in section VII below.

VII. Legislative reporting requirements.

- A. The DOH shall submit a written report to the legislature within twenty days of discovery of a security breach. The report shall include, but is not limited to the following:
 1. Detailed information relating to the nature of the breach;
 2. The number of individuals affected by the breach;
 3. A copy of the notice of security breach that was issued;
 4. The number of individuals to whom the notice was sent;
 5. Whether the notice was delayed due to law enforcement considerations;
 6. Any procedures that have been implemented to prevent the breach from reoccurring.
- B. In the event that a law enforcement agency informs the DOH that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

- VIII. Corrective Action Plan. The involved DOH program shall submit a Corrective Action Plan addressing any security breach to the Director's Office and the DOH HIPAA Office within thirty days after the discovery of a security breach. The Corrective Action Plan shall include but is not limited to the following:**

- A. The specific area(s) of improvement identified that could prevent a further security breach similar to the one that occurred;
- B. The corresponding new procedure(s) and/or activities that are being developed and implemented to prevent the type of breach from reoccurring;
- C. A timeline indicating when the program intends to have the procedure(s) and/or activities fully implemented;
- D. Specific measures that will describe how progress will be tracked and evaluated by the program.

IX. Education and training.

- A. Office/Branch/Division Chiefs shall ensure that their workforce members are capable of implementing this policy and the program's related procedures.
- B. Office/Branch/Division Chiefs shall be responsible for educating and training their workforce members so they understand the importance of notifying their respective supervising chiefs immediately after they become aware of a security breach.

X. Implementation of policy.

- A. All DOH programs shall develop and implement procedures that comply with this policy by January 1, 2007.
- B. All Deputy Directors shall ensure their respective DOH programs comply with this policy and implement procedures that comply with this policy by January 1, 2007.

XI. Audits and monitoring.

- A. The HIPAA Office may conduct audits and/or monitor security incidents and breaches on an annual or as needed basis.
- B. The HIPAA Office shall evaluate and respond to the acceptability of the DOH program's Corrective Action Plan.

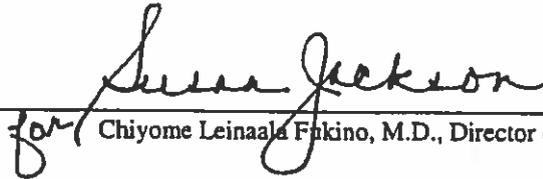
Policy 26.01
Version Number: 1

Initial Approved Date: December 15, 2006
Last Modification Date: December 15, 2006

REFERENCES

1. Hawaii Revised Statutes Chapter 487N.
2. 15 U.S.C. Section 7001
3. September 8, 2006, State of Hawaii, Governor's letter to all Department Heads, Subject: Identity Theft: Steps to be Taken by State Agencies.

APPROVED: _____


for _____

Chiyome Leinaala Fukino, M.D., Director of Health



Policy Number: P27.01
Version Number: 1

Initial Approved Date: December 15, 2006
Last Modification Date: December 15, 2006

TO

All Deputies, Division and Branch Chiefs, Staff Officers, District Health Officers, and Administrators of Attached Agencies

FROM

Director of Health

SUBJECT

Destruction of Personal Information Records

PURPOSE

To decrease the risks of identity theft by establishing policies and guidelines relating to the adequate destruction or proper disposal of the Department of Health ("DOH") records containing personal information and to comply with the requirements of Hawaii Revised Statutes ("HRS") Chapter 487R.

DEFINITIONS

Disposal – means the discarding or abandonment of records containing personal information or the sale, donation, discarding, or transfer of any medium, including computer equipment or computer media, containing records of personal information, or other nonpaper media upon which records of personal information are stored, or other equipment for nonpaper storage of information.

Personal information – means 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 name or 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.

Personal information – does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Records – means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

Workforce - Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DOH, is under the direct control of DOH, whether or not they are paid by DOH.

POLICY

It is Department policy that:

- DOH shall ensure that records containing personal information are properly destroyed before they are discarded, irrespective of whether the records are maintained by the program or by third parties.
- Any and all instances of a material occurrence of unauthorized access to personal information records in connection with or after its disposal shall be immediately reported to the appropriate Office/Branch/Division Chief, Deputy Director, HIPAA Office, and the Director. The supervising Deputy Director and Director shall evaluate the incident and determine the appropriate response.
- This policy shall be effective January 1, 2007.

I. Destruction of personal information records.

- A. DOH collects and maintains records containing personal information of Hawai'i residents. Therefore, it shall take reasonable measures to protect against the unauthorized access to or use of personal information it maintains in connection with or after its disposal.
- B. **Paper records.** Reasonable measures for destroying paper records containing personal information shall include:
 - 1. Implementing and monitoring compliance with policies and procedures that requires the burning, pulverizing, recycling, or shredding of papers containing personal information so that information cannot be practically read or reconstructed.

2. It is DOH's policy that paper records containing personal information shall comply with DAGS' record destruction policy (Refer to: DAGS. Disposal of Government Records, April 12, 2005-revised August 1, 2006).
 - a. Pursuant to DAGS' record destruction policy, proper destruction includes but is not limited to shredding of paper documents using shredders.
 - b. It is DOH's policy that shredders must meet at least DIN 32757 Security Level 3. DIN (Deutsches Institut fur Normung) or the German Institute for Standardization developed security standards for paper shredders.
 - i. **Security Level 3** is designed for shredding confidential paper documents and personal data. DIN 32757 Security Level 3 certified shredders will shred paper to 1/16-inch (strip cut); 1/8-inch x 1 1/8 inch (cross cut).
- C. **Electronic records.** Reasonable measures for destroying electronic records containing personal information shall include:
1. Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practically be read or reconstructed.
 2. It is the Department's policy that electronic records containing personal information shall comply with DAGS' record destruction policy (Refer to: DAGS. Disposal of Government Records, April 12, 2005-revised August 1, 2006.) In addition, programs shall consult with the DOH Health Information Systems Office regarding acceptable standards for properly sanitizing and disposing of electronic records and equipment.
- D. **Contracting with a disposal business and due diligence.** DOH may satisfy its obligation hereunder by exercising due diligence and entering into a written contract with, and thereafter monitoring compliance by, another party engaged in the business of record destruction to destroy personal information in a manner consistent with this section. Due diligence should at minimum include one or more of the following:
1. Reviewing an independent audit of the disposal business's operations for compliance with these policies, with HRS Chapter 487R;

2. Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party, such as the National Association for Information Destruction (NAID) (www.naidonline.org), with a reputation for high standards of review; or
3. Reviewing and evaluating the disposal business' information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the disposal business.

E. Third parties maintaining personal information records on behalf of DOH.

Third parties that maintain records that contain personal information on behalf of DOH programs must follow DOH's policy for destroying records. Programs are responsible for ensuring that any such third parties are contractually bound to follow this policy and the requirements of HRS Chapter 487R.

II. Reporting requirements.

Any and all instances of a material occurrence of unauthorized access to personal information records in connection with or after its disposal shall be immediately reported as outlined below.

A. DOH workforce member's responsibilities include, but are not limited to:

1. Notifying his/her respective Office/Branch/Division Chiefs immediately after he/she becomes aware of any material occurrence of unauthorized access to records containing personal information in connection with or after its disposal.
2. Immediately documenting all relevant facts and circumstances of the material occurrence of unauthorized access to records containing personal information in connection with or after its disposal.

B. Office/Branch/Division Chief's responsibilities include, but are not limited to:

1. Receiving the initial report from workforce member(s) or others of any material occurrence of unauthorized access to personal information records in connection with or after its disposal.

2. Collecting and documenting relevant facts and circumstances of the reported material occurrence of unauthorized access to personal information records in connection with or after its disposal within two (2) business days. In addition, the chief shall complete a "personal information security incident report form" (refer to the DOH intranet site to locate the standardized form);
3. Immediately contacting and forwarding the relevant facts and circumstances (including the "personal information security incident report form") regarding any material occurrence of unauthorized access to personal information records in connection with or after its disposal to his/her supervising Deputy Director and the HIPAA Office;
4. Being knowledgeable and familiar with this policy and the requirements and definitions in HRS Chapter 487R;
5. Ensuring that his/her program's workforce members are familiar with and trained in DOH's disposal and reporting policies and that they understand the definitions of "personal information", "records", and "disposal" as defined therein.
6. Submitting a legislative report to the Director for approval and signature within ten (10) days of the security breach.

C. Supervising Deputy Director's responsibilities include, but are not limited to:

1. Receiving the initial report of any material occurrence of unauthorized access to personal information records in connection with or after its disposal from his/her Office/Branch/Division Chief.
2. Choosing to convene or consult with the following DOH components: Administration, Health Information Systems Office, Communications Office, HIPAA Privacy Office, specific DOH programs, and/or others, such as the Attorney General's Office, regarding the initial report of a material occurrence of unauthorized access to personal information records in connection with or after its disposal.
3. Evaluating, assessing and determining if the initial incident/occurrence is defined as a material occurrence of unauthorized access to personal information records in connection with or after its disposal.

4. Evaluating and determining the appropriate response to the reported incident/occurrence which includes immediately contacting the Director and forwarding the relevant facts and circumstances regarding any material occurrence of unauthorized access to personal information records in connection with or after its disposal to the Director.

D. Director's responsibilities include, but are not limited to:

1. Immediately informing the Governor's Office of any material occurrence of unauthorized access to personal information records in connection with or after its disposal. Such notice should be given to the Chief of Staff, the Policy Office and the Communications Office.
2. Reviewing and revising, if necessary the written report to the legislature by the Office/Branch/Division Chief. Assuming responsibility for the submittal of the required written report to the legislature regarding the unauthorized access within 20 days of discovery in section III below.

III. Legislative reporting requirements.

- A. DOH shall submit a written report to the legislature within twenty (20) days of discovery of a material occurrence of unauthorized access to personal information in connection with or after its disposal. The report shall include, but is not limited to the following:
 1. Detailed information relating to the nature of the incident;
 2. The number of individuals affected by the incident; and
 3. Any procedures that have been implemented to prevent the incident from reoccurring.
- B. In the event that a law enforcement agency informs DOH that the report may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

IV. Corrective Action Plan. The involved DOH program shall submit a Corrective Action Plan addressing any material occurrence of unauthorized access to personal information records in connection with or after its disposal to the Director's office and the DOH HIPAA office within thirty days after the discovery of a material occurrence. The Corrective Action Plan shall include but is not limited to the following:

- A. The specific area(s) of improvement identified that could prevent further material occurrences;
- B. The corresponding new procedure(s) and/or activities that are being developed and implemented to prevent similar incidents from reoccurring;
- C. A timeline indicating when the program intends to have the above procedure(s) and/or activities fully implemented; and
- D. Specific measures that describe how progress will be tracked and evaluated by the program.

V. Education and training.

- A. Office/Branch/Division Chiefs shall ensure that their workforce members are capable of implementing this policy and the program's related procedures.
- B. Office/Branch/Division Chiefs shall be responsible for educating and training their workforce members so they understand the importance of notifying their respective supervisor immediately after they become aware that:
 - 1. Records containing personal information have not been destroyed in accordance with this policy; and
 - 2. There has been unauthorized access to personal information disposed of, by or on behalf of their respective programs.

VI. Implementation of policy.

- A. All DOH programs shall develop and implement records disposal and reporting procedures that comply with this policy by January 1, 2007.
- B. All Deputy Directors shall ensure their respective DOH programs comply with this policy by January 1, 2007.

VII. Audits and monitoring.

- A. The HIPAA Office may conduct audits and/or monitor material occurrences of unauthorized access to personal information records in connection with disposal on an annual or as needed basis.

Policy Number: P27.01
Version Number: 1

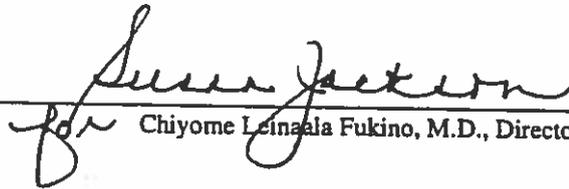
Initial Approved Date: December 15, 2006
Last Modification Date: December 15, 2006

B. The HIPAA Office shall evaluate and respond to the acceptability of the Corrective Action Plan.

REFERENCES

1. Hawaii Revised Statute Chapter 487R
2. September 8, 2006, State of Hawaii, Governor's letter to all Department Heads, Subject: Identity Theft: Steps to be Taken by State Agencies

APPROVED: _____



for Chiyome Leinaala Fukino, M.D., Director of Health



Policy 28.01
Version Number: 1

Initial Approved Date: February 26, 2007
Last Modification Date: February 26, 2007

TO

All Deputies, Division and Branch Chiefs, Staff Officers, District Health Officers, and Administrators of Attached Agencies

FROM

Director of Health

SUBJECT

Social Security Number Protection.

PURPOSE

To decrease the risks of identity theft by establishing Department of Health ("DOH") policies and guidelines relating to the protection of records containing social security numbers from unauthorized access and to comply with Hawaii Revised Statutes ("HRS") Chapter 487J.

DEFINITIONS

Government Agency – means any department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county.

Social security number – means a 9 digit number issued by the Social Security Administration to citizens, permanent residents, and temporary (working) residents under section 205(c)(2) of the Social Security Act, codified as 42 U.S.C. § 405(c)(2)(B)(i).

Encryption – means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

Records – means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

Redacted – means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

Workforce - Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DOH, is under the direct control of DOH, whether or not they are paid by DOH.

POLICY

It is Department policy that:

- DOH shall ensure that reasonable procedural safeguards are implemented to protect against unauthorized access to program records containing social security numbers.
- Any and all instances of unauthorized access to records containing social security numbers shall be immediately reported to the appropriate Office/Branch/Division Chief, Deputy Director, HIPAA Office, and the Director. The supervising Deputy Director and Director shall evaluate the incident and determine the appropriate response.
- This policy shall be effective March 5, 2007.

I. Protection of social security numbers.

A. Identify records containing social security numbers.

1. Each DOH program shall create an inventory of records that contain social security numbers within thirty (30) days of the effective date of this policy.
2. Each DOH program shall conduct an annual update of this inventory.
3. This inventory shall include the numbers, types, locations, and purposes of these records along with a list of those workforce members who are authorized to access the records.

B. Minimize, eliminate, and redact.

1. DOH programs shall determine whether they can minimize or eliminate the collection of social security numbers.
2. Whenever possible, DOH programs shall maintain social security numbers in redacted form (last four digits).
3. DOH programs shall determine which existing records are no longer needed. These records should be properly destroyed to prevent unauthorized access to individuals' social security numbers (refer to DOH Policy 27.01 Destruction of Personal Information Records).

C. Implement safeguards.

1. DOH programs shall implement reasonable safeguards to prevent unauthorized access to social security numbers which are collected and maintained. (Refer to DOH Intranet "Guidelines for Protecting Confidential Information").

D. Activities related to social security numbers that are NOT permitted.

1. Intentionally communicating or otherwise making available to the general public an individual's entire social security number.
2. Intentionally printing or imbedding an individual's entire social security number on any card required for the individual to access services provided by a DOH program.
3. Requiring an individual to transmit the individual's entire social security number over the internet, unless the connection is secure or the social security number is encrypted.
4. Requiring an individual to use the individual's entire social security number to access an internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website.
5. Printing an individual's entire social security number on any materials that are mailed to the individual, unless the materials are employer-to-employee communications, or where specifically requested by the individual.

E. Activities related to social security numbers that are permitted:

1. The inclusion of a social security number in documents that are mailed and:
 - a) Are specifically requested by the individual identified by the social security number;
 - b) Required by state or federal law to be on the document to be mailed;
 - c) Required as part of an application or enrollment process;
 - d) Used to establish, amend, or terminate an account, contract, or policy;
or
 - e) Used to confirm the accuracy of the social security number for the purpose of obtaining a credit report pursuant to 15 U.S.C. § 1681(b).

Note: A social security number that is permitted to be mailed may NOT be:

- Printed, in whole or in part, on a postcard or other mailer not requiring an envelope; nor
 - Visible on the envelope or without the envelope having been opened.
2. The opening of an account or the provision of or payment for a product or service authorized by an individual.
 3. The collection, use, or release of a social security number to:
 - a) Investigate or prevent fraud;
 - b) Conduct background checks;
 - c) Conduct social or scientific research;
 - d) Collect a debt;
 - e) Obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 to 1681x, as amended;
 - f) Undertake a permissible purpose enumerated under the federal Gramm Leach Bliley Act, 15 U.S.C. §§ 6801 to 6809, as amended;
 - g) Locate an individual who is missing or due a benefit, such as a pension, insurance, or unclaimed property benefit; or
 - h) Locate a lost relative.
 4. Acting pursuant to a court order, warrant, subpoena, or when otherwise required by law.
 5. Providing the social security number to a federal, state, or local government entity including a law enforcement agency or court, or their agents or assigns.
 6. The collection, use, or release of a social security number in the course of administering a claim, benefit, or procedure relating to an individual's employment, including:
 - a) An individual's termination from employment;
 - b) Retirement from employment;

- c) Injuries suffered during the course of employment;
 - d) Other related claims, benefits, or procedures.
7. The collection, use, or release of a social security number as required by state or federal law.
 8. The sharing of the social security number by business affiliates.
 9. The use of a social security number for internal verification or administrative purposes.
 10. The use or sharing of a social security number that has been redacted.
 11. Documents or records that are recorded or required to be open to the public pursuant to the constitution or laws of the State or court rule or order.

II. Reporting requirements.

Any and all instances of a material occurrence of unauthorized access to records containing social security numbers shall be immediately reported as outlined below.

A. DOH program workforce member's responsibilities include, but are not limited to:

1. Notifying his/her respective Office/Branch/Division Chief immediately after he/she becomes aware of any material occurrence of unauthorized access to records containing social security numbers may have occurred.
2. Immediately documenting all relevant facts and circumstances of the material occurrence of unauthorized access and submitting all documentation to his/her Office/Branch/Division Chief.

B. Office/Branch/Division Chief's responsibilities include, but are not limited to:

1. Receiving the initial report from a workforce member(s) or others of any material occurrence of unauthorized access to records containing social security numbers (alleged or confirmed) from his/her program's workforce members or others;
2. Collecting and documenting relevant facts and circumstances of the reported material occurrence within two (2) working days. In addition, the Chief shall complete a "Personal Information Security Incident Report Form" (refer to the DOH Intranet site for the standardized form);
3. Immediately contacting and forwarding the relevant facts and circumstances (including the "Personal Information Security Incident Report Form")

regarding any material occurrence to his/her supervising Deputy Director and the DOH HIPAA Office;

4. Being knowledgeable and familiar with this policy and the requirements and definitions in HRS Chapter 487J;
5. Ensuring that his/her program's workforce member(s) are familiar with and trained in DOH's reporting policies;
6. Submitting a legislative report to the Director for approval and signature within ten (10) days of the disclosure.

C. Supervising Deputy Director's responsibilities include, but are not limited to:

1. Receiving the initial report of any material occurrence of unauthorized access to records containing social security numbers from his/her Office/Branch/Division Chief;
2. Choosing to convene or consult with the following DOH components: Administration, Health Information Systems Office, Communications Office, HIPAA Office, specific DOH programs, and/or others, such as the Attorney General's Office, regarding the initial report of a material occurrence of unauthorized access to records containing social security numbers.
3. Evaluating, assessing and determining if the incident is defined as a material occurrence of unauthorized access to records containing social security numbers; and if it is reasonably likely to or will actually result in illegal use of an individual's social security number and creates a risk of harm to the individual (refer to "security breach" DOH Policy P26.01 Notification of Security Breaches);
4. Evaluating and determining the appropriate response to the reported incident/disclosure which includes but is not limited to immediately contacting the Director and forwarding the relevant facts and circumstances regarding any material occurrence of unauthorized access to records containing social security numbers to the Director.

D. Director's responsibilities include, but are not limited to:

1. Immediately informing the Governor's office of a material occurrence of unauthorized access to records containing social security numbers. Such notice should be given to the Chief of Staff, the Policy Office and the Communications Office;
2. Reviewing and revising, if necessary, the written report to the legislature as provided by the Office/Branch/Division Chief.

3. Assuming responsibility for the submittal of the required written report to the legislature regarding the unauthorized access within twenty (20) days of discovery as defined in section III below.

III. Legislative reporting requirements.

- A. The DOH shall submit a written report to the legislature within twenty (20) days of discovery of a material occurrence of unauthorized access to records containing social security numbers. The report shall include, but is not limited to the following:
 1. Detailed information relating to the nature of the incident;
 2. The number of individuals affected by the incident; and
 3. Any procedures that have been implemented to prevent the incident from reoccurring.
- B. In the event that a law enforcement agency informs the DOH that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty (20) days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security.

IV. Corrective Action Plan.

The involved DOH program shall submit a Corrective Action Plan addressing any material occurrence of unauthorized access to records containing social security numbers to the Director's Office and the DOH HIPAA Office within thirty (30) days after the discovery of a material occurrence. The Corrective Action Plan shall include but is not limited to the following:

- A. The specific area(s) of improvement identified that could prevent any future material occurrences;
- B. The corresponding new procedure(s) and/or activities that are being developed and implemented to prevent similar incidents from reoccurring;
- C. A timeline indicating when the program intends to have the procedure(s) and/or activities fully implemented; and
- D. Specific measures that will describe how progress will be tracked and evaluated by the program.

V. Education and training.

- A. Office/Branch/Division Chiefs shall ensure that their workforce members are capable of implementing this policy and the program's related procedures.
- B. Office/Branch/Division Chiefs shall be responsible for educating and training their workforce members so they understand the importance of notifying their respective supervising chiefs immediately after they become aware of an occurrence of unauthorized access to records containing social security numbers.

VI. Implementation of Policy.

- A. All DOH programs shall develop and implement procedures that comply with this policy by April 2, 2007.
- B. All Deputy Directors shall ensure their respective DOH programs comply with this policy and implement procedures that comply with this policy by April 2, 2007.

VII. Audits and monitoring.

- A. The HIPAA Office may conduct audits and/or monitor material occurrences of unauthorized access to records containing social security numbers on an annual or as needed basis.
- B. The HIPAA Office shall evaluate and respond to the acceptability of the Corrective Action Plan.

REFERENCES

1. Hawaii Revised Statutes Chapter 487J.
2. 15 U.S.C. Sec. 1681(b)
3. September 8, 2006, State of Hawaii, Governor's letter to all Department Heads, Subject: Identity Theft: Steps to be Taken by State Agencies.

APPROVED: _____



Chiyohe Leinaala Fukino, M.D., Director of Health

NEIL ABERCROMBIE
GOVERNOR OF HAWAII



LORETTA J. FUDDY, A.C.S.W., M.P.H.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH
P. O. BOX 3378
HONOLULU, HI 96801-3378

In reply, please refer to:
File:

December 10, 2013

CIRCULAR MEMORANDUM NO. 13-51
Human Resources Office
UHE 1213-1
Affirmative Action Office

TO: Director of Health, All Deputies, Division Chiefs, Staff Officers, District Health Officers and Administrators of Attached Agencies

FROM: Rita Hoopii-Hall, Human Resources Officer (HRO), *RHH*
Gerald Ohta, Affirmative Action Officer (AAO), *G.Ohta*

SUBJECT: Discrimination/Harassment-Free Workplace Policy

Purpose:

The Department of Human Resources Development adopted new policy 601.001 that applies to all executive branch agencies (except the University of Hawaii and the Department of Education).

Replaces:

It supersedes DOH Intra-Departmental Directives 83-63R, Nondiscrimination and Affirmative Action in Employment, and 00-1, Unlawful Harassment in Employment.

Background:

This is the first new executive branch-wide discrimination policy since 1987 (re-commitment 1997) and first executive branch-wide harassment-free workplace policy. While there are differences, it is consistent with prior DOH directives.

Orienting staff:

1. Effective immediately, all current and new employees are required to sign and date the "DISCRIMINATION/HARASSMENT-FREE WORKPLACE POLICY ACKNOWLEDGMENT FORM". (Attachment B)
2. Give a copy of the policy to each employee. Each employee needs to sign and date the Acknowledgement Form (Attachment B). Send the original to HRO for file in the employee's official personnel file (OPF). Please give a copy to the employee.

For current employees, please designate your appropriate Personnel Management Specialist (PMS), Public Health Administrative Officer (PHAO), and/or Secretary to coordinate the completion of the Forms by all employees. With the exception of the Hawaii State Hospital that maintains their employees' personnel records, the PMS, PHAO, and/or Secretary must submit all completed

forms to Employee Benefits/Transactions Staff where it will be filed in the Employee's OPF.

All in-processing staffs, please ensure that the form is now included with the other documents to be reviewed and signed by the new employee. Submit completed forms to Employee Benefits/Transactions Staff, where it will be filed in the Employee's OPF.

3. Post the notice on "The State of Hawaii Prohibits Workplace Discrimination, Harassment & Retaliation" on all official bulletin boards (OBB) and places where personnel recruitment occurs. Notify employees of the poster (Attachment H).
4. In most cases, complaints should be made to the supervisor. Please note that the employee may make a complaint to whatever level within DOH or with an appropriate state or federal enforcement agency.
5. As part of conducting interviews during an investigation, three notices of rights and responsibilities are to be used with the complainant, the accused and witnesses as appropriate (Attachments E, F, G). While such notices are useful in any investigation, these are for discrimination-related investigations. If the person does not want to sign, review it orally and note at the bottom that the information was communicated. HRD will provide training on conducting investigations and will provide additional resources. If you have questions, please contact AAO.
6. Training is mandatory for supervisors and non-supervisors. Every employee is expected to attend an HRD training regardless of having attended any prior HRD, DOH, or other training. The U.S. Supreme Court recently limited the definition of supervisor for EEO purposes. For the HRD training, a supervisor is someone who can take tangible employment actions such as discipline, promotion, demotion or firing. If she/he can make such recommendations and such actions are taken, she/he is a supervisor. A working supervisor who directs work but does not have authority to discipline is not a supervisor for purposes of EEO. If in doubt, send the employee to the supervisor training.
7. Each division will report monthly on the status of non-EEOC/HCRC complaints as required by HRD (Complaints log). Report to AAO by the 7th of each month for prior month. AAO will coordinate log for EEOC/HCRC complaints.

DOH HRO will announce and coordinate training. General questions on posting may be directed to the Human Resources Officer at 586-4520. For areas other than posting of notices on the official bulletin board and recruitment areas, consult with the Affirmative Action Office (AAO) at 586-4614.

Attachments:

HRD Policy No. 601.001 Discrimination/Harassment-Free Workplace Policy
Attachments A, B, E, F, G, H
HRD Complaints log

c: Division PHAOs, PMSs and Secretaries
Labor Relations Officer
Training, Safety and Employees Relations Officer



STATE OF HAWAII
DEPARTMENT OF HUMAN RESOURCES
DEVELOPMENT
POLICIES AND PROCEDURES

POLICY NO. 601.001	NO. of PAGES 7 2 Attachments
EFF. DATE October 15, 2013	REV.NO./Date N/A

TITLE: **DISCRIMINATION/HARASSMENT-FREE
WORKPLACE POLICY**

APPROVED:

Barbara A. Krieg, Director

I. POLICY

The State and its appointing authorities are committed to promoting and maintaining a productive work environment free of any form of discrimination, harassment and retaliation. The State and its appointing authorities do not tolerate workplace discrimination, harassment or retaliation. The State and its appointing authorities are required to and will take appropriate action when discrimination, harassment or retaliation is based on a person's protected class.

The State and its appointing authorities will act to curb protected class discrimination or harassment without regard to its severity or pervasiveness and does not require that discrimination or harassment rise to the level of unlawfulness before taking action. Every State employee is responsible for assuring that work in the executive branch is conducted in an atmosphere that respects the dignity of every State employee, and people with whom the State conducts business. State employees are expected to avoid behavior that could reasonably be perceived as discrimination or harassment prohibited under this policy. In addition, State employees are expected to avoid retaliation against an individual who makes a complaint, and/or participates in or provides information for an investigation relating to discrimination and/or harassment. A violation of this policy may result in disciplinary action, up to and including termination, in accordance with applicable State laws, rules, policies, and collective bargaining agreements.

The State and its appointing authorities will also make reasonable accommodations, if needed, to the extent required by law, for employees who are disabled, pregnant (including pregnancy-related disabilities), breastfeeding, victims of sexual or domestic abuse, or for bona fide religious purposes. Any employee who believes he/she needs accommodation for any of these reasons should contact his/her manager, Departmental Personnel Officer (or his/her designee), Departmental EEO or Civil Rights Compliance Officer, or the Executive Branch Equal Employment Opportunity Office (587-1162 or eeo@hawaii.gov).

II. PURPOSE

The purpose of this policy is to assure compliance with all federal and State laws and to prevent discrimination, harassment, and retaliation in the workplace.

DISCRIMINATION/HARASSMENT-FREE WORKPLACE POLICY

POLICY NO. 601.001 (Eff. 10/15/13)

This policy is intended to protect all applicants, employees, and individuals providing services to the State on a non-paid basis (e.g. volunteers or interns) from discriminatory or harassing conduct by employees or non-employees and to prevent employees from engaging in discriminatory or harassing conduct directed to any individual (whether employees or non-employees).

III. DEFINITIONS

"Gender identity or expression" includes a person's actual or perceived gender, as well as a person's gender identity, gender-related self-image, gender-related appearance, or gender-related expression, regardless of whether that gender identity, gender-related self-image, gender-related appearance, or gender-related expression is different from that traditionally associated with the person's sex at birth.

"Genetic information" includes information about an individual's genetic tests and the genetic tests of an individual's family members, as well as information about any disease, disorder, or condition of an individual's family members (i.e. an individual's family medical history). Family medical history is included in the definition of genetic information because it is often used to determine whether someone has an increased risk of getting a disease, disorder, or condition in the future.

"Protected class" means race, color, sex, including gender identity or expression, sexual orientation, condition of pregnancy, act of breastfeeding or expressing milk, religion, national origin, ancestry, age, disability, genetic information, marital or civil union status, arrest and court record (except as permitted by applicable laws), income assignment for child support, national guard absence, uniformed service, veteran status, citizenship (except as permitted by applicable laws), credit history or credit report (unless directly related to a bona fide occupational qualification), domestic or sexual violence victim status if the domestic or sexual violence victim provides notice to the victim's employer of such status or the employer has actual knowledge of such status, or any other classification protected under applicable state or federal laws.

"Protected class discrimination or harassment" means any unwelcome behavior based on a person's protected class which is sufficiently severe or pervasive and has the purpose or effect of either unreasonably interfering with the person's work performance or creating an intimidating, hostile, or offensive work environment.

"Retaliation" means an adverse action taken or threat of adverse action in response to or in an attempt to prevent an individual from opposing a

DISCRIMINATION/HARASSMENT-FREE WORKPLACE POLICY

POLICY NO. 601.001 (Eff. 10/15/13)

discriminatory practice or from participating in an employment discrimination investigation or proceeding.

IV. SCOPE

This policy applies to all employees and applicants in the executive branch under the jurisdiction of the Department of Human Resources Development, whether civil service or exempt employees, full-time or part-time employees, permanent or temporary employees.

V. PROHIBITED CONDUCT

- A. It is a violation of this policy to engage in protected class discrimination or harassment.
1. Protected class characteristics may not be used as a basis for taking employment action or making an employment decision that results in a significant change in benefits, or terms and conditions of employment.
 2. Harassing or offensive conduct directed at individuals based on protected class characteristics is prohibited under this policy, and includes, but is not limited to:
 - a. Unwanted physical contact, sexually suggestive or offensive touching, patting, hugging, or brushing against a person's clothing or body, pinching, or hitting;
 - b. Sexual advances, requests for sexual favors, repeated and unwanted attempts at a romantic relationship, sexually explicit questions, comments about physical attributes;
 - c. Lewd descriptions, sexual jokes, pressure for sexual activity, such as repeated requests for dates, and threats for refusing a sexual advance;
 - d. Displays of demeaning, insulting, objects, pictures, or photographs relating to any protected class;
 - e. Demeaning, insulting, intimidating, written, recorded, or electronically transmitted messages (such as email, text messages, voicemail, and Internet materials) relating to any protected class;
 - f. Derogatory comments, slurs, jokes, profanity, anecdotes, and/or offensive questions based on or directed at any protected class; and/or

DISCRIMINATION/HARASSMENT-FREE WORKPLACE POLICY

POLICY NO. 601.001 (Eff. 10/15/13)

name of the alleged offender(s), including position and department, if known, a summary of the offensive acts, the dates, times and places of the incidents, the names of witnesses to the events, and copies of documents, if any, that support the complaint or report.

B. CONFIDENTIALITY

The State and its appointing authorities will take appropriate steps to protect the confidentiality of discrimination, harassment and retaliation complaints, investigations, and reports, whether substantiated or unsubstantiated. However, complete confidentiality cannot be guaranteed and information regarding complaints, investigations and reports shall be shared with appropriate individuals and agencies on a "need to know" basis, with due consideration for the safety and security of individuals involved in the investigation.

C. RESPONSIBILITIES

1. Department Responsibilities

- a. In alignment with this Discrimination/Harassment-Free Workplace Policy, department or agency heads are responsible for developing and enforcing their own discrimination/harassment free workplace investigation and enforcement processes within their own departments or agencies.
- b. Should a conflict exist, this Discrimination/Harassment-Free Workplace Policy shall take precedence over all policies and/or procedures that are developed by the departments or agencies.
- c. Departments are responsible for distributing this Discrimination/Harassment-Free Workplace Policy to all of its employees using the Discrimination/Harassment-Free Workplace Policy Acknowledgment Form (see Attachment B).
- d. Departments shall forward a copy of any and all complaints of discrimination, harassment or retaliation, whether made internally or to the Equal Employment Opportunity Commission or Hawaii Civil Rights Commission, to designated persons within their department or agency and, in addition, to the Executive Branch Equal Employment Opportunity Office.

DISCRIMINATION/HARASSMENT-FREE WORKPLACE POLICY

POLICY NO. 601.001 (Eff. 10/15/13)

- e. Departments are responsible for making sure all complaints are investigated promptly. Departments may take appropriate interim action while an investigation is pending, including placing an accused person on leave or temporarily in another position.
 - f. If the Department finds that an employee violated the Discrimination/Harassment-Free Workplace Policy, the Department will take appropriate corrective action, up to and including termination of the employee, in accordance with applicable State laws, rules, policies, and collective bargaining agreements. If the person found to have violated the policy is not employed by the State or its appointing authorities, other appropriate action shall be taken, including notice to the actual employer.
2. **Managers' and Supervisors' Responsibilities**
- a. Managers and supervisors are responsible for maintaining a workplace free of harassment, discrimination and retaliation. Managers and supervisors who witness or receive reports of offending action shall take immediate and appropriate action to ensure any wrongful behavior ceases, and shall forward all such reports to the designated persons within their department.
 - b. Managers and supervisors, as assigned within their departments, shall investigate complaints of alleged violations of this Policy in a fair and impartial manner.
3. **Employee Responsibilities**
- a. Employees are expected to conduct themselves appropriately while at work and during work-related functions and refrain from any acts of discrimination, harassment or retaliation.
 - b. Employees who experience or observe any unlawful harassment, discrimination or retaliation, have a duty and responsibility to report the incident(s) in order to correct and prevent unlawful harassment, discrimination or retaliation.

DISCRIMINATION/HARASSMENT-FREE WORKPLACE POLICY

POLICY NO. 601.001 (Eff. 10/15/13)

D. REFERRING COMPLAINTS TO EXTERNAL AGENCIES

1. In addition to the procedures described above, employees may make complaints about discrimination, harassment, or retaliation in the workplace to other appropriate agencies, including but not limited to, the federal Equal Employment Opportunity Commission (www.eeoc.gov) and the Hawai'i Civil Rights Commission (<http://labor.hawaii.gov/hcrc>).
2. Employees wishing to file complaints with other agencies should contact that agency to obtain information on their specific procedures and should not wait for resolution of a complaint made to the employer. Agencies may have time limitations for filing complaints. For example, complaints of unlawful discriminatory practices must be filed with the Hawai'i Civil Rights Commission no later than one hundred eighty (180) days, or with the Equal Employment Opportunity Commission no later than three hundred (300) days from the date: (1) the alleged unlawful discriminatory act occurred; or (2) the last occurrence in a pattern of ongoing discriminatory conduct.

VII. AUTHORITIES AND REFERENCES

Title VII of the Civil Rights Act of 1964 as amended

The Pregnancy Discrimination Act

The Age Discrimination in Employment Act of 1967

The Equal Pay Act of 1963

Titles I and II of the Americans with Disabilities Act of 1990 as amended

Sections 102 and 103 of the Civil Rights Act of 1991

Sections 503 and 504 of the Rehabilitation Act of 1973

The Genetic Information Nondiscrimination Act of 2008

The Immigration Reform and Control Act of 1986

Chapter 378, Hawaii Revised Statutes

VIII. ATTACHMENTS

Attachment A: Discrimination Complaint Form, HRD Form 613

Attachment B: Discrimination/Harassment-Free Workplace Policy Acknowledgment Form

STATE OF HAWAII
Attachment A
DISCRIMINATION COMPLAINT FORM

HRU FORM 6

COMPLAINANT INFORMATION

Last Name	First Name	Middle Name
Address and Phone	Job Title, Branch, Division	

ALLEGED OFFENDERS

Name	Job Title/Organization
Name	Job Title/Organization
Name	Job Title/Organization

BASIS OF COMPLAINT

Check box or boxes for applicable protected class.

<input type="checkbox"/> Race	<input type="checkbox"/> Color	<input type="checkbox"/> Sex/Gender	<input type="checkbox"/> Gender Identity or Expression	<input type="checkbox"/> Sexual Orientation	<input type="checkbox"/> Pregnancy
<input type="checkbox"/> Breastfeeding	<input type="checkbox"/> Religion	<input type="checkbox"/> National Origin	<input type="checkbox"/> Ancestry	<input type="checkbox"/> Age	<input type="checkbox"/> Disability
<input type="checkbox"/> Genetic Information	<input type="checkbox"/> Marital Status	<input type="checkbox"/> Arrest and Court Records	<input type="checkbox"/> Income Assignment for Child Support	<input type="checkbox"/> National Guard Absence	<input type="checkbox"/> Uniformed Service/Veteran's Status
<input type="checkbox"/> Citizenship	<input type="checkbox"/> Credit History or Credit Report	<input type="checkbox"/> Domestic or Sexual Violence Victim Status	<input type="checkbox"/> Retaliation	<input type="checkbox"/> Other (Specify)	

COMPLAINT SUMMARY

(Provide details of who, what, when, and where. Attach additional pages if needed.)

REQUESTED REMEDY

(Provide corrective action or remedies you are seeking.)

WITNESS INFORMATION

(Provide names and contact information for witnesses, if any. Attach additional pages if needed.)

Witness Name	Job Title/Organization/Phone
Witness Name	Job Title/Organization/Phone
Witness Name	Job Title/Organization/Phone

The information provided above is truthful and accurate to the best of my knowledge.

Complainant's Signature: _____

Date: _____

Complaint Received by: _____

Name, Title, Signature

Date: _____

**NOTICE OF RIGHTS AND RESPONSIBILITIES - COMPLAINANT
INTERNAL INVESTIGATION**

I UNDERSTAND THAT I have the following rights and responsibilities during the internal investigative process:

1. My cooperation, as the Complainant/Reporting Party, is critical to the investigative process and I am expected to respond truthfully to questions posed and provide relevant information, documentation, and evidence in a timely and complete manner.

2. Although not required, I may have a representative of my choosing with me during the investigative interview(s). Further, I am responsible for arranging the presence of my representative at any meeting with the investigator(s). The role of the representative during these meetings will be to provide me with support and consultation, and not to respond for me or disrupt the proceedings.

3. The State may consolidate multiple or related complaints, when appropriate. Further, if I withdraw or change my mind about pursuing my complaint/report, the investigation may continue because management may have a separate duty to investigate.

4. I will be informed when the investigation of my complaint is completed, if applicable. Further, as permissible, I may be informed that corrective action has been taken as a result of my complaint; however, I will not receive information of any specific disciplinary action taken against any employee.

5. I may file a charge with the appropriate Federal or State agencies in matters alleging discrimination under law, regardless of the status of my complaint filed with the State. Further, my complaint with the State does NOT extend the filing deadlines specified by these agencies.

6. Federal and State laws, as well as State policy, expressly prohibit RETALIATION of any person who participates in the internal investigative process, including anyone who complains, makes a report, provides information, is interviewed, or aids in the investigation. Acts of RETALIATION are considered separate violations and can be upheld even if the original complaint is not sustained. Further, if I experience any action that I believe to be retaliatory because I filed a complaint, I should report it immediately. Reports of retaliation can be directed to my supervisor, manager, PMS, PHAO, Departmental Human Resources Office, Departmental Affirmative Action Office, or the Executive Branch Equal Employment Opportunity Office (587-1162 or eeo@hawaii.gov).

7. I am responsible for maintaining CONFIDENTIALITY and should not discuss matters relating to the investigation with the Accused, any potential witness, and others who do not have a legitimate "need to know."

- The investigation will be conducted in the most CONFIDENTIAL manner possible. Further, the investigator(s) or appropriate management official(s) may have an obligation to inform Accused individuals of allegations and to offer them an opportunity to respond. In addition, the investigator(s) may use and reveal information obtained during the course of the investigation to solicit further information. Absolute CONFIDENTIALITY of my identity, information provided, and/or evidence acquired during the investigation cannot be guaranteed.

- The Accused, certain managerial and supervisory personnel, and others, as necessary, may see the investigative findings and determination. Further, with appropriate certification or legal order, the report of investigation may be provided to government agencies, courts of law, parties to a grievance, arbitration, lawsuit, or others, as applicable.

8. By signing below, I acknowledge that I have received notice of the above Rights and Responsibilities. I further acknowledge that I am not waiving any of my rights, including those provided by a Collective Bargaining Agreement.

9. I understand that I may contact my supervisor, manager, PMS, PHAO, Departmental Human Resources Office, Departmental Affirmative Action Office, or the Executive Branch Equal Employment Opportunity Office (587-1162 or eeo@hawaii.gov) if I need further information about this notice.

NAME (*Please print*) _____ SIGNATURE _____

DATE _____

LINDA LINGLE
GOVERNOR OF HAWAII



CHIYOME LEINAALA FUKINO, M.D.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH
P. O. BOX 3378
HONOLULU, HI 96801-3378

In reply, please refer to:
File:

December 13, 2005

TO: All Deputies, Division Chiefs, Staff Officers, District Health Officers, and Administrators of Attached Agencies

FROM: Chiyome Leinaala Fukino, M. D. 
Director of Health

SUBJECT: **WORKPLACE VIOLENCE ACTION PLAN**

The purpose of this memo is to provide the attached Workplace Violence Action Plan. Representatives from State personnel departments and the Department of Human Resources Development (DHRD) collaboratively developed the policy to encourage and maintain a safe work environment for state employees. The Department of Health (DOH) has adopted this policy.

This plan applies to all personnel in the Department of Health and applies to any act or conduct that causes physical harm or property damage, including incidents involving co-workers, clients, customers, or other outside individuals who represent potential threats in the work environment. The action plan provides protocol options when an event occurs and should be used as a guide. Because each situation may differ, administrators, managers, supervisors, and employees should use their own judgment and discretion when responding. As a reminder, managers will continue to be responsible to conduct and conclude an investigation in a reasonable and timely manner.

DHRD offers two workplace violence training programs, one for employees, and the other for supervisors. The supervisory training program focuses on the skills necessary to resolve workplace violence complaints of employees. DHRD recommends new employees attend a session within the first six months of hire. Thereafter, refresher courses once every four years. However, programs may require re-training more often depending upon the type of work setting and past exposures to workplace violence. Cost-free sessions statewide are conducted by DHRD throughout the year.

This policy supersedes our DOH Intra-Departmental Directive 95-1 dated January 10, 1995.

If you have any questions, please contact Ms. Jan Munemitsu, Training, Safety and Employee Relations Officer, at 586-7396.

Attachments

c: Deputy Director, Department of Human Resources Development
Training, Safety and Employee Relations Officer

LINDA LINGLE
GOVERNOR OF HAWAII



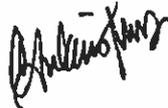
CHIYOME LEINAALA FUKINO, M.D.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH
P. O. BOX 3378
HONOLULU, HI 96801-3378

In reply, please refer to:
File:

INTRA-DEPARTMENTAL DIRECTIVE 05-1
December 13, 2005 **Page 1 of 26**

TO: All Deputies, Division Chiefs, Staff Officers, District Health Officers,
and Administrators of Attached Agencies

FROM: Chiyome Leinaala Fukino, M. D. 
Director of Health

SUBJECT: **DEPARTMENT OF HEALTH WORKPLACE VIOLENCE ACTION PLAN**

05-1.1 **POLICY**

The Department of Health is committed to partnering with its employees to encourage and maintain a safe work environment. Toward this end, all reports of incidents involving acts or displays of violence, threats of violence, intimidation, damage to property, and other disruptive behavior will be taken seriously and dealt with appropriately.

05-1.2 **RATIONALE**

State employees are a valued resource. Each employee is entitled to be treated with courtesy and respect at all times.

05-1.3 **DEFINITIONS**

"Disruptive behavior" means behavior that interrupts or impedes the progress, movement, or duties or responsibilities of an employee.

"Intimidation" means engaging in actions that include, but is not limited to, stalking or behavior that is intended to frighten, coerce, or induce duress.

"Physical attack" means unwanted or hostile physical contact such as hitting, fighting, pushing, shoving, or throwing objects.

"Property damage" means damage to property, including property owned by the State, State employees, customers, clientele, visitors, or other outside individuals.

“Threat” means an expression, verbal or non-verbal, of an intention to inflict physical or mental harm or injury. An expression constitutes a threat without regard to whether the party communicating the threat has the present ability to carry it out and without regard to whether the expression is contingent, conditional, or expected in the future.

“Workplace violence” means, but is not limited to, intimidation, threats, physical attacks, or property damage, acts of violence committed at the workplace by or against State employees, clients, customers, relatives, acquaintances, or other outside individuals.

05-1.4 SCOPE

This plan applies to all personnel in the Department of Health. It applies to any act or conduct that causes physical harm or property damage, or that makes an employee feel scared, frightened, threatened, worried, or unsafe about his or her physical safety, including incidents involving co-workers, clients, customers, or other outside individuals who represent potential threats in the work environment.

05-1.5 RESPONSIBILITIES

A. Department of Human Resources Development (HRD)

HRD shall:

1. Conduct periodic workplace violence training programs for supervisors, managers, and employees on how to identify disruptive behaviors, how to investigate complaints, and the potential consequences of failing to act;
2. Maintain and provide to the departments a current listing of references and resources available in the community as provided at www.hawaii.gov/hrd/, see Workers' Compensation and Safety menu;
3. Collect and analyze the data provided on the *Annual Workplace Violence Report*;
4. Advise departments if a trend emerges which requires immediate attention; and
5. Provide consultative services to departments on an as-needed basis.

B. Department of Health

1. Department Head

a. The Department Head shall:

- (1) Ensure compliance with the statewide policy, *Workplace Violence Program*, DHRD Policy No. 800.002 and this *Workplace Violence Action Plan*; and
- (2) Support a safe work environment by encouraging all employees and outside individuals to practice courtesy, respect, and kindness at all times.

b. The Department Head may establish departmental procedures or guidelines to supplement the statewide policy.

2. Departmental Personnel Office

The Departmental Personnel Office (DPO) shall:

- a. Advise management, supervisors, and others as appropriate, in matters relating to workplace violence;
- b. Identify, coordinate, and/or provide appropriate training for supervisors and employees on various aspects of workplace violence;
- c. Ensure all new employees receive the statewide policy, *Workplace Violence Program*, HRD Policy No. 800.002 and this *Workplace Violence Action Plan*;
- d. Coordinate REACH (Resource For Employee Assistance & Counseling Help) and other support systems for employees, as appropriate;
- e. Support a safe work environment by encouraging all employees and outside individuals to practice courtesy, respect, and kindness at all times;
- f. Review the *Department Workplace Violence Fact Finding Worksheet (Attachment D-2)* and implement appropriate corrective actions as warranted; and

- g. Prepare the *Annual Workplace Violence Report (Attachment F)* and submit to HRD/Safety Office.

3. Administrators, Managers, and Supervisors

All administrators, managers, and supervisors shall:

- a. Ensure that all employees under their chain of command are aware of and familiar with the terms of this *Workplace Violence Action Plan*, including the consequences of violating such plan;
- b. Ensure that all reports of workplace violence be treated in a confidential manner and that information is shared only on a need-to-know basis;
- c. Identify and initiate efforts to timely rectify working and/or other conditions that may contribute to a violent incident;
- d. As soon as practicable, report all incidents to appropriate department or office head of potentially violent employees, clients, or customers, including all confrontational incidents, domestic violence reports, and those incidents with clients and employees who require the support of colleagues or law enforcement officials to maintain situational control and complete and submit the *Department Workplace Violence Fact Finding Worksheet (Attachment D-2)*;
- e. Call for help/assistance as appropriate; and
- f. Support and encourage a safe work environment by getting to know employees and practicing courtesy, respect, and kindness at all times.

4. Each employee shall:

- a. Attend a workplace violence training program;
- b. Comply with work practices designed to make the workplace more secure;
- c. Refrain from engaging in verbal threats or physical actions which create a security hazard to other

employees, clients, customers, or other individuals in the workplace;

- d. Report to the immediate supervisor any acts of potentially violent behavior displayed by co-workers, clients, customers, or other individuals using the *Employee's Report of Workplace Violence Form (Attachment D-1)*;
- e. Inform his/her immediate supervisor of any domestic violence incidents, threats, restraining orders, or any violations to restraining orders as may impact the workplace;
- f. Immediately call 911 when any threat or act of violence is observed or received; and
- g. Support and encourage a safe work environment by practicing courtesy, respect, and kindness at all times.

05-1.6 EVENT PROCEDURES

A. Guidelines for Use of Protocol Options

The following protocol options shall be used as a guideline only. Because each situation will be different, administrators, managers, supervisors, and employees shall not be prevented from using their own good judgment and discretion when responding.

The protocol options listed below in part B, are also contained in the *Workplace Violence Action Plan Protocol Desk Reference (Attachment A)* which may be reproduced and used as a reference.

B. Protocol Options for Administrators, Managers, Supervisors and Employees

1. Protocol No. 1

a. Examples of Protocol No. 1 Behaviors

- Use of weapons, including items that may be used as weapons
- Threats of bodily harm
- Hostage situations
- Physical and sexual assaults

- Bomb threats
- Temporary restraining order (TRO) violations
- Property damage
- Suicide
- Stalking

b. Action Steps for Protocol 1 Situations

- (1) Call 911 immediately.
- (1a) If bomb threat, follow department bomb threat procedures.
- (2) Call building security or internal departmental security or sheriff, as applicable.
- (3) Secure the office entrances and exits, as appropriate, until police, internal departmental security, or sheriff arrives.
- (4) Call for medical assistance, if needed.
- (5) Notify your DPO at 808-586-4520.
- (6) Follow instructions provided by law enforcement.
- (7) Remain available to provide witness statements.
- (8) Manager to conduct and conclude an investigation in a reasonable and timely manner, if appropriate¹.

2. Protocol No. 2

a. Examples of Protocol No. 2 Behaviors

- Threatening Messages
 - E-mail
 - U.S. Mail
 - Phone Calls
 - Fax

¹ In consultation with DPO, consider "Leave with Pay Pending Investigation", if appropriate.

b. Action Steps for Protocol 2 Situations

- (1) Call 911 to report threats.
- (2) Call building security or internal departmental security or sheriff, as applicable.
- (3) Secure the office entrances and exits, as appropriate, until police, internal departmental security, or sheriff arrives.
- (4) Notify your DPO at 808-586-4520.
- (5) Immediately isolate the e-mail, mail, or fax.
- (6) Immediately document content of phone call.
- (7) Follow instructions provided by law enforcement.
- (8) Remain available to provide witness statements.
- (9) Manager to conduct and conclude an investigation in a reasonable and timely manner, if appropriate.²

3a. Protocol No. 3A

a. Examples of Protocol 3A Behaviors

- Abusive or vulgar language
- Yelling
- Displays of anger

b. Action Steps for Protocol 3A Situations

- (1) Diffuse anger (See Attachments B & C).
- (2) Remove and isolate the employee to a private area (supervised by 2 or more persons).

² In consultation with DPO, consider "Leave with Pay Pending Investigation", if appropriate.

- (3) If necessary, call for assistance (911 or building security or internal department security or sheriff, as applicable.
- (4) Notify your DPO at 808-586-4520 of circumstances.
- (5) Manager to conduct and conclude an investigation in a reasonable and timely manner³.
- (6) Manager to develop action plan in consultation with DPO.
- (7) Manager to implement action plan.

3b. Protocol No. 3B

a. Examples of Protocol 3B Behaviors

- Intimidation
- Repeated behavior that causes distress in a reasonable person

b. Action Steps for 3B Situations

- (1) Notify your DPO at 808-586-4520 of circumstances.
- (2) Manager to conduct and conclude an investigation in a reasonable and timely manner⁴.
- (3) Manager to develop action plan in consultation with DPO.
- (4) Manager to implement action plan.

³ In consultation with DPO, consider "Leave with Pay Pending Investigation" or "Department Directed Leave", if appropriate.

⁴ In consultation with DPO, consider "Leave with Pay Pending Investigation" or "Department Directed Leave", if appropriate.

3c. Protocol 3C

a. Examples of Protocol 3C Behaviors

- Indicators of harmful behaviors to self or others

b. Action Steps for Protocol 3C Situations

- (1) Remove the employee to a private room to calm and reassure him/her, providing continuous observation.
- (2) Notify your DPO at 808-586-4520 of circumstances.
- (3) Contact employee's emergency contact.
- (4) Contact employee's health care provider, if known, to seek assistance.
- (5) If employee's emergency contact or health care provider cannot be contacted, call DOH ACCESS Line for assistance:
 - 832-3100 (Oahu)
 - 1-800-573-6879 (Neighbor Islands)
- (6) Develop plan of action in consultation with DPO⁵.

05.1-7 POST EVENT PROCEDURES

A. Debriefing

The division, staff office, attached agency administrator, and/or supervisor shall:

1. Review and verify the *Employee's Report of Workplace Violence* from (Attachment D-1) and the *Department Workplace Violence Fact Finding Worksheet* (Attachment D-2) and work with employees involved in event to ensure documentation is correct, proper and timely;

⁵ Consider "Department Directed Leave", if appropriate.

2. Conduct investigation of incident using *Investigator's Summary Record (Attachment E)* as a guide and with assistance from the Departmental Personnel Office;
3. Analyze facts, events, evidence, etc., and determine if working and/or other conditions contributed to the event and what procedures can be implemented to prevent future occurrences;
4. Determine the need and arrange for post-trauma counseling when appropriate; and
5. Collaborate with the Departmental Personnel Office to determine if, after an investigation, whether disciplinary action is appropriate.

B. Reporting Requirement to HRD/Safety Office

Each department shall submit the *Annual Workplace Violence Report (Attachment F)* to the HRD/Safety Office one month after the conclusion of the reporting period.

05.1-8 AUTHORITIES AND REFERENCES

Workplace Violence Program, DHRD Policy No. 800.002, effective 12/18/03

Workplace Violence: Prevention, Intervention, and Recovery, Hawai'i Workplace Violence Working Group Committee, October 2001

05.1-9 ATTACHMENTS

Attachment A: Protocol Desk Reference
Attachment B: Techniques for Handling Difficult Behavior
Attachment C: Coping with Threats and Violence
Attachment D-1: *Employee's Report of Workplace Violence* form
Attachment D-2: *Department Workplace Violence Fact Finding Worksheet*
Attachment E: *Investigator Summary Record*
Attachment F: *Annual Workplace Violence Report* form

**DEPARTMENT OF HEALTH
WORKPLACE VIOLENCE ACTION PLAN PROTOCOL DESK REFERENCE**

PROTOCOL NO. 1	
<ul style="list-style-type: none"> • Weapons (Including items that may be used as weapons) • Threats of Bodily Harm • Hostage Situations • Physical and Sexual Assaults 	<ul style="list-style-type: none"> • Bomb Threats • TRO Violations • Property Damage • Suicide • Stalking
<ol style="list-style-type: none"> 1. Call 911 immediately. 1a. If bomb threat, follow department bomb threat procedures. 2. Call building security or internal departmental security or sheriff, as applicable. 3. Secure the office entrances and exits, as appropriate, until police, internal security, or sheriff arrives. 4. Call for medical assistance, if needed. 5. Notify your DPO at 808-586-4520. 6. Follow instructions provided by law enforcement. 7. Remain available to provide witness statements. 8. Manager to conduct and conclude an investigation in a reasonable and timely manner, if appropriate⁶. 	

PROTOCOL NO. 2
<ul style="list-style-type: none"> • Threatening Messages <ul style="list-style-type: none"> ▪ E-mail ▪ U.S. Mail ▪ Phone Calls ▪ Fax
<ol style="list-style-type: none"> (1) Call 911 to report threats. (2) Call building security or internal departmental security or sheriff, as applicable. (3) Secure the office entrances and exits, as appropriate, until police, internal security, or sheriff arrives. (4) Notify your DPO at 808-586-4520. (5) Immediately isolate the e-mail, mail, or fax. (6) Immediately document content of phone call. (7) Follow instructions provided by law enforcement. (8) Remain available to provide witness statements. (9) Manager to conduct and conclude an investigation in a reasonable and timely manner, if appropriate⁷.

⁶ In consultation with DPO, consider "Leave with Pay Pending Investigation", if appropriate.

⁷ In consultation with DPO, consider "Leave with Pay Pending Investigation", if appropriate.

PROTOCOL NO. 3A	
<ul style="list-style-type: none"> • Abusive or Vulgar Language • Yelling • Displays of Anger 	
<ol style="list-style-type: none"> 1. Diffuse anger. <u>See</u> Techniques for Handling Difficult Behavior and Coping with Threats & Violence 2. Remove and isolate the employee to a private area (supervised by 2 or more persons). 3. If necessary, call for assistance (911 or building security or internal department security or sheriff, as applicable). 	<ol style="list-style-type: none"> 4. Notify your DPO at 808-586-4520 of circumstances. 5. Manager to conduct and conclude an investigation in a reasonable and timely manner⁸. 6. Manager to develop action plan in consultation with DPO. 7. Manager to implement action plan.

PROTOCOL NO. 3B	
<ul style="list-style-type: none"> • Intimidation • Repeated Behavior That Causes Distress in a Reasonable Person 	
<ol style="list-style-type: none"> 1. Notify your DPO at 808-586-4520 of circumstances. 2. Manager to conduct and conclude an investigation in a reasonable and timely manner⁹. 3. Manager to develop action plan in consultation with DPO. 4. Manager to implement action plan. 	

PROTOCOL NO. 3C	
<ul style="list-style-type: none"> • Indicators of harmful behaviors to self/others 	
<ol style="list-style-type: none"> 1. Remove the employee to a private room to calm and reassure him/her, providing continuous observation. 2. Notify your DPO at 808-586-4520 of circumstances. 3. Contact employee's emergency contact. 4. Contact employee's health care provider, if known, to seek assistance. 	<ol style="list-style-type: none"> 5. If employee's emergency contact or health care provider <u>cannot</u> be contacted, call DOH ACCESS Line for assistance: <ul style="list-style-type: none"> ➢ 832-3100 (Oahu) ➢ 1-800-573-6879 (Neighbor Islands) 6. Develop plan of action in consultation with DPO¹⁰.

⁸ In consultation with DPO, consider "Leave with Pay Pending Investigation" or "Department Directed Leave", if appropriate.

⁹ In consultation with DPO, consider "Leave with Pay Pending Investigation" or "Department Directed Leave", if appropriate.

¹⁰ Consider "Department Directed Leave", if appropriate.

Techniques for Handling Difficult Behavior

1. Be aware of the individual's and your own nonverbal cues (avoid negative nonverbal signals, lack of sensitivity, empathy).
2. Recognize and deal with your own feelings. Focus on not being defensive in your communication.
3. If you have to confront the individual, decide to do so with care and respect.
4. Use active listening techniques. Do not reply to abusive or destructive statements. Reply only to constructive statements. (This is effective for those who use obscene language and are defensive.)
5. Keep focus from shifting away from problems. Be assertive by repeating key ideas. (This is effective for those who are vague, talkative, mentally ill, or visibly restless.)
6. Recognize and acknowledge individual's feelings and allow time to vent emotions.
7. Refrain from arguing, giving advice, or expressing personal feelings.
8. Avoid manipulation. Explain consequences of behavior honestly and directly.
9. Explain and clearly define the role of agency and your own role. (The perpetrator's concern and reaction may be due to confusion.)
10. Take responsibility for your own behavior – apologize when appropriate.
11. Show respect by leaving responsibility for change up to perpetrator.
12. If behavior continues to be unyielding or dangerous, leave the site of confrontation immediately and seek additional assistance from co-worker or the supervisor by using predetermined code words.

Coping with Threats and Violence

For someone angry or hostile:

- Stay calm. Listen attentively.
- Maintain eye contact.
- Be courteous. Be patient.
- Keep the situation in your control.

For someone shouting, swearing, or threatening:

- Signal co-worker or supervisor that you need help. (Use prearranged code word.)
- Do not make any calls yourself.
- If necessary, call for assistance (911 or building security or internal department security or sheriff, as applicable).

For someone threatening you with a gun, knife or other weapon:

- Stay calm. Quietly signal for help. (Use prearranged code words.)
- Maintain eye contact.
- Stall for time.
- Keep talking – but follow instructions from the person who has the weapon.
- Don't risk harm to yourself or others.
- Never try to grab a weapon.
- Don't try to be a hero.
- Watch for a safe chance to escape.

TECHNIQUES FOR HANDLING DIFFICULT BEHAVIOR

1. Be aware of the individual's and your own nonverbal cues (avoid negative nonverbal signals, lack of sensitivity, empathy).
2. Recognize and deal with your own feelings. Focus on not being defensive in your communication.
3. If you have to confront the individual, decide to do so with care and respect.
4. Use active listening techniques. Do not reply to abusive or destructive statements. Reply only to constructive statements. (This is effective for those who use obscene language and are defensive.)
5. Keep focus from shifting away from problems. Be assertive by repeating key ideas. (This is effective for those who are vague, talkative, mentally ill, or visibly restless.)
6. Recognize and acknowledge individual's feelings and allow time to vent emotions.
7. Refrain from arguing, giving advice, or expressing personal feelings.
8. Avoid manipulation. Explain consequences of behavior honestly and directly.
9. Explain and clearly define the role of agency and your own role. (The perpetrator's concern and reaction may be due to confusion.)
10. Take responsibility for your own behavior – apologize when appropriate.
11. Show respect by leaving responsibility for change up to perpetrator.
12. If behavior continues to be unyielding or dangerous, leave the site of confrontation immediately and seek additional assistance from co-worker or the supervisor by using predetermined code words.

COPING WITH THREATS AND VIOLENCE

For someone angry or hostile:

- Stay calm. Listen attentively.
- Maintain eye contact.
- Be courteous. Be patient.
- Keep the situation in your control.

For someone shouting, swearing, or threatening:

- Signal co-worker or supervisor that you need help. (Use prearranged code word.)
- Do not make any calls yourself.
- If necessary, call for assistance (911 or building security or internal department security or sheriff, as applicable).

For someone threatening you with a gun, knife or other weapon:

- Stay calm. Quietly signal for help. (Use prearranged code words.)
- Maintain eye contact.
- Stall for time.
- Keep talking – but follow instructions from the person who has the weapon.
- Don't risk harm to yourself or others.
- Never try to grab a weapon.
- Don't try to be a hero.
- Watch for a safe chance to escape.

Instructions to Complete the Employee's Report of Workplace Violence Form (Attach. D-1)

WHO COMPLETES THE EMPLOYEE'S REPORT OF WORKPLACE VIOLENCE FORM?

Workplace violence may be personal and directed at a specific employee, therefore, the employee who believes that unacceptable workplace behavior has been committed shall complete this report.

Where the unacceptable behavior is overt and directed at more than one employee, each employee may submit a report or, as a group, submit the report. Reports of similar behavior(s) exhibited by the same alleged perpetrator(s) may be combined.

1. UNDESIRE BEHAVIOR OR ACTIVITY

- Describe and be specific as to the type of behavior exhibited, and pattern, if applicable. For example: "John Doe uses abusive language toward me every time I operate the reproduction machine" or "Jane Doe slammed her files loudly around her office when her supervisor goes on vacation" or "Jane Roe said, 'I'll get you' and pointed her index finger 2-inch away from my face."

2. DATE, TIME, LOCATION, FACILITY

- Describe when and where the behavior occurred.
- If behavior is continuous, state frequency. For example: "Everyday," or "When required to do a specific task."

3. EXACT PLACE

- Describe the precise location. For example: "Mauka end of parking Lot C" or "Immediately outside Jane Doe's office."

4. DESCRIBE THE ALLEGED PERPETRATOR

- Provide name, if known, or provide physical description. For example: "About 35 years of age, 5 foot, 10 inches tall, male, Asian, tattooed cross on left forearm, unkempt hair."
- Provide clothing descriptions. For example: "Wore baseball cap, cargo shorts." [Check off appropriate blocks, as applicable.]

5. VICTIMS

- Provide name(s) of victim(s).

6. WITNESS

- Provide names(s) and phone number(s).

7. INJURY

- Describe all cuts/contusions/types of injuries. For example, "Arm contusion from being hit by baseball bat."

8. PROPERTY DAMAGE

- Describe item(s) and how damaged.

9. ASSISTANCE REQUESTED

- Check appropriate blocks. If other, describe.

10. PREPARED BY:

- Provide name(s) of employee(s) submitting report.

11. SUBMITTED TO:

- Provide name and follow the "chain of command", which usually begins with the supervisor. However, if the supervisor is the alleged perpetrator, then refer to the division chief or the Departmental Personnel Officer.

12. DATES (MM / DD / YY)

Employee's Report of Workplace Violence

Objective: To record instance(s) of observed or experienced violent or disruptive behavior in the workplace with the intent of management or personnel office intervention to mitigate or eliminate such activity.

Describe the undesired behavior or activity (specific language, gesture, physical contact or conduct):

Date of incident: _____ **Approximate time:** _____ a.m. or p.m.

Location address _____ **Facility/building:** _____

Exact place of incident (hallway, locker room, break area I, room no., parking lot, etc.):

Describe perpetrator: _____

Stranger: ; **Customer:** ; **Employee:** ; **Supervisor:** ; **Family member:** ; **Other:**

Victim or intended victim(s): _____

Witness (Names and Phone no.): _____

Injury (location, type, degree): _____

Property damage (items damaged): _____

Assistance requested: **Police:** **Division Chief:** **Personnel Office:** **Other** _____

Note: There shall be no retaliation or discrimination against an employee who submits this report, calls for appropriate assistance, complains of an incident, or who is called upon as a witness.

Prepared by: _____

Date: _____

Submitted to: _____

Date: _____

6/29/05

Instructions to Complete Department Workplace Violence Fact Finding Worksheet (Attach. D-2)

WHO COMPLETES THE DEPARTMENT WORKPLACE VIOLENCE FACT FINDING WORKSHEET?

The worksheet is usually completed by the supervisor of the unit where the alleged workplace violence behavior was reported. The purpose of fact finding is to obtain preliminary data for further action.

While the Employee's Report of Workplace Violence form is usually the report of facts witnessed by an employee, fact finding is primarily gathering data from the employee as well as other witnesses within the work unit. The fact finding may also include witnesses outside of the work unit.

- 1. SPECIFIC BEHAVIOR EXHIBITED**
Describe with specificity. For example: "Threw a paperback instruction manual across the room at John Doe" or "Repeatedly hit the employee with a baseball bat" or "Shouted expletives and threw a pen at Roe."
- 2. NAME OF PERSON(S) AND FUNCTION OF PERSON**
Identify the person(s) and his/her relationship to staff. For example: "John Doe—customer" or "John Roe—client" or "Jane Q. Public—agitator/demonstrator" or "Jane Doe—co-worker."
- 3. DATE, TIME, LOCATION - Self explanatory**
- 4. LIST VICTIM(S) OR OTHER(S)**
Identify all individuals who were the target of the alleged perpetrator's actions.
- 5. LIST WEAPONS, TOOLS, ETC. WHICH WERE USED IN THE INCIDENT**
Describe the weapon/tool used, e.g., knife, letter opener, baseball bat, pencil. Note: Leave weapon in place for investigator's review, take pictures, or bag/isolate weapon, if possible (without compromising blood, finger print evidence, etc.).
- 6. NAME OF WITNESS AND PHONE NUMBER**
Identify and obtain name(s) and phone number(s) only – do not interrogate.
- 7. PERSONS INJURED - Self explanatory**
- 8. STATEMENT**
State only what you saw and heard in the incident. Do not include what others may have heard or seen.
- 9. WHY DID THE INCIDENT OCCUR?**
If possible, identify potential explanations for the alleged perpetrator's behavior, including precipitating events such as divorce, debt, management style, or court outcome. For example: "Client felt she was denied perceived benefits/rights."
- 10. WHAT HAPPENED?**
Identify individuals, offensive/abusive/ belittling comments, statements, gestures, etc.
- 11. CHECK APPROPRIATE BLOCK OR DESCRIBE IN "OTHER"**
- 12. NAME OF OTHER INDIVIDUAL(S)**
Identify the instigator, bully, front man, denied client, etc.
- 13. NAME OF PERSONS AND ORGANIZATIONS**
Identify the attorneys, investigators, unions, mediators, etc.
- 14. RECOMMENDATIONS**
Based on the facts presented, recommend potential (and alternate) outcome of the incident to minimize reoccurrences.
- 15. SIGN AND SUBMIT**

Department Workplace Violence Fact Finding Worksheet

Department: _____ Division: _____

Work unit: _____ Island: _____ Date: _____

1. Describe behavior or activity of the offender:

2. Name of person(s) exhibiting, verbalizing, demonstrating, or otherwise conveying the behaviors or activities.

3. Date _____ and time _____ of behavior. If recurring, list past dates and times where the behavior or activity was exhibited:

Date	Time	Location/Address
___/___/___	_____ am/pm	_____
___/___/___	_____ am/pm	_____
___/___/___	_____ am/pm	_____

4. List employee(s) that were subject to or the target of the behavior or activity:

5. If a weapon, tool, or items used in the incident, describe the items (type, kind, size, etc.):

6. Names of individuals present (witness) when the incident occurred:

Name	Address/Organization	Phone
_____	_____	_____
_____	_____	_____
_____	_____	_____

7. Persons Injured:	Name	Organization/Name of Employer	Type of Injury	Body Part
	_____	_____	_____	_____
	_____	_____	_____	_____
	_____	_____	_____	_____

8. State in your own words what happened in the order it occurred, what you saw, and what you heard from those involved in the incident: (Attach additional pages as needed)

9. Why/how did the incident occur?

10. Who started or initiated the behavior or activity?

11. Check the behavior(s) that best describes the situation:

- Race/ethnicity slurs
- Sexual inferences
- Finger Gestures
- Harassing
- Disruptive Customer
- Touching
- Stalking
- Bullying
- Assaults
- Threats w/wo weapons
- Domestic threats
- Other (Describe): _____

12. Name of other individuals (including non-employees), who were (may have been) involved or in some way contributed to the behavior:

13. Name of persons and organizations used to assist in resolving the behavior or activity:

14. Recommendation(s):

Submitted by: Name: _____; to whom: _____

Signature: _____; Date: _____

Division Chief review: _____ Date: _____

Comments/Action by Division Chief:

Forward to Department Personnel Officer: _____ Date: _____

Workplace violence Classification Category (circle): ONE TWO THREE

Action by DPO:

Resources used by the DPO to assist in the resolution of the behavior or activity:

Investigator Summary Record (Attach. E)

WHO COMPLETES THE INVESTIGATOR'S SUMMARY RECORD?

The department is ultimately responsible for taking action for all workplace violence and other inappropriate incidences in the workplace. A department is culpable for all undesired incidences in their facilities including not identifying the cause of the disruption and for not taking action to prevent future reoccurrences.

A department may call upon private investigators, the Attorney General's Investigator's Office, or Public Safety Security Office, and county police, who will file a report if called upon in response to the incident. However, a departmental manager or personnel officer should be the "neutral third party" who completes the investigation and ensures compliance action and/or remedies are instituted.

1. ALLEGATION AND DATE

- The allegation is the initial description of what is contained in the Employee's and Fact Finding Reports. However, in the course of the investigation, the investigator may want to restate or refine the allegations as well as summarize the issue.

2. SUMMATION OF INVESTIGATION

- Conduct investigations in sequence, beginning with any witnesses first, and the alleged perpetrator last. The investigator shall have all the pertinent facts addressed before talking to the alleged perpetrator.
- Note any initial assessments of unacceptable behavior from all parties' point of view.
- Explain extenuating circumstances. If possible, consider cultural values, perceived power brokers, management styles, cliques, biases, etc. that impeded quick resolution and conditions that must be addressed in resolving the incident.

3. IDENTIFY ALLEGED PERPETRATOR'S BEHAVIOR

- Circle all that apply.

4. PERTINENT QUESTIONS

- Address all that apply.

5. OTHER POINTS OF INTEREST

- Identify any other impediments toward resolution.

6. COLLABORATION

- Identify name(s) of individuals, organizations, etc. that were consulted regarding the incident (including their phone numbers).

7. DISPOSITION

- Note all action/activities taken, prior to, or after the investigation was concluded. Identify individuals and specify action(s) taken.

8. REMARKS

- Identify available resources to assist those involved to return to a more normal workplace situation. Identify witness, victim, perpetrator, etc.

9. RECOMMENDATION

- Provide recommendations on possible actions to be taken, including consequences.

Investigator's Summary Record

The objective of an investigation is to obtain facts from what was brought forth for review. Ideally, investigations are initiated for the purpose of minimizing the potential for the same or a similar situation occurring due to corrective and preventive inactions. Adverse action should not be contemplated until the investigation is completed, causal factors conclusive, and due process procedures observed throughout the investigation, as appropriate. The use of physical force upon another should not be tolerated in the workplace.

Allegation and date occurred:

Issue: WP Violence: ; Performance: ; Sexual Harassment: ; Other: (explain)

Summation of Investigator's interview with parties involved.

Witness 1:

Witness 2:

Witness 3:

Victim 1:

Victim 2:

Perpetrator:

Initial assessment of unacceptable behavior: Identify victim(s), perpetrator(s), instigator(s), group vs. individual activity,

Explain extenuating circumstances that impede quick resolution of the condition, situation, or problem (relationships, outside influences, management style, etc.).

Identify perpetrator behavior(s). Circle all that apply.

- | | | |
|------------------------------------|---|--|
| Disruptive | Threat verbal | Suicidal threats |
| Shows belligerence | Threat non-verbal | Physical fight |
| Instigates malicious gossip/rumors | Sends unwanted communications | Assaults workers, customers or supervisors |
| Argues frequently | Stalking | Criminal act(s) |
| Verbally abuses | Vandalizes property | Displays weapons |
| Throws, kicks, punches walls | Intentionally wastes property/merchandise | Disobeys departmental policies |
| Hostage | Harassment | Destruction of property |

Other: _____

Pertinent questions that should be clarified in the interviews include (on separate sheet):

- Did the incident involve a weapon (what type, owner, intended use, etc.)?
- Did the incident result in any lost work time and/or a workers' compensation claim?
- Was the violence or threat directed at a specific individual?
- Did the victim or anyone have prior knowledge of, or warning of, a potential incident?
- Was the perpetrator involved in any previous incidence of violence?
- Has this type of or similar incident happened before?
- If yes, what preventive actions were implemented previously, and why did it not prevent a repeat?
- Should the incident be reported to the police?
- What preventive actions will be implemented to minimize reoccurrence?

Other points of interest: _____

Collaboration in the resolution of the report or complaint was accomplished with (organization, individual, date, synopsis; e.g., UPW and DPO/LR Tom Jones, 10-10-2003).

Disposition of incident (circle all that apply, provide synopsis and name of individual):

- No action taken
- Verbal warning; date: _____
- Written warning; date: _____
- Suspension; number of days: _____
- Termination; date: _____
- Criminal indictment; charges: _____
- Corrective Action describe: _____

- Other; describe: _____

Remarks (training program, such as Anger Management, Team Building, Workplace Violence, etc. and who attended – perpetrator only, selected employees, or all, etc.):

Recommendations and reoccurrence prevention actions:

Investigation conducted by: _____ Phone No.: _____

Position title: _____ Date: _____

Office: _____ Department/Agency: _____

Annual Workplace Violence Report

Department: _____ **Year:** _____ **July – June**

Number of Workplace Violence incidents reported in the period by category and disposition:

PROTOCOL NO:	DISPOSITION:				
	No Action	Counsel/Trained	Re-assigned	Suspended	Terminated
1	_____	_____	_____	_____	_____
2	_____	_____	_____	_____	_____
3A	_____	_____	_____	_____	_____
3B	_____	_____	_____	_____	_____
3C	_____	_____	_____	_____	_____

Use of external assistance/support agencies used in the disposition of incidents:

PROTOCOL NO:	REACH	Police/PSD	DHRD	AG	Other	Gov/Media**
1	_____	_____	_____	_____	_____	_____
2	_____	_____	_____	_____	_____	_____
3A	_____	_____	_____	_____	_____	_____
3B	_____	_____	_____	_____	_____	_____
3C	_____	_____	_____	_____	_____	_____

* List agencies used to assist in the addressing workplace violence incidents:

** List incidents when the Governor's Communications/Media Office assisted in the resolution of a workplace violence incident:

Remarks:

Report completed by: _____ Date: _____