PROTECTION OF PERSONAL / PERSONNEL INFORMATION (P O P P I)

POLICY

All employees of the BWS shall take **EVERY** precaution to protect the personal information of its employees, customer, and vendors. Employees will only divulge personal information to those who have a legitimate right or need to know, and such disclosure shall be limited to only required information.

What is PERSONAL INFORMATION

An individual's first name **OR** first initial **AND** last name together with ***ANY*** of the following data:

- Social security number
- Driver's license number or HI State Identification card number
- Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

What is PERSONNEL INFORMATION

All identifiable information maintained on an employee for employment related purposes, and which is under the jurisdiction of the BWS, regardless of whether such information is also considered "personal information". This includes, but is not limited to:

- Employee's name
- Social security number
- Home address
- Birth date
- Salary

What is a SECURITY BREACH

An incident of unauthorized access to and acquisition of, unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonable likely to occur and that creates a risk of harm to a person.

Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

Employee RESPONSIBILITIES

- Treat data as **CONFIDENTIAL**
- Disclose **personal information** only when authorized to do so
- Disclose information only to those **authorized** to receive the information

Information Technology Division RESPONSIBILITIES

- Establish appropriate electronic data security programs and policies
- Identify an IT Protection Coordinator responsible for the IT aspects of POPPI
- Require written request for personal data or electronic media or printed copy authorized in writing by the departmental coordinator(s)
- Ensure that any data breach involving personal information is reported to HRO

Protecting PAPER RECORDS

- Retain records/folders in a **secure location with limited access**
- Keep records/files not being actively worked on in **locked file cabinets**
- **Protect** personal information when actively working on records containing personal information
- **Lock** record(s) in your desk, in a file cabinet with limited access, or in an individual's office when you leave your desk or work area

Protecting ELECTRONIC RECORDS

All of the following are PROHIBITED:

- Storing personal information on laptop computers
- Placing of storing personal information on removable devices and media (flash drives, CD, DVD, tapes, or diskettes) *unless* you have permission from the departmental coordinator AND the information has been encrypted (not just password protected)
- Placing large amounts of personal information (names, addresses and phone numbers of all employees) on diskettes, CD's, DVD's or flash drives, even when the data is encrypted
- Placing personal information in electronic folders on file servers that are accessible to other employees not authorized to access the information
- E-mailing entire social security numbers. However, when necessary, the last four digits may be e-mailed
- Do not send personal information by email

When you MAY disclose information

- Only when a **written and signed request** from an employee, customer, or vendor for the disclosure of his/her records is submitted
- A **collective bargaining agreement** requires the disclosure
- To respond to a **subpoena or court order**

DISPOSING of Protected Information

All **paper documents** containing personal information must be:

- **DESTROYED** in such a manner that the information *cannot be read or reconstructed*
  - Burned
  - Pulverized
  - Cross Shredded

All **electronic documents**, files or media (including hard drives, laptops, diskettes, CD's, DVD's or flash drives) containing personal information must be:

- **DESTROYED / ERASED** in such a manner that the information *cannot be practicably read or reconstructed*
- Consult with I.T. Division

Using a Contractor to Destroy Records

- Divisions must ensure that all requirements of the law are met
- Division representatives must **witness destruction** of documents

REMEMBER:

- Unauthorized communication is strictly prohibited
- Be alert for possible information breaches
- Report/consult with HRO when in doubt

In the Event of a Security Breach:

Step 1: Employee reports breach to supervisor
Step 2: Supervisor reports breach to Program Administrator/Officer
Step 3: Program Administrator/Officer reports to Manager & Chief Engineer, departmental coordinator(s), HR Office, Legal, and I.T. if breach involves IT data
Step 4: Departmental coordinator(s) report to HPD when illegal actions are suspected

Any questions, contact Human Resources at 748-5160.