WIRELESS ENHANCED 911 BOARD

POLICY ON PROPRIETARY AND CONFIDENTIAL INFORMATION

In order to meet its obligations under chapter 138, HRS, the wireless enhanced 911 board must obtain and review information deemed proprietary by wireless providers. HRS § 138-8(b) requires the board to maintain the confidentiality of all proprietary information submitted to it, and to adopt reasonable procedures to prevent the disclosure of, or access to, such information to members of the public and competitors, including members of the board representing other wireless providers and the wireline provider of enhanced 911.

Accordingly, the board adopts the following procedures:

Section 1. Identification of Confidential or Proprietary Information.

(1) "Proprietary information" is that as defined in HRS § 138-1.

(2) Information identifying subscribers shall be held confidential by the board and each of its employees, as being proprietary information belonging to the disclosing wireless provider. Identifying information shall include a subscriber's:
(a) Name;
(b) Telephone number; and
(c) Billing address.

(3) A wireless provider shall explicitly and clearly mark as confidential, prior to submission, information supplied and regarded by the carrier as proprietary.

(4) The board shall not regard as confidential or proprietary the identification of a wireless provider or a subsidiary of a wireless provider.

Section 2. Permissible Uses of Confidential and Proprietary Information. The use of confidential or proprietary information shall be limited to:

(1) Disburse funds as provided in HRS § 138-5;

(2) Discharge the duties of the board and its agents as provided in HRS chapter 138;

(3) Process revenues remitted to the board by wireless providers; and

(4) Manage calls by PSAPs in accordance with HRS § 138-5.

Section 3. Management of Confidential and Proprietary Information in the Possession of the Board.

(1) The board shall instruct, in writing, all board personnel, agents of the board, and PSAPs as to the proper management and uses of confidential and proprietary information.

(2) A nondisclosure agreement shall be signed by each board member, and any employee or agent of the board who may handle or possess information deemed confidential or proprietary.

(3) Material deemed confidential or proprietary shall be specifically and clearly identified as such by the board.

(4) Only persons specifically authorized by the board shall open board correspondence. Correspondence received by postal mail, electronic mail, or facsimile and opened by an unauthorized person shall:
(a) Not be copied;
(b) Be immediately returned to its container; and
(c) Immediately forwarded to the board.

(5) Proprietary and confidential information in the possession of the board, or any of its ~~a~~ members, agents, or others with legitimate purpose, shall be stored in a secure room, vault, or container as determined by the board. The room, vault, or container shall be kept locked when unattended or outside of normal business hours. Electronic files containing confidential or proprietary information shall be secured utilizing established mainframe protocols, stand alone servers, secured sockets, or password protected desktop applications, as determined by the board.

(6) Each copy of confidential or proprietary information may be distributed as necessary for the efficient discharge of board duties and responsibilities.
(a) Copies shall be explicitly and clearly marked as confidential.
(b) A person possessing copies of documents containing confidential or proprietary information shall be responsible for document security.
(c) A copy no longer required shall be;
1. Returned to the board immediately; or
2. Destroyed immediately in such a manner as to prevent its reconstruction.

(7) An original record or file no longer needed for processing shall be, with board approval:
(a) Sealed securely, retaining the notice of confidentiality, and transferred to the state archives and record storage center;
(b) Destroyed; or
(c) Returned to the proprietor.

Section 4. <u>Breaches of Security</u>.

(1) The board shall take immediate action to determine the cause, impact, and persons involved in a security violation of the confidential information entrusted to the board.

(2) Unauthorized access to confidential or proprietary information shall be promptly reported to the board in writing.

(3) A report of a security breach shall include a description of the incident, specific identification of the information disclosed, identification of each person who accessed the records, and the purposes for which access was obtained.

(4) The board shall notify an affected party immediately, providing a copy of the written report detailing the incident.

[Effective: May 27, 2005]