Personal Information Security Policy and Procedures
Version 1.0
Approved 11 January 2010

Purpose

The purpose of this policy is to establish procedures, in accordance with best practices and the requirements of applicable laws, for protecting personal information held by The Software Defined Radio Forum Inc. (the Forum) from compromise.

Definition of personal information

Massachusetts Personal Information Security Law 201 CRM 17.00 defines personal information that must be protected as a combination of an individual's name and any of the following: drivers license number, credit card number, or social security number.

Responsibility for protecting personal information

The Forum CEO or his designee shall be responsible for maintaining and administering this policy.

Personal Information held by the Forum

Short term: The Forum shall hold personal information regarding credit card information and related data only as long as necessary to process payment for an invoice or meeting fees, normally less than 24 hours. Such information may be received through on-line forms which have been processed by secure sites, by fax, by telephone, by mail, or by email. All credit card transactions shall be processed over secure sockets layer (SSL) links or equivalent. Neither the Forum nor its employees, shall collect, store, or maintain any personal information for more than the minimum time necessary to process such transactions. After the transaction is complete, credit card information shall be destroyed as appropriate (see below).

Long term: The Forum shall not own or maintain any corporate repository of personal information, written or electronic, other than information required for employee records as defined in the Employee Policy (Forum Policy 008).

Protection

Access: Access to all personal information shall be restricted to the minimum number of authorized employees.

Hard copy: All personal information shall be held in a locked file.

Soft copy: All personal information shall be held in password protected locations

Disposal

After use, all personal information in hard copy shall be shredded; that which is in electronic form shall be deleted from permanent and temporary storage.

Notification of compromise

If personal information held by the Forum or its employees is compromised, the individual(s) involved shall be notified as soon as possible after the compromise is discovered.

Penalties

Significant compromise of personal information on the part of a Forum employee shall result in the following penalties:

- First offense: written warning;
- Second offense: suspension for a period to be determined by the CEO;
- Third offense: dismissal.

Training

All employees shall be advised of the Forum's policies and procedures for handling personal information, and shall be reminded of these requirements annually.

References

1. Federal Trade Commission, "Fighting Fraud With The Red Flags Rule."
2. National Institute of Standards and Technology (NIST), "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," Special Publication 800-122, January 2009
3. Massachusetts 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth Federal Trade Commission "Protecting personal information: a guide for business"