Subject: **Information Security and Data Protection Policy**

Issue Date: **6/15/2010**

Issued by: **CIO**

Approved by: **CEO**

Background and purpose:

In a number of jurisdictions in which the council operates, laws have been introduced in relation to the processing of information relating to identifiable individuals - referred to in this policy as "**personal data**". These laws are primarily designed to protect our members so that their **personal data** are held, used and otherwise dealt with in appropriate ways, by imposing corresponding responsibilities on people and organizations which collect and use the data. In response to these laws, Girl Scouts of Northern California developed this policy, reflecting the council's commitment to dealing appropriately with the **personal data** which comes into its possession during the course of its business, and to explain the responsibilities of all Girl Scouts of Northern California **volunteers** when dealing with **personal data**.

When this policy refers to **"volunteers", it applies to all volunteers working with the Girl Scouts of Northern California.**

This and other Human Resources policies applicable to volunteers may be obtained from the Adult Development Department.

Introduction

Information Security is characterized by the following:

- The preservation of confidentiality, i.e. ensuring that information is accessible only to those authorized to have access;
- The preservation of integrity, i.e. the safeguarding of accuracy and completeness of information and processing methods.

Objectives

Information Security and data protection measures taken within the Council are intended to:

- Protect the information resources of the Council, its members and its business partners and suppliers, to an appropriate level depending on the criticality and/or sensitivity of the information;
- Preserve the privacy of members, volunteers, employees, business partners and other third parties that work with or for the Council, and
- Protect the integrity of the Council.

These objectives are to be achieved in a flexible manner consistent with the Girl Scouts of Northern California Mission that Girl Scouting builds girls of courage, confidence and character who make the world a better place.

Policy

Information is regarded as an asset belonging to the Council and is to be appropriately evaluated and protected against all forms of unauthorized action, whether this is access, use, disclosure, modification, destruction or denial of service. Security controls used must be sufficient to ensure the confidentiality, integrity and availability of information.

Security controls applied must be consistent with the value of the information and associated processes to the Council. Information that is considered by management to be critical and/or sensitive will require more stringent controls.

Scope

This policy applies to **volunteers** throughout the Girl Scouts of Northern California jurisdiction, wherever Girl Scout business and or activities are conducted.

It covers all organizational information and all information related to member activities, in any form and on any medium, referring to past, current and future activities.

It covers relationships with members, volunteers, employees, contractors, consultants, business partners and suppliers.

It covers all creation, processing, communication, distribution, storage and disposal of all information whether by the Council or by third parties acting on behalf of the Council.

Responsibilities and Compliance

Volunteers are responsible to read and comply with the Council's information technology policies, standards, and procedures regarding the protection of information assets, as published by the Council.

Penalties for non-compliance with this and related policies may include disciplinary action and the loss of volunteer status, depending upon the severity of the incident.

The Council retains the right to refer incidents to the police where it feels the situation requires such action or where the law demands. The Council retains the right to take legal action where it feels the situation requires such action.

Security incident reporting

All actual or suspected instances of information theft or abuse, as well as potential threats or obvious control weaknesses should be reported. For computer, data, communications or other information technology issues, the Information Technology Help Desk should receive these reports. Volunteers should report issues to the Information Technology Help Desk via 1-800-447-4475 x131 or itsupport@girlscoutsnorcal.org.

Data Processing Activities

Girl Scouts of Northern California may collect and process **personal data** about its employees and members (including ex-employees and ex-members), the employees of its business partners and suppliers and other individuals for a number of purposes related to the council's business.

Personal data includes, but is not limited to, a person's name, address(es), phone number(s), employer(s), spouse/partner name, names of children, parents, age, emergency contact information, physician or medical contacts and email address(es).

For example, the council may use **personal data** for the following purposes:

- Event and program registration, back ground and credit checks for crime prevention purposes and in the course of the Girl Scouts of Northern California's normal, legitimate business purposes.

Protection of data

To protect the **personal data** that comes into Girl Scouts of Northern California's possession, **volunteers** are required to ensure that **personal data** are used fairly and lawfully in the course of their volunteer work and not for any other purposes. The council is committed to protecting all **personal data** which it receives in the course of its business and to ensure that it is used solely for the council's legitimate business purposes, and otherwise to comply with applicable data protection or privacy law. The following principles apply to all circumstances where **personal data** are collected by or on behalf of the council:

- When an individual provides **personal data** to the council, where appropriate (i.e. unless the information is obvious or cannot reasonably be provided), the individual should be appropriately informed that Girl Scouts of Northern California will process and maintain **personal data** for Girl Scouts business **purposes only.**

- **Sensitive personal data** includes, but is not limited to, **social security number, date of birth, credit card numbers, bank account numbers and driver's license number**.

- You should seek to ensure that:

  a) **You do not transfer or communicate sensitive personal data unless it is absolutely necessary and approved. All requests for sensitive personal data related to members must be approved by the Senior Director of Membership.**

  b) You do not collect excessive or irrelevant **personal data** given the purposes for which the **personal data** is collected; and

  c) **Personal data** collected and used on Girl Scouts systems or reports should be verified as much as is possible to ensure accuracy; **personal data** where known to be inaccurate should be corrected.

  d) You do not hold **personal data** for longer than is necessary, given the purpose for which they were obtained.

  e) Paper documents that contain personal data should be kept secure and not left exposed at your home or any public location.

  f) Once the paper documents are processed they should be filed away securely, or if applicable, sent to a Girls Scouts of Northern California office for storage or destroyed when no longer needed for Council purposes.

  g) You follow appropriate security arrangements in relation to **personal data** that you hold.

- Personal member data that contains **sensitive personal data** should not be transmitted or provided to volunteers or members.

- All requests by individuals, organizations or companies to have access to girl or adult member personal data should be referred to the Senior Director of Membership and/or Adult Development.

Credit Card Data

Credit card data is considered sensitive, **personal data** and specific credit card data, as defined by the Payment Card Industry Data Security Standards (PCI DSS), may and may not be collected or stored. Due to strict compliance requirements and the risk associated with not properly securing credit card data, **the Girl Scouts of Northern California chooses NOT to store or transmit any Cardholder data or Sensitive Authentication data <u>electronically</u>.**

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether storage of each data element is permitted or prohibited; and if each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

** These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment.*

*** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).*

Definitions of Data Elements:

- **Primary Account Number** is the sixteen digit card number.
- **Cardholder Name** is the name of the person on the card.

- **Service Code** is the three or four digit number on the magnetic-stripe that specifies acceptance requirements and limitation for magnetic-stripe read transactions.
- **Expiration Date** is the expiration data shown on the card.
- **Full Magnetic Stripe** is the data stored in the magnetic strip on the card.
- **CVC2/CVV2/CID** is the three digit code on the back of the card.
- **PIN / PIN Block** is the personal identification number assigned to the card.

Storing and Handling Credit Card Data

Under the PCI DSS, if **ANY** electronic files contain data elements that require protection, they must be encrypted with 128 bit encryption and must have a password associated with the encrypted file. **In addition** the network used to store the electronic files must be separated from the "primary" network and additional security measures apply in order to meet the PCI DSS compliance requirements.

As explained above, due to these strict compliance requirements and the risk associated with not properly securing credit card data, **the Girl Scouts of Northern California chooses NOT to store or transmit any Cardholder data or Sensitive Authentication data <u>electronically</u>.**

Credit card data may not be emailed under any circumstances. Scanned images, photocopies, word processing or spreadsheet documents may NEVER be used, in any form, to SAVE or transmit Cardholder or Sensitive Authentication data. Faxing forms that contain credit card data should also be avoided. Fax machines often store the fax image electronically.

All credit card data, as previously defined, must be handled in a secure manner. If credit card data is received by fax, hard copy or exists on other hard copy paper format, the paper must be secured under lock while the credit card data is waiting to be processed. Once the credit card data has been used for payment purposes, the credit card data MUST be destroyed; cut from the form, or at a minimum blacked out and rendered unreadable, before the paper is filed for storage.

Where volunteers are involved in the collection of credit card data on paper forms for processing by the Girl Scouts of Northern California, the volunteers must:

- Never save or otherwise store, or record the credit card data under any circumstances.
- Ensure that they keep close, personal control of the paper forms while information is collected and prior to transferring the forms to the Girl Scouts of Northern California office or staff member.
- Strive to ensure that they relay any paper forms with credit card data to a Girl Scouts of Northern California office or staff member as soon as possible after collecting the information.
- Ensure that any forms that are in their possession that contain credit card data, must be completely destroyed, preferably by cross cut shredders, and is never kept or stored for any reason.
- **Ensure that under NO CIRCUMSTANCES, that they photo copy, scan, fax or otherwise electronically store or transmit copies of forms containing credit card data.**