

## **Girl Scouts of Eastern Mass**

### **Comprehensive Information Security Program Summary (CISP)**

#### **Objective:**

The objective of developing, adopting and implementing this Comprehensive Information Security Program (the “CISP”) is to **create effective administrative, technical and physical safeguards** for the protection of personal information regarding residents of The Commonwealth of Massachusetts that is collected, used, maintained, stored or transmitted by our organization and to comply with our organization’s obligations under the Massachusetts Data Security Laws and Regulations, the Federal Trade Commission’s Red Flags Rules and the General Data Protection Regulations (GDPR) governing working with data of EU citizens and people residing in the EU.

#### **The purpose of GSEM’s CISP is:**

- 1) to ensure the security and confidentiality of personal information collected, used, maintained, stored or transmitted by our organization in a manner that is consistent with industry standards;
- 2) to protect our organization against any anticipated threats or hazards to the security or integrity of personal information collected, used, maintained, stored or transmitted by our organization; and
- 3) to protect our organization against the unauthorized acquisition or unauthorized use of personal information collected, used, maintained, stored or transmitted by our organization that creates a substantial risk of identity theft or fraud against residents of Massachusetts.

#### **The scope of GSEM’s CISP includes:**

- 1) identification of the personal information collected, used, maintained, stored and/or transmitted by our organization and inventory of locations where such information is collected, used, maintained, stored and/or transmitted and the equipment that collects, uses, maintains, stores and/or transmits such information;
- 2) assignment of responsibility within our organization for implementing the various components of the CISP and specifically outlines the responsibilities of the Chief Information Security Officer, the designated individual most directly responsible for implementing and monitoring the CISP;
- 3) identification of reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of the records of our organization that contain personal information, assessment of the likelihood of the threats and the potential damage that can result from such threats, taking into consideration the sensitivity of the personal information collected, used,

- maintained, stored and/or transmitted by our organization, and evaluation of the sufficiency of existing policies, procedures, and protocols to ensure the confidentiality and integrity of personal information;
- 4) setting forth the policies and procedures our organization will utilize to safeguard the security, confidentiality and/or integrity of our records containing personal information and to ensure compliance with the Massachusetts Data Security Laws and Regulations;
  - 5) setting forth the procedures to be followed when our organization learns of a breach of security;
  - 6) provision of disciplinary actions that can be imposed on members of our workforce who fail to adhere to the requirements of the CISP, including the Data Security Policies and Procedures;
  - 7) establishment of an Identity Theft Prevention Plan consistent with the Federal Trade Commission's Red Flags Rule as applicable to our organization; and
  - 8) setting forth the policies and procedures for reviewing, modifying and approving the CISP from time to time.
  9. incorporating the General Data Protection Regulations (GDPR) governing the data of EU citizens and people residing in the EU.

GSEM will perform a complete audit, review and update of the CISP every June to ensure compliance with CISP criteria as well as with any changes/updates to Massachusetts Data Security Laws and Regulations, the Federal Trade Commission's Red Flags Rule and the General Data Protection Regulations (GDPR).

**Volunteer responsibilities under CISP:**

1. Use of Personal Information by our workforce/volunteer base:
  - a. May not use or access personal information collected, used, maintained, stored and/or transmitted by our organization for any purpose other than to fulfill their assigned responsibility.
  - b. May not disclose or transmit, intentionally or unintentionally, directly or indirectly, any personal information collected, used, maintained, stored and/or transmitted by our organization to any third party unless such disclosure or transmittal is required to fulfill such individual's assigned responsibility.
  - c. Information collected, used, maintained, stored and/or transmitted by our organization shall be limited to that amount reasonably necessary to accomplish our legitimate business purposes or necessary to comply with applicable state or federal laws or regulations.
  - d. Personal information shall be retained only for such period of time that we reasonably need such information to accomplish our legitimate business purposes or is necessary to comply with applicable state or federal laws or regulations. The Chief Information Security Officer shall periodically, and at least annually, purge or remove or direct the

purging or removal of personal information from records maintained by our organization which is no longer necessary for us to accomplish our business purposes or to comply with applicable state or federal laws or regulations. The Chief Information Security Officer shall maintain written documentation of the purging or removal of any unneeded personal information.

- e. Access to records containing personal information shall be limited to those members of our workforce/volunteer base who are reasonably required to know or have access to such information in order to accomplish their responsibilities. Members of our workforce/volunteer base who do not need access to personal information regarding a member of our workforce or a customer shall not seek access to such information and shall not examine such information if they come into contact with such information outside the scope of their responsibilities.
- f. Only employees, volunteers or contracted individuals that require access to our computer system to fulfill their job responsibilities shall have access to our computer system. Access to our computer system shall be restricted by the issuance of individualized user ID names and passwords.
- g. Any member of our workforce/volunteer base who has been terminated or their contract or agreement has expired, voluntarily or involuntarily, shall no longer have physical access to any records maintained by our organization containing any personal information effective immediately upon such termination.

## 2. Hard-Copy Records Containing Personal Information

- a. Members of our workforce/volunteer base are not permitted to take hard-copy records containing personal information off of our premises, unless authorized by the Chief Information Security Officer and necessary for such individual to fulfill their job responsibilities. If a member of our workforce/volunteer base takes hard-copy records containing personal information off our premises for any reason, whether authorized or not, such person shall maintain such records in a secure fashion (i.e., locked brief case, placed in a locked car trunk, etc.) and shall be responsible for ensuring that no third party (including family members or friends) has an opportunity to view or copy such records. Such hard copy records shall not be copied and shall be returned to the office as soon as practicable.
- b. No member of our workforce shall electronically transmit any record containing personal information wirelessly or over the internet, including as part of or an attachment to email messages, unless such record is appropriately encrypted (digitally scrambled) to the satisfaction of the Chief Information Security Officer or is through a secure website approved by the Chief Information Security Officer.

- c. No member of our workforce/volunteer base shall transmit a copy of any hard-copy record containing personal information by facsimile transmission unless such transmission is specifically within the individual's authorized scope of work, the recipient is a person our organization has a written agreement with, and the sender receives a confirmation that the transmission was duly received by the desired recipient. The person sending the facsimile shall place a copy of the confirmation that the transmission was received by the appropriate recipient with the record.
  - d. Members of our workforce/volunteer base are not permitted to take devices containing or storing electronic records containing personal information (e.g., laptops, portable hard drives, thumb drives, flash drives, CD's, DVD's or other electronic storage devices or media) off of our premises unless required by such person's job responsibilities and authorized by the Chief Information Security Officer.
3. Any member of our workforce/volunteer base who violates any part of the CISP or fails to fully comply with any Data Security Policy or Procedure contained in the CISP shall be subject to disciplinary action, up to and including termination of employment or contractual termination, all in accordance with our personnel policies and procedures as in effect from time to time. Independent contractors and other non-employees, including volunteers, who violate the relevant portions of the CISP or fail to comply with applicable Data Security Policies or Procedures are subject to appropriate action by our organization, up to and including termination of services.