WRITTEN INFORMATION SECURITY PROGRAM (WISP)

Revised and Adopted March 12, 2025

I. GENERAL

A. Objective of WISP

The objective of **Girl Scouts of Eastern Massachusetts, Inc. ("GSEMA"),** in the development and implementation of this comprehensive Written Information Security Program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of Personal Information (as herein after defined) of residents of the Commonwealth of Massachusetts (collectively, "Residents" and individually, a "Resident"), and to comply with GSEMA's obligation under Massachusetts law (i.e., M.G.L. c. 93H, M.G.L. c. 931, and 201 CMR 17.00) (collectively, "Applicable Law").

The WISP sets forth GSEMA's procedure for evaluating GSEMA's electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Personal Information of Residents.

For purposes of this WISP, "Personal Information" means the following, whether in paper, electronic, or other form:

1. A Resident's first name and last name or first initial and last name;
2. In combination with any one or more of the following data elements that relate to such Resident:
    a. Social Security number;
    b. Driver's license/number or state-issued identification card/number;
    c. Financial account number, or credit or debit card number (with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account);
    d. Medical information;
    e. Health insurance information;
    f. A user name or email address in combination with a password or security questions and answer that would permit access to the online account; or
    g. Biometric information.

B. Purposes of WISP

The purpose of GSEMA's WISP is to:

1. Ensure the security and confidentiality of Personal Information;
2. Protect against threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to, or use of, such information in a manner that creates a substantial risk of identity theft or fraud.

C. Scope of WISP

In formulating and implementing GSEMA's WISP, the intended scope is to do the following:

1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information;
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Information;
3. Evaluate the sufficiency of existing policies, procedures, client information systems, and other safeguards in place to control risks;
4. Design and implement a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of Applicable Law; and
5. Regularly monitor the effectiveness of those safeguards.

D. Data Security Coordinator

GSEMA has designated the Director of Information Technology to be GSEMA's Data Security Coordinator. He or she will be responsible for implementing, supervising and maintaining GSEMA's WISP, including:

1. Initial implementation of GSEMA's WISP;
2. Training of the following persons regarding GSEMA's WISP and Personal Information security: (a) all employees; (b) directors, officers, managers and/or partners (as applicable), if not employees (collectively, "Officers"); (c) independent contractors with access to Personal Information; and (d) any other person involved with GSEMA who has or will have access to Personal Information;
3. Regular testing of the WISP's safeguards;
4. Evaluating the ability of each of GSEMA's third-party service providers to implement and maintain appropriate Personal Information security measures for the Personal Information to which GSEMA has permitted them access, consistent with Applicable Law, and requiring such third-party service providers by contract to implement and maintain appropriate Personal Information security measures; and
5. Reviewing the scope of the Personal Information security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing Personal Information.

E. Limits on Collection and Storage of Personal Information at GSEMA

1. GSEMA is in possession of Personal Information of Residents both as an employer and conducting its day-to-day operations with Residents.
2. As an employer, GSEMA possesses Personal Information for its employees and volunteers. The Personal Information that is collected and stored for each employee and volunteer shall be limited to: that information which is necessary for employment or to volunteer, such as, but not limited to, tax forms; that information which is voluntarily provided to obtain certain benefits of employment, such as pension, health, life and disability insurances; and that information which is necessary for GSEMA to comply with state or federal laws and regulations or best practices with respect to both employees and volunteers.
3. As part of its legitimate organizational purpose, GSEMA possesses Personal Information of Residents obtained during the course of GSEMA's activities. The Personal Information that is collected and stored shall be limited to: that information which is reasonably necessary to accomplish GSEMA's legitimate organizational purpose; and that information which is necessary for GSEMA to comply with state or federal laws and regulations.
4. GSEMA shall not retain Personal Information for a period longer than reasonably required to provide requested services or meet the purpose of its collection or as required by Applicable Law.

F. Review of WISP and Procedures

GSEMA's WISP and all security measures and procedures shall be reviewed at least annually and, in addition, whenever there is a material change in GSEMA's practices that may reasonably implicate the security or integrity of records containing Personal Information. The Data Security Coordinator shall be responsible for this review and shall fully apprise the then-serving Chief Executive Officer of GSEMA of the results of that review and any recommendations for improved security arising out of that review.

II. PROTECTIONS AGAINST INTERNAL DATA SECURITY BREACH

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

A. Information and Access

1. The amount of Personal Information collected shall be limited to that amount reasonably necessary to accomplish GSEMA's legitimate organizational purposes, or necessary for GSEMA to comply with other state or federal regulations.
2. Access to records containing Personal Information shall be limited to those persons who are reasonably required to know such information in order to accomplish GSEMA's legitimate organizational purpose or to enable GSEMA to comply with other

state or federal regulations.

3. Access to electronic Personal Information shall be restricted to active users and active user accounts only.
4. Access to electronically stored Personal Information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.
5. Paper or electronic records (including records stored on hard drives or other electronic media) containing Personal Information shall be disposed of only in the following manner, in compliance with Applicable Law:
    a. Paper documents containing Personal Information shall be either redacted, burned, pulverized or shredded so that Personal Information cannot practicably be read or reconstructed; and
    b. Electronic media or other non-paper media containing Personal Information shall be destroyed or erased so that Personal Information cannot practically be read or reconstructed.

B. Officers and Employees

1. There must be regular training of employees and Officers on the detailed provisions of the WISP, including training at the inception of a new employee's employment or new Officer's service. The Data Security Coordinator shall organize such training.
2. Employees and Officers are prohibited from keeping unsecured files containing Personal Information in their work area when they are not present, or otherwise failing to take reasonable measures to protect the security of Personal Information.
3. At the end of the workday, all files and other records containing Personal Information must be secured in a manner that protects the security of Personal Information.
4. Resigned or terminated employees or Officers must return all records containing Personal Information, in any form, that may be in the former employee's or Officer's possession (including all such information stored on laptops or other portable device or media, and in files, records, work papers, etc.).
5. A resigned or terminated employee's or Officer's physical and electronic access to Personal Information must be immediately blocked. Such resigned or terminated employee shall be required to surrender all keys, access codes or badges, business cards, and the like, that permit access to GSEMA's premises or information. Moreover, such resigned or terminated employee's or Officer's remote access to Personal Information (such as internet access, e-mail access, voicemail access) must be disabled. The Data Security Coordinator shall have the right and ability to disable access to any and all computer systems and/or to change an employee's password at any time.
6. Employees and Officers are encouraged to report any suspicious or unauthorized use of Personal Information.

C. Violation of WISP by Officers or Employees

If GSEMA determines an officer or employee violates any part of the WISP shall be subject to disciplinary action, up to and including termination of employment, in accordance with any other applicable policies in place at the time of disciplinary action.

III. PROTECTIONS AGAINST EXTERNAL DATA SECURITY BREACH

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are effective immediately:

A. GSEMA's Office

1. GSEMA's office is intended to be a secure facility, due to the Personal Information contained in GSEMA's files. All paper records containing Personal Information shall be maintained in storage cabinets when the office is unoccupied.
2. Visitors shall not be permitted to visit unescorted any area within GSEMA's office that contains Personal Information.
3. GSEMA's office shall be locked at all times when unoccupied.

B. Third-Party Service Providers

1. "Third-Party Service Providers" are defined as any non-employee to whom GSEMA grants partial or full access to GSEMA's paper or electronic data that contains Personal Information or to areas within GSEMA's office in which Personal Information is stored, including but not limited to, independent contractors, vendors, andvolunteers.
2. All Third-Party Service Providers shall be subject to the standards set forth herein in that they have instituted Personal Information security measures and their business operations are in compliance with the requirements of Applicable Law as it relates to Personal Information to which GSEMA has granted them access.
3. The Data Security Coordinator shall maintain all Third-Party Service Providers acknowledgments.
4. If any member of GSEMA's workforce discovers a breach of the WISP by a Third-Party Service Provider, this must be promptly reported to the Data Security Coordinator. The Data Security Coordinator and other relevant individuals must evaluate whether the breach requires reporting as detailed in Section 4 and whether GSEMA must cease its relationship with the breaching Third-Party Service Provider.

C. GSEMA's Computers and Electronic Information Systems

1. The wireless network at GSEMA shall always be encrypted.
2. All laptops used by GSEMA personnel must be password protected. Passwords will be valid for 180 days, and must be at least 12 characters in length.
3. All portable devices used by employees or Officers of GSEMA to

send and receive their GSEMA email shall be password protected and shall be locked when not in use. Employees are discouraged from using personal portable devices for GSEMA business purposes.

4. GSEMA's computers and computer system, including any wireless system, shall, at a minimum, and to the extent technically feasible, have the following elements:

    a. Secure user authentication protocols, including:

        i. Control of user IDs and other identifiers;

        ii. A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

        iii. Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

        iv. Restricting access to active users and active user accounts only; and

        v. Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation based on geographic location for access to a particular system.

    b. Secure access control measures that:

        i. Restrict access to records and files containing Personal Information to those who need such information to perform their job duties; and

        ii. Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

    c. Encryption of all transmitted records and files containing Personal Information that will travel across public networks, and encryption of all data containing Personal Information to be transmitted wirelessly.

    d. Reasonable monitoring systems, for unauthorized use of or access to Personal Information.

    e. Encryption of all Personal Information stored on laptops or other portable devices.

    f. For files containing Personal Information on a system that is connected to the Internet, there must be reasonably up-to- date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Personal Information.

g. Reasonably up-to-date versions of system security agent software installed and active at all times, which must include anti-virus, anti-spyware, and anti-malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up- to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

D. Personal Information Removed from GSEMA

1. Employees and Officers shall only remove paper or electronic Personal Information from GSEMA when they have a legitimate and authorized business purpose for removing such information and only with prior authorization of the Data Security Coordinator.
2. Any employee or Officer of GSEMA removing electronic Personal Information from GSEMA's office shall only do so on a secure device, such as an encrypted laptop or encrypted USB drive.
3. Any employee or Officer who removes Personal Information from GSEMA must keep the Personal Information secured. The measures taken to secure such Personal Information shall include whatever is necessary to secure the information from unauthorized use or access in the environment in which the employee or Officer must use this information for their legitimate business purpose.
4. Any employee or Officer who experiences a data security breach relating to Personal Information removed from GSEMA shall immediately inform the Data Security Coordinator.

IV. PERSONAL INFORMATION SECURITY BREACH

A. Employees and Officers must notify the Data Security Coordinator in the event of a known or suspected Personal Information security breach or unauthorized use of Personal Information.

B. GSEMA shall provide notice as soon as practicable and without unreasonable delay when GSEMA (a) knows or has reason to know of a Personal Information security breach, or (b) knows or has reason to know that the Personal Information of a Resident was acquired or used by an unauthorized person or used for an unauthorized purpose. The following notices shall be issued:

1. Notice shall be provided to the Resident whose information was acquired or otherwise affected by an unauthorized person. Such notice shall include the nature of the breach of security or unauthorized acquisition or use, and any steps GSEMA has taken or plans to take relating to the incident.
2. Notice shall be provided to the applicable authorities of the state each affected Resident, to the extent required by Applicable Law. Such notice shall include the nature of the breach of security or unauthorized acquisition or use, the number of Residents affected by such incident at the time of notification, and any steps GSEMA has taken or plans to take relating to the incident.

C. Whenever there is a Personal Information security breach or unauthorized use of Personal Information, there shall be an immediate mandatory post-incident review of events and actions, taken, if any, with a view to determining whether any changes in GSEMA's security practices are required to improve the security of Personal Information for which GSEMA is responsible.

This revised and updated WISP is adopted as of 12 day of March, 2025.

Acknowledgement of Receipt- Name:

Date: