FAMILY VISIONS INCORPORATED
POLICY AND PROCEDURE MANUAL

<table>
<tr><td rowspan="3">POLICY:

SECURITY, STORAGE, RETENTION AND DESTRUCTION OF INFORMATION</td><td></td><td>POLICY NO: GEA-010</td></tr>
<tr><td>DATE Issued:
September 28, 2011</td><td>PREVIOUS POLICY DATE/NAME:
Security, Storage, Retention & Destruction of Information
BDA01-80</td></tr>
<tr><td>DATE Reviewed:</td><td>RELATED DOCUMENTS:</td></tr>
<tr><td>APPROVED BY:
Board of Directors</td><td colspan="2">DISTRIBUTION: Board Policy

APPLICATION: Family Visions Employees</td></tr>
</table>

POLICY:

To ensure that security and integrity measures are in place and followed in order to protect the integrity of information within Family Visions Inc.

To ensure that all confidential information pertaining to residents, participants or employees of Family Visions Inc., including confidential corporate information, regardless of media (electronic form, paper file, or digital image), is properly stored in a secure environment.

To ensure the security and integrity of information during transmittal by any means, including by internal and external delivery networks, voice mail, wireless technology, email and the Internet.

To establish a consistent process for the retention and destruction of information within Family Visions Inc. in accordance with various legislative requirements.

1. Family Visions Inc. as an Agency privy to confidential information will ensure that:
    a) Confidential information, regardless of medium (electronic format, paper file, microfilm, graphic, audio or digital image), is properly stored in a secure environment.
    b) Security and integrity measures are in place and followed in order to protect the confidentiality and integrity of confidential information within Family Visions Inc.
    c) The security and integrity of coincidental information is maintained during transmittal by any means, including internal and external delivery networks, voice mail, wireless technology, email and the Internet.
2. Confidential information is to be collected, used, disclosed or accessed only by individuals who are authorized for that purpose. Individuals who are authorized must have a clear understanding of the authority, parameters, purpose, and responsibilities of their access, and the consequences of failing to fulfill their responsibilities.

3. All other Family Visions Inc. information shall be stored in a secure environment that protects such information from destruction and shall only be destroyed in accordance with Family Visions Inc. policy.
4. All documents containing personal health information, personal information, or confidential agency information shall be disposed of by supervised incineration, shredding or other approved method.
5. Proper controls shall be developed to segregate confidential material from non-confidential and other waste streams. "Confidential waste" must be clearly identified so as not to be disposed of along with ordinary waste.
6. All documents containing personal health information, personal information or confidential agency information requiring the off-site disposal shall be stored and transported in a secure manner and shall be turned over only to personnel authorized by the agency to complete the process of destruction.

DEFINITIONS:

1. **Breach of Security** – occurs whenever confidential information is collected, used, disclosed or accessed by other than as authorized, or its integrity is compromised.
2. **Confidential Agency Information** – means any personnel, statistical or financial information regarding the agency which has not been authorized by release by the agency, and includes:
    a) Any documents marked confidential
    b) Any tender or proposal document
    c) Any information learned regarding an employee's salary, work history or work performance, except as released by Family Visions Inc. Administration office to comply with the Public Sector Compensation, Disclosure Act.
    d) Any information learned regarding an employee such as medical history, attendance at Employee Assistance Programs, home conditions, financial situation, and demographics including home address and home telephone number, domestic difficulties, or any other private matters that have been disclosed to Employee in the course of work or business.
    e) Any statistical or financial information learned regarding the Agency that has not been authorized for release by Family Visions Inc. office.
    f) All incident reports.
3. **Confidential Information** – includes personal health information, confidential agency information and personnel information.
4. **Integrity of Confidential Information** – means the preservation of its content throughout storage, use, transfer and retrieval so that there is confidence that the information has not been tampered with or modified other than as authorized.
5. **Personal Health Information –** refers to recorded information about an identifiable individual that relates to:
    a) The individual's health, or health care history, including genetic information about the individual.
    b) The payment for health care.

c) The Personal Health Care Number (PHIN) assigned to an individual. Personal health information may be held in any type of file, document or report. It may be in any type of medium, including paper or electronic format and stored in any facility, department or program of Family Visions Inc.

6. **Personnel Information** – means any personnel/employment information which can be traced back to a particular employee or person associated with Family Visions Inc. including:
    a) Social Insurance Number.
    b) Any information about an employee's or person associated with Family Visions Inc.'s salary, work history or work performance.
    c) Any information learned regarding an employee such as medical history, attendance at Employee Assistance Programs, home conditions, financial situation, demographics including home address and home telephone number, domestic difficulties or any other private matters that have been disclosed to Employee in the course of work or business.
7. **Secured Environment** – means a physical environment for the temporary or permanent storage, use, processing or transmittal of information that has the following characteristics:
    a) Not readily accessible by unauthorized users.
    b) Supervised or monitored by authorized users.
    c) Locked when authorized users are not in attendance.
    d) Protected by controls to minimize loss, destruction or deterioration caused by fire, water, humidity, theft, vandalism or other hazards; and,
    e) Stored in proper containers and adequately labelled to reduce accidental loss or destruction.
8. **Security Safeguards** – shall include both physical and human resource safeguards to prevent unauthorized collection, use, disclosure of and access to information. Physical security measures include such safeguards as locked filing cabinets, restricted access to certain offices or areas, the use of locked boxes and computer passwords. Human resource security measures include authorization, training and contracts.

PROCEDURE:

1. All confidential information will be placed/stored in an appropriately secured place.
2. Confidential information stored in electronic format will be properly secured from unauthorized access.
3. Individuals working on a computer must not leave the computer unattended in accessible areas. User password protocols must be in place and utilized.
4. Individuals using, accessing, transmitting, or otherwise working with confidential information contained in electronic databases should follow appropriate security measures.
5. All confidential information that is mailed through regular postal service, interdepartmental mail or sent via courier must be marked “Confidential” and have reasonable safeguards put in place to ensure security and integrity of the information.

6. Confidential information should never be left on voice mail, unless authorized by the receiver.
7. An appropriate cover sheet must be attached to all documents containing confidential information being transmitted via facsimile stating that the transmittal is confidential and that any unintended receiving party is prohibited from reading or disclosing the information to anyone else.
8. If confidential information is removed from the Employer's premises by an authorized individual, that individual shall carry the file/electronic media with them or secure storage at all times. If it is necessary to leave confidential in a vehicle or other location, it must be stored in a secure environment such as a locked trunk, file cabinet, etc.
9. No confidential information will be transported, stored, or left in a location that could result in the destruction or deterioration of that information.
10. Employees in facilities and programs will retain information in accordance with Schedule for Retention of Corporate Records (Appendix). Administration Employee will designate appropriate Employee to maintain retention schedules for their site/program.
11. Information will be destroyed or transported according to the following process at the end of the retention period.
    a) Administration will designate appropriate Employee to assume responsibility for the destruction of information. The Executive Director/designate will provide written authorization for the destruction of specific material.
    b) Designated Employee will annually sort the information by placing in appropriate containers.
    c) Containers will be packaged securely for pick up and/or storage in a secure location until incineration, shredding or transportation.
    d) Containers containing confidential information will be clearly labelled as "Confidential Material for Destruction or Transportation".
    e) Designated Employee will arrange for the shredding, incineration or transportation of the authorized information.
    f) In situations where shredding and/or incineration cannot be accommodated locally, appropriate security measure will be taken in the transportation of the confidential material to an alternate site for destruction.
12. Any service contract for the transport of delivery of confidential information shall contain:
    a) A provision providing the service provider of the requirements to safeguard the confidentiality of that information and to physically protect it from unintended destruction, including any appropriate cautions as to the perish ability of the particular medium used for the information in question.
    b) An agreement by the service provider that it and its employees or agents will protect the confidentiality, security and physical integrity of the information.