Family Focus Inc.		**Policy Number:** AG-054
Subject:	CONFIDENTIALITY AND USAGE OF ALL INFORMATION (CLIENT, EMPLOYEE, COMPANY)	
Section:	ADMINISTRATIVE GENERAL	
Effective Date 01/01/2004	**Review Date: 04/01/2015**	
	Revised Date: 02/27/2012	
☐ **New Policy**	☐ **Supersedes Policy Dated:**	
Issued by: HR Administrator	**Concurred with and Approved by:** Jim Burns, Director Initial: _____	
Cross Reference:	CR-001 Client Rights to Confidentiality; AG-003 Technology Use; AG-004 Secure Mailing and Faxing	
Distribution:	All employees of Family Focus, Inc., Inc.	

I. PURPOSE

The purpose of this policy is to provide guidelines for an appropriate and consistent level of information security for Family Focus, Inc.

In order to receive care, people entrust Family Focus, Inc. with private and sensitive information. Most people believe and expect that privacy and integrity of care information will be preserved by all who use and maintain that information. Family Focus, Inc., has a legal and ethical responsibility to honor this trust. Family Focus, Inc. is also required to protect sensitive and private records about employees, contracted employees, and other caregivers. The confidentiality, integrity, and availability of sensitive and valuable business records must be protected to enable the continued successful functioning of Family Focus, Inc.

A. Client Rights

The client has the right, within the law, to expect that all communications and records pertaining to his/her care be treated confidentially and be read only by individuals directly involved in his/her treatment or the monitoring of its quality. The client has a right to expect these records be only read by other individuals upon his/her written authorization or that of his/her legally authorized representatives. Family Focus, Inc., is committed to uphold this trust.

B. Protection of Employee/Student/Volunteer Information

Family Focus, Inc., also commits to the protection of information regarding those who care for clients. Specific information about those staff, students or volunteers directly or indirectly working with a client will not be disclosed unless in accordance with a subpoena for mental health or alcohol treatment records, or court

order, or the written request of a client as required by law. In such cases, the Family Focus, Inc., worker, volunteer will be notified regarding any release of information to a client.

C. Protection of Employee Information

Family Focus, Inc., also protects employee information that is sensitive or confidential in nature. Employees must be assured that only those individuals who require access to confidential employee information to perform their duties will, in fact, have access. Employee information includes, but is not limited to, personnel files, which are maintained by the HR Department. All employee records are the property of Family Focus, Inc., and are considered confidential. Access to personnel files is limited to Officers and Department Directors/Managers. The HR Department will provide managers with requested information, however the original file must, under most circumstances, remain secured in the HR Department's office. Records of terminated employees are the property of Family Focus, Inc., and may only be accessed by the HR Department and/or the Director. Employees wishing to review their file may make an appointment with the Director.

D. Protection of Employee Files

Employee Personnel records are maintained in our Human Resource Department. As required by law, some records pertaining to employees are maintained in a separate file relating to medical issues. The internal investigations and Performance evaluations are filed in section B of the employee personnel file. The employees, or their representative, may request access to their basic personnel file not including Medical records or Section B. Depending upon the circumstances, employees may be provided access to records pertaining to internal investigation with appropriate editing to protect the rights of others.

All requests to have access to your personnel file must be provided in writing to the HR Administrator. Upon receipt of your written request, the HR Administrator will schedule an appointment for you to view your file during normal office hours. Employees are not permitted to remove any documents from the personnel file but may provide a written response to any document in the personnel file. Written responses will be attached to the original document in the personnel file.

Employees may request copies of documents in their personnel file. Request for copies must be made in writing to the HR Administrator.

E. Staff confidentiality on Personal concerns such as Bereavement issues, illness, pregnancy, etc.

When a staff member requests leave due to personal concerns or due to the death of an immediate family member, which *includes: a son or daughter – biological, adopted or foster child; a stepchild, or a child of a person standing in the place of a parent.* A spouse (the spouse must be legal in the state), a parent (the parent must be a parent or someone who stood in loco), or a parent of current legal spouse, immediate grandparents of the employee or immediate grandparents of their spouse (the spouse must be legal in the state) and siblings of employee or the siblings of a current spouse (the spouse must be legal in the state), the HR Department or their supervisor will ask staff approval to disclose information to other staff members.

F. Protection of Corporate Information

To carry out its mission, Family Focus, Inc., must survive in an increasingly competitive environment. Corporate economic information, corporate plans and corporate business communications all play an integral

part in our ability to compete successfully. They must therefore be protected with the same level of diligence given to individual and personal confidential information.

II. GENERAL INFORMATION

A. Definition Section

Information Security is the protection of information against unauthorized access, modification or disclosure, whether in storage, processing or transit.

Information Resources includes all media that store or communicate information including, but not limited to: paper records (client records, business office records, personnel records, financial records, administrative records, etc.), computers (hardware, software, and storage media), Internet, copy machines, fax machines, telephones, answering machines, employees, printers, and typewriters.

Confidential Information is information for which the inappropriate disclosure could cause harm to a client, staff member or Family Focus, Inc.,

1) Client care information, includes, but is not limited to, all information regarding a client's identity, financial information, treatment, diagnosis, and communication between a client and family, and friends.

2) Personnel information includes, but is not limited to, employee salaries, benefits, performance review, performance Improvement processes, and any other information in the personnel file.

3) Family Focus, Inc., business information includes, but is not limited to financial and strategic performance information regarding the business transactions of Family Focus, Inc.,

The above issues will be addressed as part of

a. The purchase and implementation of new information systems or information-processing technologies.

b. Daily Family Focus, Inc., business processes which involves the actual or potential exchange of Confidential Information.

Management staff of each department will develop and maintain information security policies specific to their department, which are consistent with and support the implementation of this policy and procedure that address departmental-specific aspects of the above issues.

B. Definition of WHO has Access to Information.

Access to Family Focus, Inc., information resources will be granted based on the user's job function, business need, research requirement or legal authority.

1. Family Focus, Inc., Employees
2. Referral sources

3. Consultants
4. Authorized Government or Legal Representatives

C. Definition of HOW Information Access will be authorized:

1. Confidentiality Agreement
   a. Employees will, upon acceptance of a position as an employee of Family Focus, Inc., review the Employee Handbook, which includes a Confidentiality Agreement. Upon receipt of the Handbook, the employee will sign a document acknowledging receipt of the handbook. Thereafter, an annual review and revision as necessary of the Employee Handbook will be distributed to all employees. Employees will sign documents acknowledging each updated Handbook, and the signed document will be maintained in the employee's personnel file. It is the responsibility of each employee to review the Employee Handbook including the confidentiality agreement and the conditions under which disciplinary action may be taken should a willful security breach occur.

   b. Non-employees (defined as anyone working with or providing a service for Family Focus, Inc., who is not an employee of Family Focus, Inc., including but not limited to, volunteers, consultants, or contract services individuals) may, as part of the normal execution of their duties, come in contact with confidential and/or client specific information. Non-employees entering into an engagement and/or contract with Family Focus, Inc., are expected to complete a Confidentiality Agreement. Subsequent agreements must be completed annually thereafter or at the beginning of a new engagement/contract when a break in continuous service is greater than one year. Obtaining and storing Confidentiality Agreements from non-employees is the responsibility of the appropriate Department Head.

2. Access authentication on a computer will be accomplished through user names and passwords.
   a. Issuance of Network/System User ID's
      1) No one may access Family Focus, Inc.'s information resources or computer applications without approval from the Director.
   b. Passwords
      1) Users may choose their own passwords for access to PC workstations.
      2) Passwords are to be memorized and never written down. Passwords are never to be shared with anyone.
      3) Avoid easy-to-guess passwords, such as children's names, make of car, etc. Use complex passwords (letters and numbers, etc.).

D. Definition of Individual Responsibilities to Safeguard Confidential Information

1. Responsibilities of Information System Individuals

   a. Each individual is responsible for understanding and observing the provisions of this policy. If an employee is in doubt whether information is confidential and how it should be protected, it is his or her responsibility to consult their immediate supervisor. Contractors' questions regarding this policy should be discussed with the appropriate department or business affiliate at Family Focus, Inc., Inc.

   b. Failure to comply with Family Focus, Inc.,'s Information Security policies and procedures may result in disciplinary action, including termination without warning or notice and civil or criminal legal penalties, at the discretion of Family Focus, Inc., administration.

2. Termination of access to information resources

A person's access to Family Focus, Inc., will be revoked upon termination of employment or contract with Family Focus, Inc., Inc., when job duties no longer require access to information resources.

3. Individual Obligations under this Policy and the Confidentiality Agreement

a. During the performance of their duties, individuals may be required to have access to and be involved in the processing of confidential information, including but not limited to, client records, indexes of information, client demographics, client billing and appointment history, confidential communications made for purposes of treatment of a client, employee personnel records, including employee health records and information regarding the business strategy, financial transactions, or performance of the corporation.

b. Confidential information is not confined to written materials or hard copy, but includes information derived from any source, including, without limitation to, computer data, verbal communications or recordings, faxes, phone conversations, dictation, and videotape.

c. Confidential information is to be handled with strict discretion and not to be read, discussed, utilized by or disclosed to any person without proper authorization. All persons should exercise a high degree of professionalism and restraint when discussing or utilizing client information. If an individual is uncertain about the confidentiality status of any information, he/she should solicit assistance from a supervisor or manager.

d. Individuals are only to access, or attempt to access, information they are authorized to.

e. Individuals are to utilize Family Focus, Inc., information resources for business reasons only and will not use information resources for personal use or competitive businesses. Under no circumstances may an individual utilize the Family Focus, Inc., information resources (specifically e-mail and Internet), for personal messages, solicitation, or distribution of information that is not related to Family Focus, Inc., business.

f. Information resources, including but not limited to, Family Focus paper records, electronic communications, e-mail, and the contents of an employee's computer, are the sole property of Family Focus, Inc.,

g. User IDs and passwords are to be used solely by the individual in connection with their authorized access of information. Individuals are to take all necessary steps to prevent anyone from gaining knowledge or use of their password.

h. E-mail communications, computer systems, the Internet and any other information resources are not private and may be monitored by Family Focus, Inc., to ensure that there is no unauthorized use of the company's systems (see policy *AG-006 Technology*), to assure compliance with Family Focus, Inc.,'s policies and to investigate conduct or behavior that may be illegal or adversely affect the organization

or its employees and other constituents. (Title I of the Electronic Communications Privacy Act prohibits interception of electronic communications and Title II of the Electronic Communications Privacy Act prohibits retrieval of messages from storage. However, both Titles grant the provider of the service, Family Focus, Inc., exceptions to the prohibitions)

i. Individuals are to respect laws regarding copyrighted software and not make unauthorized copies of software.

j. Individuals are not authorized to install any software on any computer provided by Family Focus, Inc., without prior approval of administration.

k. Individuals should not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry.

l. Individuals are to report any violation of the information security policy to their supervisors. All notifications will be logged and investigated.

m. Individual obligations and responsibilities continue after termination of employment, contract, affiliation, etc. Individual access privileges are subject to periodic review, revision and if appropriate, renewal.

n. Use of Family Focus, Inc., communications facilities to convey offensive, harassing, vulgar, obscene or threatening information, including disparagement of others based on race, national origin, marital status, gender, age, disability, pregnancy, religious or political beliefs, or any other characteristic protected under federal, state or local law, is strictly prohibited.

o. Each Family Focus, Inc., information individual (employee, contract worker, students, volunteers, etc.) will be accountable for the information he/she enters, alters, and views within the Family Focus, Inc., information resources.

p. Each Family Focus, Inc., individual who signs on to a computer must sign off or lock PC when leaving it unattended in a location where it is accessible to the public or unauthorized persons.

q. Individuals will secure personal computers against theft and physical damage.

r. Definition of Mechanisms to Secure Information

1. Access Security

    a. Workstation monitors in public-access areas are to be pointed away from public view when possible.

2. Computer-Related Media Security

a. Printed reports containing confidential or sensitive information are to be stored in a lockable receptacle or secured area, inaccessible to unauthorized persons. When confidential printed reports are no longer needed, they should be shredded.

b. Flash Drives containing confidential information are to be labeled confidential and protected in a container or a secure area.

c. Flash Drives and other media containing computer files will be stored in areas accessible only to authorized persons.

3. Computerized Files Security

a. Backup copies will be stored in a safe location (not exposed to heat or magnetic fields).

b. Virus software will be used to scan flash drives and other media containing computer files and network file server disk storage.

c. Computers that need disposed will be cleared of all information and taken to a licensed disposal facility.

d. The IT Department will clear all information from cell phones that need disposed of by using the factory reset which clears the phone.

1. When each individual logs on to the Family Focus, Inc., network, his/her workstation's memory and specific system files will be automatically scanned by network-resident anti-virus software. Individuals ARE NOT AUTHORIZED to bypass or attempt to bypass this check.

2. The network anti-virus scan will automatically check any flash drive that is inserted into a Family Focus, Inc., network-attached machine. Individuals ARE NOT AUTHORIZED to bypass or attempt to bypass this check.

3. Copyright Protection / Security

a. "Shareware" or "Freeware" (software programs that are not protected by copyright) will NOT be loaded on any Family Focus, Inc., computer without approval by the Executive Director.

b. Copyrighted software may not, under any circumstances, be copied by Family Focus, Inc. staff for any purpose, even if such software is not protected by copy-protect features.

4. Copier Security

a. Confidential originals will not be left in the copier feeder or on the copier glass unattended.

b. Disposal containers will be provided near each copier for the proper disposal of pages or entire documents.

5. Data Integrity Security (computerized data)

a. Additions and alterations to information must be traceable to the individual (or the application and the user that sent the information) for the life of the information.

b. Modification history will be retrievable and reportable.

6. Data Transmission Security to/from External Locations

a. Systems which support transmission of confidential information outside the Family Focus, Inc., data network (e.g., Internet) are NOT authorized to transmit client or Family Focus, Inc., -proprietary confidential information unless:

i. Both the sending and receiving systems encrypt such data, OR

ii. Such data is transmitted exclusively via a protected medium (e.g., fiber-optic cabling, point-to-point, dedicated data line or virtual private network technologies). This network security plan requires approval by the Director.

7. Equipment Security

a. Personal computers will be kept either in offices, which can be locked after hours, or in areas, which are staffed continuously.

b. Workstation units are not to be placed on their sides unless installed or designed to operate this way (i.e., in a “tower” configuration).

c. Workstations will be placed on a clean, level surface.

d. Liquids (drinks, coffee, medicines, etc) will NOT be placed in the vicinity of a workstation where they could spill onto the equipment.

e. Workstations will not be exposed to hazardous vapors such as those from cleaning solvents.

8. Fax Machine Security

a. Numbers which are programmed or entered into fax machines to receive confidential information MUST be validated before they are actually used.

b. Disposal containers will be provided near fax machines.

c. Fax machines will be placed in secure locations - inaccessible to the general public.

9. Internet Security

a. The technical aspects of the electronic communications (Internet) shall be managed and maintained by the Family Focus contracted IT service.

b. Acceptable uses of the Internet are, but not limited to:

1. Enhance client care
2. Benefit community health
3. Provide continuing education
4. Enhance client/family education
5. Positively affect operations (cost reduction or revenue/efficiency increase)
6. Public service

c. Internet Management:

1) It is the responsibility of the immediate supervisor to state specific purposes and manage time on-line for research and professional correspondence activity.

2) It is the responsibility of the departmental manager or supervisor to address abuse of Internet Access.

10. Printer Security

a. Printers will be located in secure areas, inaccessible to the general public.
b. Individuals should be aware of the locations of printers available on print menus and which printers can be used to print confidential information.

11. Purchase / Procurement / Support of Computer Hardware and Software

a. Purchase
1) All purchase of computer hardware and software shall be approved by the Director.

b. Installation

1) Installation of all hardware, software and peripherals is performed by, or coordinated through, the contracted IT services. Such installation shall include any software not purchased by Family Focus, Inc., but approved for installation on Family Focus, Inc., -owned devices.

2) All software / flash drives which are processed on machines outside of Family Focus, Inc., Inc. must be subject to the current virus protection installed on Family Focus, Inc., computers.

c. Support

1. Family Focus, Inc., has standardized on certain desktop productivity tools and software, which are to be used by all authorized Family Focus, Inc., employees. Purchase and/or installation of any productivity software outside this group on any Family Focus, Inc.,-owned device is not permitted without prior approval from the Director.

12. Telephone Security

a. Conversations involving confidential information will be held in a private setting or with the maximum level of discretion. Verbal information should be held in the same regard as electronic and paper information.

b. Access to playback of dictation and automated voice response systems will be controlled using unique PIN numbers.

III. RESPONSIBILITIES:

It is the responsibility of each employee at Family Focus, Inc., to abide by this Policy and associated information security directives. Penalties for non-compliance with this policy may include discontinuation of Family Focus, Inc., Information Services and support, disciplinary action, termination of employment, and/or criminal prosecution depending upon the severity of the incident.