TABLE OF CONTENTS

I. Policy

The purpose of this information security policy is to protect the information possessed and used by the Department of Elder Affairs (DOEA), whether it is stored in electronic data systems or by any other means. This policy will emphasize guidelines for the protection of the confidential data that are vital to agency operations.

The data security policy is designed to provide a level of confidence that information provided to the Department of Elder Affairs by business partners, contractors and clients will be adequately protected. The Department of Elder Affairs has a responsibility to protect the privacy of our clients by establishing especially stringent protections for client data.

This policy applies to all DOEA employees, contractors and other entities that access the information resources of DOEA including paper documents and electronic data systems.

II. Authority

N/A

III. Supportive Data

A. Federal

- Section 45 CFR 160 and 164. Health Insurance Portability and Accountability Act of 1996.

B. State of Florida Statutes

- Chapter 119, Government in the Sunshine
- Chapter 213.053, Confidentiality and Information Sharing

C. State of Florida Administrative Code

- Chapter 60-DD, Information Resource Security Policies and Standards

D. Department of Elder Affairs Policies and Procedures

- **DOEA 420.10 MIS Policy and Procedures Policies** – Detailed Computer Network Security and Acceptable Computer Use Policies for the Department of Elder Affairs
- **DOEA Helpdesk Policy** – Detailed Information Technology policy on Helpdesk operation, including procedures for network access.
- **DOEA 530.30 DOEA MyFlorida Marketplace Confidential Information Policy** – DOEA policy regarding confidential data in attachments to MyFlorida Marketplace purchasing documents.

IV. Signature Block with Effective Date

Ashley Stacell
Deputy Secretary, Department of Elder Affairs

Date: 07/31/2006

V. Definitions

Information User Roles

- **All information Users –** This group includes anyone who interacts with information belonging to the Department of Elder Affairs
- **Chief Information Officer (CIO)–** The administrator responsible for the coordination of all information technology services including those related to information privacy and security.
- **DOEA Managers –** This role includes DOEA employees who supervise employees using DOEA information. DOEA managers are responsible to ensure that the employees they manage adequately protect the security of DOEA information.
- **External Information Users / Providers –** This role includes all contractors and subcontractors, service providers and vendors who use information from or provide information to the Florida Department of Elder Affairs.
- **HIPAA Privacy Officer** – The person responsible for privacy issues related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). At Elder Affairs, this is the General Counsel, and the role extends to privacy issues beyond HIPPA.
- **Information Technology Security Manager (ISM) –** This person is appointed by the Secretary to administer the department's Information Security Program, and to serve as the department's internal and external point of contact on information security matters. While these duties primarily involve information technology issues they extend to all matters related to information security.

Information Types

- **Manual Data** – Manual data comprise all data not stored or transmitted electronically. Examples include copies of faxed correspondence, client case files, paper personnel files.
- **Electronic Data –** Electronic data refers to information that is stored or transmitted electronically. Examples include information in database applications, images of documents, electronic mail messages.
- **Confidential Client Data –** Confidential client data requires the highest level of protection to ensure client privacy. Examples include client

assessment data, services provided to clients and any documents that specifically identify a client.

- **Confidential Data –** Confidential data is data that contains personal identification information. The category includes identification of vendors, subcontractors and employees. Examples include attachments to vendor invoices, time sheets and personnel records.
- **Public Record Data –** Data subject to the Florida State Government in the Sunshine Law. This includes most non-client data used in the operation of state agencies. It is generally available to the public upon request. DOEA employees are required to submit any public records requests through the General Counsel's office.

VI. Protocol

Employees and other users of information at DOEA have different roles in information security. The responsibilities and procedural guidelines will be organized according to these roles. These guidelines are to assist employees in identifying confidential data and protecting its security. Employees should refer data security questions to their supervisor, who will confer with the appropriate data security officer.

VII. Procedure

Data Confidentiality and Security Guidelines

A. Confidential Client Data – Confidential client data is any information electronic or otherwise which identifies an individual client. It addition to the identifying information such as Social Security number or name, there may be information such as the services the client has received, addresses, or medical and psychosocial assessment information. These data are protected under the Health Insurance Portability and Accountability Act (HIPPA). The department requires training in the security and privacy provisions of HIPPA to all employees.

1. The DOEA application programs such as CIRTS and CMS have security roles assigned that allow users to view the information required to perform their jobs, while protecting the privacy of our clients. All users of DOEA confidential client data should adopt similar protocols: **Share confidential client information only with persons who need the information to serve the client, and provide only the minimum amount of information required.**

2. Do not leave confidential client information in public view; this applies to paper documents and data on computer screens. **Do not remain logged into client applications such as CIRTS, CMS, or FMMIS when you are not in your office. Do not leave**

client records or other client specific data in plain view when you are not in your office.

3. Generally, any information provided to individuals who are not involved in client services should have all identifying information redacted (obscured or encrypted). **If you receive requests for client information from research organizations or other parties not involved directly in client services, please contact the Office of the Secretary or the Office of the General Counsel.**

B. Confidential Data – Confidential data is distinguished from confidential client data where the person identified is not a DOEA client but is rather an employee, vendor, contractor, volunteer, or other business associate.

1. Share confidential information only with persons who need the information for business purposes, and provide only the minimum amount of information required.
2. Do not leave confidential information in public view; this applies to paper documents and data on computer screens. **Do not leave computers screens or paper documents displaying confidential information unattended.**
3. Any supportive documents intended for MyFlorida Marketplace (MFMP) must have all identifying information obscured (redacted) before being scanned into MFMP.
4. If you need assistance in determining how to handle confidential data, please contact your supervisor, the agency HIPPA Privacy officer, or the Office of the Secretary.

C. Public Records Data – Much of the information possessed by the department is in the public domain; however, there are many important exceptions. The General Counsel's office makes determinations about what information is a public record under the Sunshine Law and what information is exempt.

1. Copies of available final published documents can be provided upon request.
2. Aggregated research data that do not identify individual clients can be provided upon request.
3. Public records requests other then routine requests for reports as indicated above should be referred to the General Counsel's office.
4. Any public record request that identifies individual people, be they clients, employees, vendors, volunteers, or any other person should be referred to the General Counsel's office for approval.

Enforcement

Any employee found to have violated these data security guidelines may be subject to disciplinary action, up to and including termination of employment.

VIII. Distribution List

Secretary
Deputy Secretary
Division Directors
Personnel Manager/Liaison
Policy and Procedures Library
Web Manager

IX. History Notes

X. Appendix