

MyFloridaMarketPlace Confidential Information Policy

1. Purpose

The purpose of this directive is to establish the policy of the Department of Environmental Protection (DEP) not to disclose protected information violating areas referenced in Chapter 119, F.S., as well as federal law and regulations such as American Health Insurance Portability and Accountability Act of 1996 (HIPAA), and any other state confidentiality laws. The directive provides guidelines for Department staff to ensure that confidential information is edited or redacted out of requisition details/comments, including supporting documentation scanned into MyFloridaMarketPlace (MFMP). It affects all MFMP users of the DEP who develop, scan, attach documents/comments, and/or review and approve MFMP records. Employees who deliberately violate this policy will be subject to disciplinary action up to and including termination.

2. Authority

The Public Records Law, Chapter 119, F.S. DEP will adhere to any State or Federal law and regulations regarding confidential information.

3. MFMP Security Officers

The DEP shall establish two MFMP Security Officers who will oversee the administration of this policy. These Security Officers shall be recognized using the following titles under this directive.

- a. MFMP Security Officer for Procurement – the person filling this position shall serve the DEP as its MFMP System Administrator. Responsibilities shall be limited to records associated with the processing of MFMP requisitions and the issuance of MFMP orders.
- b. MFMP Security Officer for Accounting – the person filling this position shall serve the DEP as the Finance and Accounting Director III responsible for Disbursements. Responsibilities shall be limited to records associated with the payment of invoices as a result of MFMP transactions.

The MFMP Security Officers shall be responsible for ensuring that all DEP MFMP users receive training on this policy and for monitoring policy compliance.

Should confidential information be found in the system, the appropriate MFMP Security Officer will be responsible for identifying the nature of the confidential information and expediting a purge request.

4. Definitions

a. Confidential Information - Records which are provided by law to be confidential or which are prohibited from being inspected by the public, whether by general or special law. DEP specific questions about confidential information should be directed to the DEP Office of General Counsel. Some examples of confidential information are provided below:

- (1) Section 119.071(4)(a)1, F.S. - The social security numbers of all current and former agency employees which numbers are contained in agency employment records are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
- (2) Section 119.071(4)(d)1, F.S. - The home addresses, telephone numbers, social security numbers, and photographs of active or former law enforcement personnel, including correctional and correctional probation officers, personnel of the Department of Children and Family Services whose duties include the investigation of abuse, neglect, exploitation, fraud, theft, or other criminal activities, personnel of the Department of Health whose duties are to support the investigation of child abuse or neglect, and personnel of the Department of Revenue or local governments whose responsibilities include revenue collection and enforcement or child support enforcement; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from s. 119.07(1). The home addresses, telephone numbers, and photographs of firefighters certified in compliance with s. 633.35; the home addresses, telephone numbers, photographs, and places of employment of the spouses and children of such firefighters; and the names and locations of schools and day care facilities attended by the children of such firefighters are exempt from s. 119.07(1). The home addresses and telephone numbers of justices of the Supreme Court, district court of appeal judges, circuit court judges,

and county court judges; the home addresses, telephone numbers, and places of employment of the spouses and children of justices and judges; and the names and locations of schools and day care facilities attended by the children of justices and judges are exempt from s. 119.07(1). The home addresses, telephone numbers, social security numbers, and photographs of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors; and the names and locations of schools and day care facilities attended by the children of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

The examples above were taken from the Florida Statutes (2005) and are subject to change/deletion through legislative action.

- b. HIPAA - American Health Insurance Portability and Accountability Act of 1996 – Law that provides compliance guidelines for handling of Protected Health Information and other confidential personal information.
- c. MFMP - MyFloridaMarketPlace – Electronic procurement system for the State of Florida.
- d. MFMP Transaction – The creation of any action within the MFMP system.
- e. Program Area – The area within the Department that generates a MFMP Transaction.
- f. Redact - to conceal from a copy of an original public record, or to conceal from an electronic image that is available for public viewing, that portion of the record containing exempt or confidential information.
- g. Supporting Attachments:
 - (1) Purchase Order Processing

Attachments sent to vendor: Any necessary terms and conditions required for the vendor to have the complete description of the transaction, such as specification sheets, diagrams and sketches, or statements of work or supplier contract forms.

(2) Payment Processing

Attachments made via the invoice eForm, Master Agreement setup, paper invoices received by the agency and input into MFMP, and any other documentation needed to support the transaction and/or show compliance with applicable laws, rules and regulations.

4. Policy

The DEP is charged with the protection of records recognized by general or special law as confidential information and shall not include in MFMP such information in any documentation supporting its MFMP transactions.

a. MFMP User Responsibilities

In order to protect confidential information from appearing in MFMP, DEP MFMP users:

- (1) Shall not enter or attach confidential information into MFMP.
- (2) Shall copy purchase order supporting documentation and edit or redact all confidential information prior to scanning into MFMP. To the extent required by law, originals will be maintained for subsequent audit purposes by the program area following established procedures to protect confidential records.
- (3) Shall copy supporting documentation for paper invoices, contractual service agreements, and any other payment documents, and edit or redact all confidential information prior to scanning into MFMP. Originals will be maintained for subsequent audit purposes by the program area following established procedures to protect confidential records.

- (4) Shall take the following action should a transaction be identified to have confidential information: Any requisition or invoice that contains confidential information and is received by a subsequent approver will be denied back to the requisitioner for deletion of the transaction and preparation of a new transaction. The requisitioner must not make the change on the non-compliant transaction for resubmission, as the history of transactions for the requisition will continue to allow access to the confidential data.
- (5) Shall not enter any confidential information into any of the comment boxes in MFMP.
- (6) Shall request assistance from the appropriate MFMP Security Officer if confidential information is found in any MFMP file that cannot be deleted without assistance from the MFMP help desk. To remove an attachment or comment that includes confidential information, the appropriate MFMP Security Office shall initiate the Florida Department of Management Services (DMS) Attachment Purge Process through the MFMP help desk.

b. Training Responsibilities

DEP shall incorporate training related to the requirements of this directive in its MFMP training program for users. This training shall address the following:

- (1) In addition to MFMP system training and prior to being granted access to MFMP, each new user will receive training on the agency's MFMP security policy, including the appropriate action(s) to be taken should confidential information be identified.
- (2) By August 1st of each year, all employees who have access to MFMP shall be provided with refresher training on the agency's MFMP security policy, including the appropriate action(s) to be taken should confidential information be identified.

c. Monitoring Efforts

To further support the policy established herein, the DEP MFMP Security Officers shall be responsible for performing the following activities at the frequency established within this directive.

- (1) On a monthly basis, the MFMP Security Officers shall:

Conduct a sampling of 10% of transactions (purchase orders and invoices) associated with object codes at risk for carrying confidential information and review attachments and comments to ensure that confidential information has not been included. A matrix summarizing the findings will be made for distribution to the Division/District/Office Directors for appropriate action. Patterns of continued non-compliance with this directive shall be reported to the Office of Inspector General for review.

To remove an attachment or comment that includes confidential information, the appropriate MFMP Security Office shall initiate the DMS Attachment Purge Process through the MFMP help desk.

- (2) On a quarterly basis, the MFMP Security Officer for Procurement shall:
- (a) Send an e-mail to remind all users within the agency of their responsibilities for identifying, removing and protecting confidential information.
 - (b) Review agency training with the MFMP Security Officer for Accounting to ensure that it includes information regarding:
 - 1 the redaction of confidential information from attachments that are to be included in MFMP, and
 - 2 the attachment removal process should confidential information be identified in the system.
- (3) On an annual basis, the MFMP Security Officers shall:

- (a) Review agency assignment of roles. MFMP Security Officer for Procurement will assign user roles based on the roles recommended by Division/District/Office Directors or their designee. Division/District/Office Directors are responsible for notifying the MFMP Security Officer for Procurement immediately if staff roles need modification/cancellation as a result of changes in staffing or changes to staff responsibilities.

Roles with "QueryAll" access should be limited to staff where this access is necessary to perform their job responsibilities. At a minimum, the following positions shall be eligible for "QueryAll" access in the system: DEP Secretary, DEP Deputy Secretaries, DEP Chief of Staff and Deputy Chiefs of Staff, Division/District/Office Directors and their Deputy/Assistant Directors, Bureau Chiefs and their Assistant Bureau Chiefs, Budget Coordinators, MFMP Coordinators and employees of the Bureaus of General Services/Finance and Accounting working in MFMP.

- (b) Review and sign-off on the DEP's training program to confirm that the requirements of this directive have been accomplished.
- (c) Review DEP Directive 390 entitled "Information Resources Security Policies and Standards" to confirm that the policy addresses the control of computers and information resources and the proper handling of confidential information.
- (d) Submit copies of the current DEP Directives 301 and 390 to the Governor's Office and the Department of Management Services upon signing by the Secretary or designee, and every subsequent year by August 1st.

Should a violation be identified or if there are specific questions about this policy, staff should immediately consult with the appropriate MFMP Security Officer.

