Florida Department of Transportation

RICK SCOTT
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

RACHEL CONE
INTERIM SECRETARY

POLICY

Effective: February 18, 2015
Review: May 1, 2017
Office: Procurement
Topic No.: 001-375-005-d
Authority: 20.23(3)(a), 334.048(3), F.S.

CONFIDENTIAL INFORMATION IN MyFloridaMarketPlace

It is the policy of the Department of Transportation (Department) to not improperly or inadvertently disclose information that is exempt from public records requirements. The Department has existing policies and procedures that govern the handling of exempt public documents, the security of information technology resources, and the security of electronic public records. These policies and procedures include access control for computer network resources, and instructions for safeguarding confidential data.

MyFloridaMarketPlace (MFMP) is a state wide electronic procurement system which does not provide access control at the agency level. The Department recognizes the need to maintain access control for its own MFMP system users and to inform those users of the importance of properly handling exempt and confidential information because of the potential for access by others outside the Department.

The Department's Procurement Officer shall be responsible for ensuring that the Department's MFMP users are familiar with this policy and understand the process for preventing the improper or inadvertent disclosure of exempt or confidential data in the requisition, purchase order and contract functions of MFMP. The Disbursement Operations Officer shall be responsible for ensuring that financial services staff responsible for the invoice reconciliation process in MFMP are familiar with this policy and understand the process for preventing the improper or inadvertent disclosure of exempt or confidential data. They are also responsible for periodic monitoring of data in the system to ensure that potentially exempt or confidential data is not entered or attached. Deliberate violation of this policy can result in appropriate disciplinary action.

Pursuant to ***Section 334.048, Florida Statutes***, the Department's Central Office shall monitor the Districts and the Central Office units that provide transportation programs, to assess their performance, and to determine their compliance with all applicable laws,

rules and procedures. The Department has established a Quality Assurance process that effectively measures compliance with critical requirements and provides for corrective actions when these requirements are not met. The process for monitoring compliance with the critical requirement of ensuring that potentially exempt or confidential data is not improperly entered in MFMP has been incorporated in the Quality Assurance process.

AUTHORITY

This policy is adopted in accordance with the following:

- Section 20.23(3)(a), Florida Statutes (F.S.)
- Chapter 119, Florida Statutes (F.S.), "Public Records"
- Section 282.318, F. S., "Security of data and information technology"
- Section 334.048, F. S., "Legislative intent with respect to department management accountability and monitoring systems."

REFERENCES

- DOT Policy No.: 001-260-001, "Quality Assurance / Quality Control"
- DOT Policy No.: 001-325-060, "Security and Use of Information Technology Resources"
- DOT Manual No.: 325-000-002, "Information Technology Resources User's Manual"
- DOT Manual No.: 375-040-020. "Commodities and Contractual Services Procurement Manual"

DEFINITIONS

For the purpose of understanding this policy, the following definitions apply:

Confidential Information: Generally, information that is specifically exempt from the public records requirements of ***Chapter 119, F.S.***, and any other data that is prohibited by Federal or State law from being disclosed. Such data may not be entered into or attached to MFMP. The following examples of confidential data are not comprehensive and all questions concerning the confidentiality of data should be addressed to the Office of the General Counsel. Data directly related to an individual that is potentially exempt or confidential includes: social security numbers, personal addresses and phone numbers, health information, medical records, date of birth, health plan beneficiary numbers, and account numbers.

Critical requirement: A measurable activity in a Departmental process that indicates whether or not the process is being properly carried out and if the quality of the product is being controlled. A critical requirement could reveal significant problems or indicate beneficial results for the Department.

MFMP: MyFloridaMarketPlace – Electronic procurement system for the State of Florida.

Quality Assurance Monitoring Plan: A monitoring plan based on critical requirements prepared by Central Office managers to outline the criteria, frequency and methods for conducting Quality Assurance Reviews.

Supporting Attachments: Any documents attached to requisitions or invoices in MFMP.

System Administrator: The position assigned the duties of approving the roles assigned to MFMP users and granting password access.

1. PROCEDURE

1.1 SYSTEM USERS AND ROLES

The Department's System Administrator shall assign user roles and passwords to Department employees after reviewing the duties and responsibilities of the user and determining the need for access to MFMP and the appropriate role. To ensure the integrity of internal controls, users with the "requester" role are not permitted to also be assigned the "approver" role, and Senior Management approval of all users' roles is required. The duties, responsibilities and roles of users are reviewed annually by the System Administrator. Each user is required to sign Department ***Form No. 375-040-51, MyFloridaMarketPlace User Registration/Update*** that includes certification that they have completed the appropriate training modules on MFMP and that they have read and understand this policy.

1.2 ENTERING DATA AND ATTACHING DOCUMENTS

Users entering data in the comments field of a requisition in MFMP will ensure that no potentially exempt or confidential data is included. Requesters will carefully review any document that needs to be attached to a requisition to determine if the document contains potentially exempt or confidential data. If the document does contain potentially exempt or confidential information, a copy must be made and the data must be redacted prior to attaching the document to the requisition. The original of the document must be maintained by the requester in a secure file for audit purposes. Invoice processors shall review all invoices and attached documents for potentially exempt or confidential data prior to scanning into the system. If potentially exempt or confidential data is found, a copy of the document must be made and the data must be redacted prior to scanning. The original documents will become part of the invoice file.

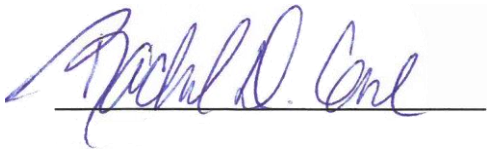
1.3 REVIEW AND APPROVAL

All approvers and purchasing staff shall review comments and attachments for potentially exempt or confidential data prior to approval. If any potentially exempt or confidential data is found in a requisition, it shall be denied back to the requester who shall delete the requisition and resubmit without the data. To remove an attachment to

an approved requisition, Purchase Order, or invoice that contains potentially exempt or confidential data, the attachment purge process must be initiated.

1.4 MONITORING

The Procurement Office and the Disbursements Operations Office shall sample data in MFMP for exempt and confidential data.



Rachel Cone
Interim Secretary