Procedure Number: 329
Effective Date: 01/14

RED FLAG IDENTITY THEFT FRAUD PREVENTION PROGRAM

SUMMARY

The Red Flag Identity Theft Fraud Prevention Program is a Federal Trade Commission regulated requirement that was signed into legislation on December 31, 2010. The Miami-Dade County policy is outlined in Resolution R-580-10, and allows individual departments to establish procedures for the prevention, detection, and mitigation of any incidents covered by this law. Identity fraud is one of the leading crimes in the world, and all preventive steps must be taken for the County to protect its constituents as well as their employees.

PROCEDURE

1. Employees should be familiar with the Resolution.
2. Employees should be aware of the risks inherent in handling secure data. Examples of data that must be protected include:
   a. Social Security numbers
   b. Bank account numbers
   c. Credit card information over the phone, in person, or via the internet.
3. All employees with access to financial information are required to take the E-Net Learning training module S-107 “Recognizing Identity Theft Red Flags”. The module has an exam which employees must pass. Once the exam is passed, the printable certificate should be submitted to their Departmental Personnel Representative (DPR) for inclusion in the employee’s personnel file.
4. Employees should be on the lookout for any potential cases of ID Theft or any compromise to personal information.
5. Any possible suspected ID Theft compromise should be immediately reported to the Departmental Red Flag Liaison.
6. The Department Red Flag Liaison will then enter the data into a Red Flag database and inform the Finance Department and Deputy Mayor. If other similar occurrences have been reported these will be viewable by the Liaisons.
7. All possible incidents must be reported to the Finance Red Flag Program Administrator immediately within 48 hours of their discovery.
8. The Administrator will access the entire County’s Red Flag database, and review if other instances of a similar variety have occurred or been reported by other departments.
9. The Departmental Liaison will work with the Administrator and Manager of the Section or Division to determine what action, if any, is needed. If there does not appear to be any fraudulent intent, it will be so noted on the database.
10. If the Administrator feels that there are sufficient grounds for a full-fledged fraud investigation, the Administrator and Departmental Liaison will coordinate these efforts with the appropriate law enforcement agency.

11. Certain employees are privy to private information of customers, citizens, constituents, and employees. It is imperative that this information be safeguarded at all times. Directors and supervisors must ensure that they maintain an active role in overseeing the handling of this data. DPRs are responsible for ensuring that all designated employees complete training on an annual basis, and that new hires or transfers with access to confidential information immediately complete the training module.

CONTACT(S):
Department/Division
Information Technology Department/Security and Finance Department