

Federal Communications Commission Washington, D.C. FCC Directive	FCC DIRECTIVE	
	FCCINST 1139	
	Effective Date: March 2007	Expiration date: March 2012

TO: All Employees

SUBJECT: Management of Non-Public Information

1. Purpose and Scope

The purpose of this directive is to establish policies and procedures for managing and safeguarding non-public information. The Commission has four general categories of information: (1) classified national security information; (2) sensitive but unclassified information having to do with homeland security, law enforcement, intelligence, defense, and foreign affairs; (3) non-public information; and (4) public information routinely made available for public inspection.

While the Commission routinely makes a great deal of category 4 information available for public inspection, there are situations in which statute, regulation, policy, and the integrity of the Commission's decision-making process require that the agency protect certain materials that are not already protected under categories 1 and 2 identified above. Therefore, this directive applies to all category 3 non-public information as set forth in 47 C.F.R. Section 0.457. It DOES NOT apply to category 1 classified information related to national security and category 2 homeland security, law enforcement, intelligence, defense, and foreign affairs information categorized as sensitive but unclassified. Category 1 and 2 information are subject to procedures set forth in separate statutes, regulations, and policy statements. Information on how to deal with Category 1 and 2 information can be found in the Information Security Manual (FCC Instruction 1131.1).

DISTRIBUTION:

ORIGINATOR:

Performance Evaluation and Records Management
 Office of the Managing Director

Form A-312
 January 1985

The Freedom of Information Act and Privacy Act apply to all four categories of Commission information and this directive does not negate or supersede the requirements of those statutes.

All employees are subject to the requirements outlined here. These requirements are also applicable to contractors as a term of their contract with the Commission.

2. Policy

Unauthorized disclosure of non-public information is prohibited by the Commission's rules, and those rules set forth the procedures under which non-public information may be publicly disclosed (47 C.F.R. Section 19.735-203). Unauthorized disclosure of non-public information may result in disciplinary action (47 C.F.R. Section 19.735-107). In the case of contractors, unauthorized disclosure may result in termination of the contract, replacement of a contract employee, or other appropriate measures.

3. Definitions

a. **Non-public information.** Section 0.457 of the Commission's Rules provides a list of the different types of non-public information maintained at the Commission. This directive applies to all information listed in Section 0.457, except for: (1) information related to national security and (2) homeland security, law enforcement, intelligence, defense, and foreign affairs information categorized as sensitive but unclassified. This directive applies to material in all formats, including but not limited to paper, computer files, e-mails, diskettes, CD-ROMs, audio and video recordings, and oral communications. There are two categories of non-public information:

- (1) **Non-Public-Highly Sensitive/Restricted.** Information that is highly market-sensitive (i.e., disclosure of which is likely substantially to affect the value of securities traded publicly or a company's market valuation); commercial or financial information the Commission considers confidential and highly sensitive; and any other material that is deemed highly sensitive, in the discretion of a Bureau/Office Chief.

For purposes of determining whether disclosure of information is likely substantially to affect the value of securities or market valuation, factors to consider include: the size of the transaction, in total dollar value or other objective measure (where applicable); the level of external interest; and/or whether the proceeding is likely to set a novel or important precedent.

- (2) **Non-Public-For Internal Use Only.** All other non-public information not routinely available for public inspection.

4. Designation of an Internal Security Officer

An individual will be designated in each Bureau or Office, including the Chairman's and Commissioners' offices, to oversee implementation of this directive. Internal Security Officers will provide guidance to the Bureau or Office Chief about which matters or items should be categorized as Non-Public-Highly Sensitive/Restricted; authorize the removal of such documents from the agency on a case-by-case basis; and ensure employees are informed of the proper handling of non-public information.

5. Unauthorized Disclosure, Loss or Theft

- a. Any unauthorized disclosure, loss, or theft of non-public information should be reported to the Bureau or Office Internal Security Officer or the Inspector General.
- b. An Internal Security Officer who receives a report of an unauthorized disclosure, loss or theft must take appropriate action, such as referring the matter to the Inspector General for possible investigation.

6. Procedures for Handling Non-Public Information

- a. **Determination of category.** The Bureau or Office responsible for creating or using information (in the case of material submitted to the agency) is responsible for determining into which category it falls. This may be accomplished in consultation with the Bureau or Office Internal Security Officer. Where more than one Bureau or Office is participating in a matter, the lead Bureau or Office (i.e., the organization responsible for drafting a decision, preparing a report or audit, etc.) will make the determination. Except for information specifically categorized as Non-Public-Highly Sensitive/Restricted, all non-public information is deemed Non-Public-For Internal Use Only.
- b. **All non-public information.** All non-public information must be handled in accordance with the procedures for creating, maintaining, and disposing of information (in whatever form) that are identified in this directive and:
 - (1) The FCC Computer Security Program directive (FCC INST 1479.2)
 - (2) The Commission's Records Management Program (FCC INST 1110.1)
 - (3) The Commission's Freedom of Information Act Program (FCC INST 1179.1)
 - (4) The Commission's Privacy Act Program (FCC INST 1113.1)

Non-public information at the Commission's headquarters building must be disposed of in a locked document disposal bin. These bins are located throughout the Portals building, including in all copier rooms, front offices, and Chairman/Commissioners' offices. Material at non-headquarters locations (for example, in field offices, Gettysburg, Laurel lab, etc.) should be disposed of in a manner that protects it from unauthorized public disclosure consistent with local practices.

c. Commission agenda and circulation items

Circulation and agenda items that are not categorized as Highly Sensitive/Restricted and that are distributed to any person or Bureau or Office must bear a cover sheet marked "Non-Public-For Internal Use Only." These cover sheets are available from the Office of the Secretary to be used for open meeting items (blue) or circulation items (pink). This directive does not modify procedures for electronic distribution of agenda items set forth in the Agenda Handbook for items categorized as Non-Public-For Internal Use Only. Agenda items categorized as Non-Public-Highly Sensitive/Restricted shall be handled as specified in Section 6d below.

d. Non-Public-Highly Sensitive/Restricted information.

The following procedures apply only to Non-Public-Highly Sensitive/Restricted information:

- (1) Each time a decision is made to designate a piece of information as Non-Public-Highly Sensitive/Restricted, a primary contact must be designated by a Bureau or Office Chief or other senior official as having lead responsibility for the particular matter or item that is considered Non-Public-Highly Sensitive/Restricted. Where more than one Bureau or Office is participating in a matter, the Primary Contact will be designated by the Bureau or Office having lead responsibility for that matter. The lead Bureau or Office may also designate a back-up Primary Contact in the event that the Primary Contact is unavailable.
- (2) Commercial or financial information for which a request for confidential treatment is pending may be accorded the protections set forth in this directive that are applicable to Highly Sensitive/Restricted information, in the discretion of the Bureau or Office handling the matter. Otherwise, until a determination is made, such material will be accorded confidential treatment, consistent with Section 0.459 of the rules.
- (3) Only staff directly responsible for handling the matter or those with a "need to know" may have access to Highly Sensitive/Restricted information. This requirement applies to both written and oral communications. The Primary Contact will monitor who has access to Highly Sensitive/Restricted information through means determined by the Primary Contact as appropriate to each specific situation.
- (4) In no circumstances should Highly Sensitive/Restricted information be left in a place accessible to non-authorized personnel when not in use.
- (5) Labeling, copying and dissemination.
 - a. Each page of documents created by the agency should be labeled "Non-Public-Highly Sensitive/Restricted." A document template is available in the agency's Word software. For material that can only be labeled manually, ink stamps are available on request from the Administrative Services Center.

- b. Special care should be exercised when copies are made on shared printers and copying machines.
- c. Paper copies must be distributed in sealed envelopes labeled "Special Attention Mail; To be opened by _____." These envelopes may be obtained from the Administrative Services Center. Labeled cover sheets, which are also available from the Administrative Services Center, may be placed on top of the document as a further precaution.
- d. Copies should never be left in unsecured In-Boxes or on unattended desks or chairs.
- e. If electronic dissemination occurs, the transmission should clearly note that the information is Highly Sensitive/Restricted and the information should only be transmitted under secure conditions to individuals with a need to know

7. Training Program

Every new employee must receive and review a brochure setting forth the policies in this directive during their new employee orientation. Internal Security Officers are responsible for assuring that on-going employees are familiar with the requirements for handling of non-public information. Certifying that employees are properly trained and equipped to carry out the requirements of this directive is one element of the annual certification required by Section 8 (below).

COTRs will also be provided with copies of the brochure to provide to contractors who have access to non-public information. COTRs will be annually asked to certify that their contractors are familiar with the requirements for handling non-public information.

8. Annual Certification

The Chairman, Commissioners and Bureau and Office Chiefs will annually certify to the Office of Managing Director that procedures are in place for the handling of non-public information in compliance with this directive. In the offices of Chairman and Commissioners, the certification may be made by the Internal Security Officer. Certifications are to be made on the last workday of June of each year.

9. Responsibilities

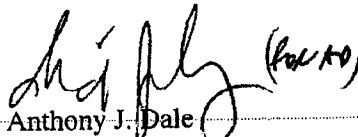
a. **Office of the Chairman and Commissioners, Bureaus and Offices**

- (1) Appoint an Internal Security Officer and make the identity of that individual known to all staff. In a case where the Internal Security Officer is unavailable, the Bureau or Office Chief, Chairman or Commissioner will serve in that capacity.
- (2) Ensure, through the Internal Security Officer or his or her designee, that appropriate training on the principles of this directive is afforded to all employees within that Bureau, Office or Chairman's/Commissioner's Office. The Internal Security Officer of the Office of Managing Director or his or her designee will, on request, provide training to the Offices of the Chairman and Commissioners.

- (3) Appoint a Primary Contact and a back-up for each matter involving Highly Sensitive/Restricted information in which the Bureau or Office has lead responsibility.
- (4) Take reasonable measures to ensure compliance with non-public information management controls set forth in Section 4.
- (5) Categorize information into levels of protection noted above, and determine who within the organization should have access to Highly Sensitive/Restricted material.
- (6) Advise OMD if additional computer or other security resources are needed to maintain security for Highly Sensitive/Restricted information.
- (7) Refer as appropriate alleged unauthorized disclosure, loss or theft to the Internal Security Officer and Inspector General.
- (8) Seek appropriate authorization pursuant to Part 19.735.203 of the Commission's rules prior to disclosure of non-public information when appropriate.
- (9) Make the annual certification of compliance noted in Section 8 above.

b. Managing Director

- (1) Appoint an agency-wide Internal Security Officer for non-public information.
- (2) Establish and disseminate policies and procedures to protect non-public information and ensure those policies are coordinated with all the information policies noted in Section 6b of this directive.
- (3) Provide material necessary to the implementation of this policy (document disposal bins, stamps, templates, envelopes, cover sheets, etc.).


Anthony J. Dale
Managing Director

Stocked:

Performance Evaluation and Records Management
On the Intranet – <http://intranet.fcc.gov/omd/perm/directives/index.html>