

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	Management of Nonpublic Information	
	Directive Number: FCC INST 1139.1	Effective Date: February 2015

TO: All Employees

SUBJECT: Management of Nonpublic Information

1. Purpose and Scope

The purpose of this directive is to establish policies and procedures for managing and safeguarding nonpublic 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) nonpublic information; and (4) information routinely made available for public inspection.

This directive applies to all category 3 nonpublic information in all formats, including, but not limited to, paper, computer files, emails, diskettes, CD-ROMs, audio and video recordings, and oral communications. This directive DOES NOT apply to category 1 classified national security information and category 2 sensitive but unclassified information having to do with homeland security, law enforcement, intelligence, defense and foreign affairs. The policies and procedures for managing and safeguarding category 1 and 2 information can be found in the Information Security Manual (FCC Instruction 1131.2).

The Freedom of Information Act and the Privacy Act apply to all four categories of information and this directive neither negates nor supersedes the requirements of those statutes.

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

2. Policy

Unauthorized disclosure of nonpublic information is prohibited by Section 19.735-203 of the Commission's rules and 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. Background

Section 0.451 of the Commission's rules explains that records routinely available for public inspection are listed in Sections 0.453 and 0.455 of the Commission's rules and all other records are not routinely available for public inspection. Section 0.457 of the Commission's rules lists by category information the Commission has determined to withhold from public inspection. Section 0.457 explains, as appropriate, the legal and policy rationale for withholding from public inspection each category of information listed in the rule.

4. Definitions

Nonpublic Information. Nonpublic information includes all information that (i) is NOT routinely available for public inspection and (ii) is NOT characterized as category 1 classified national security or category 2 sensitive but unclassified having to do with homeland security, law enforcement, intelligence, defense and foreign affairs. As defined below, there are two types of nonpublic information: "Highly Sensitive/Restricted" and "For-Internal Use Only."

(1) **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.

- a. 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.
- b. Bureau and Office Chiefs in exercising their discretion may conclude that particular types of proceedings are always deemed Highly Sensitive/Restricted. For example, agenda: and circulation enforcement cases are particularly sensitive because unauthorized disclosures of nonpublic information to a target of an enforcement

action or to a third party can have potentially severe consequences for the enforcement matter itself as well as for targets, other parties involved in investigations, the Commission as a whole, and individual employees at every level. As a result, to protect the identity of the target and the nature of the investigation against it until the Commission acts by taking public action, all circulation and agenda enforcement cases are deemed Highly Sensitive/Restricted.

(2) **For-Internal Use Only.** All nonpublic information that is NOT Highly Sensitive/Restricted.

5. Unauthorized Disclosure, Loss or Theft

Any unauthorized disclosure, loss, or theft of nonpublic information should be reported to the Bureau or Office Chief or the Inspector General.

6. Procedures for Handling Nonpublic Information

- a. **Determination of Category.** The Bureau or Office responsible for creating information or using information (in the case of material submitted to the agency) is responsible for determining into which category the information falls. This may be accomplished in consultation with the Office of General Counsel. 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. As noted above, all circulation and agenda enforcement cases are deemed Highly Sensitive/Restricted. 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 Commission's rules.
- b. **Other Relevant Directives.** Guidance regarding maintaining and disposing of nonpublic information is also included in the following directives:
 - (1) FCC Cyber Security Program (FCC INST 1479.4)
 - (2) Records Management Program (FCC INST 1110.1)
 - (3) Freedom of Information Act (FOIA) Request (FCC INST 1179.2)
 - (4) Privacy Act Manual (FCC INST 1113.1)
- c. **Disposal.** Nonpublic information at the Commission's headquarters building must be disposed of in a locked document disposal bin. These bins are located throughout the Portals I and II buildings, including all copier rooms, front offices and Chairman/Commissioner' 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.
- d. **Commission Agenda and Circulation Items/Cover Sheets.** 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 "For Internal Use Only/Nonpublic." 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 For Internal Use Only. Agenda items categorized as Highly Sensitive/Restricted shall be handled as specified below.
- e. **Special Procedures for Nonpublic Highly Sensitive/Restricted Information.** The following procedures apply only to Highly Sensitive/Restricted information:
 - (1) Each time a decision is made to designate a piece of nonpublic information as 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 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) 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.
 - (3) In no circumstances should Highly Sensitive/Restricted information be left in a place accessible to non-authorized personnel when not in use.
 - (4) Labeling, copying and dissemination.
 - a. Each page of Highly Sensitive/Restricted documents created by the agency should be labeled. For most documents, the label should denote that the document contains "NONPUBLIC, CONFIDENTIAL, HIGHLY SENSITIVE/RESTRICTED INFORMATION." Highly Sensitive/Restricted documents created by the Enforcement Bureau should be labeled "NONPUBLIC, CONFIDENTIAL, HIGHLY SENSITIVE LAW ENFORCEMENT INFORMATION."
 - b. Enforcement cases on circulation shall include a special notice at the top of the Cover Memo. This notice shall clearly denote that the case on circulation is an "Enforcement Case" and cite the Commission's

rules prohibiting the disclosure of nonpublic information. The notice shall be printed in red or other color to highlight the importance of protecting Highly Sensitive/Restricted nonpublic information in enforcement cases and shall include, at a minimum, the following text:

NONPUBLIC, CONFIDENTIAL, HIGHLY SENSITIVE
THIS IS AN ENFORCEMENT CASE.
UNAUTHORIZED DISCLOSURE IS PROHIBITED.

Enforcement investigations and actions are strictly confidential. All employees are prohibited from disclosing any information about an enforcement matter to any person outside the Commission, whether directly or indirectly. *See* 47 C.F.R. §§ 0.457, 0.459(d)(3), 19.735-203(a). Unauthorized disclosure of nonpublic information about enforcement matters subjects the Commission employee to possible disciplinary action pursuant to 47 C.F.R. § 19.735-107.

- c. Special care should be exercised when copies are made on shared printers and copying machines.
- d. 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 (ASC). Labeled cover sheets, which are also available from the ASC, may be placed on top of the document as a further precaution.
- e. Copies should never be left in unsecured In-Boxes or on unattended desks or chairs.
- f. For electronic dissemination, 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.
- g. Notwithstanding the Highly Sensitive/Restricted nature of all circulation and agenda enforcement cases, the Office of Inspector General may disclose information about an enforcement matter to another law enforcement agency as authorized by the Inspector General Act of 1978, as amended.

7. Training Program

Every new employee shall receive a brochure setting forth the policies in this directive during their new employee orientation.

8. Responsibilities

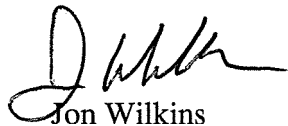
a. **Bureau and Office Chiefs (or their designees) shall:**

- (1) 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.
- (2) Take reasonable measures to ensure compliance with nonpublic information management controls set forth herein.
- (3) Categorize information into levels of protection noted above, and determine who within the organization should have access to Highly Sensitive/Restricted material.
- (4) Advise OMD if additional computer or other security resources are needed to maintain security for Highly Sensitive/Restricted information.
- (5) Refer as appropriate alleged unauthorized disclosure, loss or theft to the Inspector General.
- (6) Seek appropriate authorization pursuant to Section 19.735.203 of the Commission's rules prior to disclosure of nonpublic information when appropriate.

b. **The Managing Director shall:**

Establish and disseminate policies and procedures to protect nonpublic information and ensure those polices are coordinated with all the information policies noted in this directive.

Provide material necessary to the implementation of this policy (document disposal bins, stamps, templates, envelopes, cover sheets, etc.).


Jon Wilkins
Managing Director