NEW YORK STATE Corrections and Community Supervision **DIRECTIVE**	TITLE **Confidential Security Information**		NO. 0410 DATE 11/21/2019
SUPERSEDES DIR # 0410 Dtd. 12/13/16	DISTRIBUTION A B	PAGES PAGE 1 OF 2	DATE LAST REVISED
REFERENCES (Include but are not limited to) Public Officer's Law; 7NYCRR Part 51.1; ACA Expected Practices 4-APPFS-3D-28, 2-1079; Directive #2009, #2010, #2012 2012, #2111, and #2260, Employees' Manual; Health Services Policy Manual	APPROVING AUTHORITY 		

I. PURPOSE: This directive defines confidential security information, and is intended to enhance controls over unauthorized or unmindful disclosure of such information.

II. SCOPE: Confidential security information is handled and transmitted by employees throughout the typical work day. Employees become knowledgeable about institutional environments, individual incarcerated individuals or parolees, procedural details, and institutional and Departmental affairs in the performance of their assigned duties. Accordingly, this directive applies to all employees. This directive should not be construed to limit or interpret any other Departmental directives or regulations on Departmental information as identified below.

III. REFERENCES

Public Officer's Law, Section 74, states in relevant part "No officer ... should disclose confidential information acquired by him in the course of his official duties ..." This is restated in the Employees' Manual, Section 4.2, and summarized in Directive #2260, "New York State Ethics."

7NYCRR Part 51.1, "Divulgence of information," states in relevant part "Information relative to institutional or departmental affairs and individual inmates must be authorized and given out by the commissioner ... Inquiries ... shall not be answered by the employee but referred to the Superintendent."

Employees' Manual, Section 2.2 states in relevant part "An employee shall not knowingly or willingly violate any law ... of ... the State of New York or any rule, regulation, or directive of the Department."

Directive #2010, "FOIL/Access to Departmental Records," sets forth procedures and additional references for disclosure of information, including information subject to the Freedom of Information Law (FOIL).

Directive #2111, "Report of Employee Misconduct," sets forth the procedure for reporting employee misconduct and recommending disciplinary action.

IV. POLICY

A. Confidential Security Information: Is defined as any information which, if disclosed, could compromise the safety and security of incarcerated individuals, parolees, employees, or the public, or which would otherwise violate the Public Officers Law or Departmental regulations listed as references above.

Although this definition is broad, it must be generally considered that Department employees, like employees in many industries and military services, work in an environment and handle information that must not be discussed outside the workplace or communicated over non-secure media.

Accordingly, employees should be on guard in public to refrain from discussions of internal affairs and specific incarcerated individuals or parolees. This will minimize the risk of unintended disclosure of confidential security information.

Note: In accordance with Section 4.7 of the Employees' Manual, Department staff shall not have access to the personnel records of any other employee or to the case records of any incarcerated individual or parolee except as required in the discharge of his or her official duties. All employees shall take precautions to ensure that unauthorized persons do not have access to confidential material.

Requests for information should be handled by facility, regional office, and Department staff who have been specifically designated to process and fill such requests. Curious acquaintances and members of the public seeking information should not be given informal responses but should be directed to call a facility Superintendent, Regional Director, or Central Office, or to make a FOIL request.

Confidential security information includes, but is not limited to:

- Contents of "D" classification directives
- Contents of manuals or documentation which describe emergency or security procedures
- Descriptions of institutional environments
- Information about incarcerated individual moves
- Information about a parolee supervision

B. Note that information which may not be categorized as confidential security may be protected by the Privacy Act or regulations restricting dissemination of personal or criminal history information. See Directives #2009 through #2012, and the Health Services Policy Manual.

C. In addition to the risks of unintended disclosure of confidential security information from casual conversations in public places, all employees are reminded that cellular and cordless phones and computer on-line services use non-secure media which can be monitored or intercepted by outside parties.

D. Employees who have any questions about the interpretation or application of this directive or any referenced material should discuss them with supervisory or executive staff.

E. Employees responsible for unauthorized or unmindful disclosure of confidential security information may be subject to a report of misconduct and possible disciplinary action.