



DEPARTMENT MANUAL

Section 104.07

CHAPTER: Regulations			
SUBJECT: USE OF DEPARTMENT INFORMATION ASSETS			
ISSUE DATE: 5/2/2022	EFFECTIVE DATE: 5/2/2022	REVISES/SUPERSEDES: 11/29/2021 Issue	PAGE: 1 of 5

PURPOSE:

To regulate Employees' use of County or Department computer workstations, laptop computers, smart-phone devices, electronic mail ("e-mail"), databases, networks and connections (wired and wireless) to the County or other intranet, internet and any other information technology services available both now and in the future (hereinafter, "Information Assets").

POLICY:

Employees shall use Department Information Assets primarily for the purpose of accomplishing Westchester County and Department objectives and shall not compromise the integrity or security of either the data contained therein or the equipment itself.

PROCEDURE:

COUNTY INFORMATION ASSET USE POLICY

1. Employees shall comply with the County "Security and Technology Use Policy" governing the use of Information Assets.

SUPPLEMENTAL REGULATIONS

2. Employees shall report any problems with Information Assets assigned to or used by them to the Department of Information Technology ("DoIT"):
 - a. by e-mail to HelpDesk@westchestergov.com with a copy to their immediate Supervisors and to the Commanding Officer of the Information Technology Unit, or;
 - b. by telephone to the help desk at (914) 995-5513 and, in the event of any significant issue, with follow-up notice to their immediate Supervisors and to the Department of Commanding Officer of the Information Technology Unit.
3. If a reported problem is not corrected in a reasonable amount of time, Employees shall contact the Department of Information Technology to follow up and ensure that the problem will be resolved.
4. Employees shall not connect any personally owned computer equipment, software or data to County or Department owned Information Assets without the express permission of the Commanding Officer of the Information Technology Unit or the

SUBJECT: USE OF DEPARTMENT INFORMATION ASSETS		SECTION NO: 104.07	
ISSUE DATE: 5/2/2022	EFFECTIVE DATE: 5/2/2022	REVISES/SUPERSEDES: 11/29/2021 Issue	PAGE: 2 of 9

County Department of Information Technology, except that Employees may use personal devices to access the County's public networks and internet pages consistent with the rules and regulations governing same.

5. Unit Supervisors may create guidelines for their staff concerning reasonable incidental personal usage of County or Department computer systems or smart-phone devices which are no less restrictive than that which is provided for in the County Security and Technology Use Policy.
6. Employees are responsible for the security of County or Department Information Assets assigned to or used by them and shall take all reasonable precautions with respect to such equipment.

NOTE: Reasonable precautions include, but are not limited to, maintaining the privacy of their identification codes, accounts and passwords, logging off or locking Information Assets when not actually using them, closing any software when not actually using it, and maintaining reasonable physical security for any Information Assets.

7. Employees shall not use County or Department Information Assets to access, create, transmit or delete typed language, words, symbols or data consisting of jokes and pranks.
8. Employees shall not copy any data, information or software using County or Department Information Assets for other than archive or 'back up' purposes.
9. Employees shall not use County or Department Information Assets to solicit for personal purposes, for personal gain or for the advancement of political or religious beliefs.
10. Employees shall not use any law enforcement database (including any license plate reader database and any database accessed through a Division of Criminal Justice Services portal) or disclose any information obtained therefrom for other than law enforcement purposes or authorized background investigation, or in any manner which violates the user agreement governing access to such database.
11. Employees shall not violate the integrity or security of Department Information Assets through their use thereof, and shall:
 - a. change their passwords periodically, as directed, or immediately if the password may have been compromised;
 - b. keep their passwords confidential and secure at all times by not sharing their passwords with others and by not using any function of their computers that allow for saving their user names and passwords on a given workstation unless such workstation is dedicated to a single user within a private office;

SUBJECT: USE OF DEPARTMENT INFORMATION ASSETS		SECTION NO: 104.07	
ISSUE DATE: 5/2/2022	EFFECTIVE DATE: 5/2/2022	REVISES/SUPERSEDES: 11/29/2021 Issue	PAGE: 3 of 9

- c. not leave any Department Information Asset unattended when data is not secured by password or other means; and
 - d. report to the Commanding Officer of the Information Systems Unit (with notification to their own immediate Supervisors) any attempt, or suspected attempt, at unauthorized access into Department Information Assets.
12. All data accessed, created, transmitted, or deleted by employees using County or Department Information Assets may be considered public records, and Employees are required to follow the applicable records retention procedures for same, except as may otherwise be provide for herein.
13. Notification of violations:
- a. Employees who become aware of any violation of the laws, regulations or rules pertaining to the use of the Department Information Assets shall immediately notify their immediate Supervisors and the Commanding Officer of the Information Systems Unit of the facts, in writing.
 - b. If the Commanding Officer of the Information Systems Unit becomes aware of any violation of the laws, regulations or rules pertaining to the use of Department Information Assets, he or she shall immediately notify the violating Employee's Supervisor of the circumstances and take such other action as may be required by Department, County, Division of Criminal Justice Services and/or other applicable regulations.

CRIMINAL HISTORY RECORD INFORMATION

14. "Criminal History Record Information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release (the term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.)¹
15. Criminal History Record Information may be obtained by authorized Employees through the Division of Criminal Justice Services (DCJS) portal, eJusticeNY, however, these provisions shall pertain to Criminal History Record Information regardless of how it is accessed.
16. The Commissioner shall designate an Employee to act as the Department's Local Agency Security Officer (LASO) who shall:

¹ As provided in 28 CFR § 20.3 which is incorporated in the DCJS Use & Dissemination Agreement for Criminal History Record Information and federal Criminal Justice Information Services data files.

SUBJECT: USE OF DEPARTMENT INFORMATION ASSETS		SECTION NO: 104.07	
ISSUE DATE: 5/2/2022	EFFECTIVE DATE: 5/2/2022	REVISES/SUPERSEDES: 11/29/2021 Issue	PAGE: 4 of 9

- a. identify users of the DCJS - approved electronic systems and ensure no unauthorized individuals or processes have access to same;
 - b. identify and document how the Department equipment is connected to the state system;
 - c. ensure that personnel security screening procedures are being followed as stated in this policy.
 - d. ensure the approved and appropriate security measures are in place and working as expected; and
 - e. support policy compliance and ensure that the DCJS Director of Audit Services is promptly informed of security incidents.
17. The Commissioner shall designate one Employee to act as the Terminal Agency Coordinator (TAC) for each segment of the Department operating under its own DCJS Use and Dissemination Agreement who shall:
- a. be the point of contact for matters relating to Criminal History Record Information access;
 - b. administer Criminal History Record Information programs and oversee compliance with Criminal History Record Information systems policies;
 - c. maintain a complete, accurate, and current listing of all terminal operators and their user identifications together with copies of training and screening completion certificates;
 - d. notify DCJS when a user's access to Criminal History Record Information should be removed due to change in responsibilities or employment status or other reason; and
 - e. conduct periodic audits to ensure compliance with applicable regulations governing system use.
18. Sworn Members, Communications Operators, members of the Taxi & Limousine Commission designated by its Chairperson and other Employees as may be designated by the Commissioner are authorized to access Criminal History Record Information, provided that they have successfully completed such security screening procedures as may be required by DCJS.
19. Criminal History Record Information may be obtained only for the purposes permitted under the Use and Dissemination Agreement applicable to the Employee obtaining such information (see Appendix "A," attached).

SUBJECT: USE OF DEPARTMENT INFORMATION ASSETS		SECTION NO: 104.07	
ISSUE DATE: 5/2/2022	EFFECTIVE DATE: 5/2/2022	REVISES/SUPERSEDES: 11/29/2021 Issue	PAGE: 5 of 9

20. Notwithstanding any contrary directive, Criminal History Record Information may not be disclosed by any Employee to another agency or individual unless specifically authorized by law.
21. When Criminal History Record Information is being used solely for licensing or employment background investigation:
- a. the Criminal History Record Information shall be retained only for the duration of such investigation process, including any subsequent administrative or judicial appeal of denial of the license or employment and, thereafter destroyed in a secure manner to preclude unauthorized access or use;

NOTE: Pursuant to the above, Criminal History Record Information obtained for background investigation purposes shall be discarded by the Taxi & Limousine Commission, the Pistol Licensing Unit and Background Investigation Coordinator (relating to Department employment background investigations) within **five months** following an adverse determination.

- b. the Commanding Officer of each Unit which has requested to receive reports of subsequent arrests of individuals who are the subject of a Criminal History Record Information inquiry shall, at least once per year, provide to DCJS:
 - i. the names and NYSID numbers of individuals whose fingerprints were sent to DCJS for identification processing and retention, but whose applications were not approved for employment or licensure by the Department; and
 - ii. the names and NYSID numbers of individuals who subsequently left the Department's employment or relinquished licensure.

RELATED PROVISIONS:

104.01 General Rules of Conduct

**Appendix A
Authorized Inquiry Specification List**

Agency Name: Westchester County Department of Public Safety

ORI Number: NY0590000

On-Line Inquiry Reason Code	Purpose of Inquiries	Enabling Authority
ARR	Can only be used by Police Departments / Agencies, Sheriff's Offices, or District Attorney's when criminal history record information is needed during arrest processing. Should not be used in lieu of an available fingerprint-based rap sheet.	Executive Law §837(6)
CJE	Can only be used to make non-finger printable inquiries for perspective employees (including vendors/contractors involved with the administration of criminal justice for the criminal justice agency), not current employees or visitors. An applicant fingerprint submission will ensure a definitive criminal history for the employee as well as provide the agency with a hit notice if the individual is arrested for a finger printable offense in New York State.	28 CFR 20.33 FBI NCIC Operating Manual
CRI	Can only be used by Police Departments / Agencies, Sheriff's Offices, District Attorney's or interstate cooperation with law enforcement officers and agencies of other states and the federal government, to request criminal history record information of an individual currently under investigation for a crime/alleged crime.	Executive Law §837(6)
DET	Can only be used by Police Departments / Agencies, Sheriff's Offices or Correctional Facilities to perform inquiries when a person is being detained but is not a sentenced offender. This includes offenders who are held under securing orders, but not a commitment order.	Executive Law 837(6)
DNA	Can only be used by Police Departments / Agencies, Sheriff's Offices, probation, parole, DOCCS, OCFS facilities, district attorney offices, and courts to verify charge information for DNA eligibility.	Executive Law 837(6)
GUN	Can only be used by Police Departments / Agencies, Sheriff's Offices, and courts in connection with firearm releases, permits, or renewals.	Penal Law §400.00(9) and (10)

**Appendix A
Authorized Inquiry Specification List**

Agency Name: Westchester County Department of Public Safety

ORI Number: NY0590000

HOU	Can only be used by Police Departments / Agencies or Sheriff's Offices to conduct a name-based search for a qualified Public Housing Authority (PHA). The law enforcement agency may advise the PHA if there is a hit, but may not provide a rap sheet to the PHA. If the PHA wishes to pursue this, they should submit civil fingerprints to DCJS.	Housing Opportunity Program Extension Act of 1996; Public Law 104-120
PDI	Can only be used by Police Departments / Agencies, Sheriff's Offices to request criminal history record information of an individual currently under investigation for a crime/alleged crime.	Executive Law §837(6)
WAR	Can only be used by Police Departments / Agencies, Sheriff's Offices, District Attorneys or Courts for investigations involving the issuance of a warrant or an individual's warrant status.	Executive Law §837(6)
	ARREST Adult Arrest Fingerprint Submission	Criminal Procedural Law (CPL) 160.10(1)
	ARREST Juvenile Arrest Fingerprint Submission	Family Court Act §306.1
	CORRECTION ADMISSION Correction Admission Fingerprint Submission	Correction Law §618(2)
	DCJS CRIMINAL INQUIRY 52B – 15 Days or Less Non-Finger Printable Amnesia Victim County Incar. > 1 Year Not Cons. Detention Inquiry Fugitive Inv ID Only Investigative Fingerprints Non-Finger Printable Charge Turnover to another Agency Violation of Probation Warrant Invest - PD. Sex Offender Registry	Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) Executive Law 837(6) COR 6C SORA
	DCJS DEATH Death Fingerprint Card	Executive Law §837(6)

**Appendix A
Authorized Inquiry Specification List**

Agency Name: Westchester County Department of Public Safety

ORI Number: NY0590000

	<p>NON CRIM FINGERPRINT CARD Police Officer Applicant Fingerprint Submission* Peace Officer Applicant Fingerprint Submission* Park Ranger Applicant Fingerprint Submission* Deputy Sheriff Applicant Fingerprint Submission* Police Department Employee Applicant Fingerprint Submission* (NY State and Federal CHRI response)</p>	<p>CPL 1.20 CPL 2.10 CPL 2.10 CPL 1.20 Executive Law §837-c</p>
	<p>NON CRIM FINGERPRINT CARD Non-Criminal fingerprint submissions pertaining to contractors, vendors, custodial workers and other support personnel with unescorted access to physically secure locations or controlled areas * (NY State and Federal CHRI response)</p>	<p>CJIS Site Security 5.12</p>
	<p>NON CRIM FINGERPRINT CARD Pistol License Fingerprint Submission* (NY State and Federal CHRI response)</p>	<p>Penal Law §400.00(4)</p>

Remarks:

* Fingerprint processing fee required pursuant to Executive Law §837(8-a)

Agencies that are authorized to conduct a FBI fingerprint background check on an applicant (i.e. employment, license, permit, adoption) are obligated to ensure the applicant is provided certain notice. Refer to <https://www.fbi.gov/services/cjis/compact-council> for the following documents regarding the privacy protection of a non-criminal fingerprint submissions:

- Privacy Act Statement
- Guiding Principles: Agency Privacy Requirements for Noncriminal Justice Applicants
- Guiding Principles: Noncriminal Justice Applicants Privacy Rights

Appendix A

Authorized Inquiry Specification List

User Agency: Westchester County Taxi & Limousine Commission

ORI Number: NY059TL3Y

On-Line Inquiry Reason Code	Purpose of Inquiries	Enabling Authority
	NON CRIM FINGERPRINT CARD Non-criminal fingerprint submissions pertaining to the licensing of for-hire vehicles, drivers and base stations by Westchester County Taxi & Limousine Commission* (NY State CHRI response)	Westchester County Administrative Code Chapter 270 and Westchester County Local Law 9-1998
	NON CRIM FINGERPRINT CARD Non-criminal fingerprint submissions for employees who have access to NY State or Federal Criminal History Record Information (CHRI), whether hard copy or electronic form, in the course of their job duties* (NY State CHRI response)	9 NYCRR 6051.1(a)(3)

Remarks:

* Fingerprint processing fee required pursuant to Executive Law §837(8-a)

Agencies that are authorized to conduct a FBI fingerprint background check on an applicant (i.e. employment, license, permit, adoption) are obligated to ensure the applicant is provided certain notice. Refer to <https://www.fbi.gov/services/cjis/compact-council> for the following documents regarding the privacy protection of a non-criminal fingerprint submissions:

- Privacy Act Statement
- Guiding Principles: Agency Privacy Requirements for Noncriminal Justice Applicants
- Guiding Principles: Noncriminal Justice Applicants Privacy Rights