1.0 PURPOSE

To establish procedures for the control of access to, dissemination, and retention of National Crime Information Center (NCIC) and/or Interstate Identification Index (III) data which will ensure the security and integrity of that information within the Department.

2.0 SCOPE

This policy applies to all employees within the Department.

3.0 REFERENCES, DEFINITIONS & FORMS

.1 References

a. U.S. Department of Justice, Federal Bureau of Investigation, NCIC Security Policy.

b. Department Policy ADM.05.01, Access Control to Department Confidential Information.

.2 Definitions

a. Control Terminal Agency (CTA): This is represented by the Honolulu Police Department.

b. Authorized Personnel: An individual who does not have a Hawaii or national criminal record of any kind and has successfully completed a training course in computer accessing of NCIC information provided by the CTA.

c. Control Terminal Operator (CTO): This is the title of the individual who functions as the Department's liaison with the CTA.

4.0 POLICY

.1 To ensure compliance with security standards established by NCIC for the utilization of their information, a control system shall be established within the Department for the management of all computers, electronic switches,

and terminal devices interfaced directly with the NCIC computer for the access of III information.

.2 All departmental personnel who access NCIC information through a computer shall have their background investigated for a criminal history, and trained in system use, prior to authorization for utilization of the terminal. A criminal history check shall also be required of any personnel employed or utilized to effectuate access to or initiate transmission of NCIC information.

5.0 PROCEDURES

.1 Authorization for Terminal Use

Any organization within the Department that feels the need to install an NCIC access terminal must receive prior approval from their deputy director.

Prior to the use of any terminal accessing NCIC information, the user must pass a criminal history check and show successful completion of training in the use of the access equipment.

a. Application

An employee must apply for terminal use by completing a Fingerprint Report, Form DCR 0127 (Attachment A). The form is to be forwarded to the CTO for further processing.

b. Background Screening

The CTO shall be responsible for the following screening process:

1. Forward a completed applicant fingerprint card to the FBI Identification Division.

2. Conduct a Hawaii and national III record check by fingerprint identification on the applicant. This shall include local, state, and national arrest and fugitive files as well as former employer history.

3. If a criminal record of any kind is found, access to NCIC information shall be denied.

4. Complete forms DCR 0126 and 0127 (Attachment B) and forward them with a memo attached to the applicant's deputy director. Any pertinent investigative information shall also be attached. The memo shall recommend approval or disapproval based upon the data on Forms DCR 0126 and 0127.

c. Approval

1. Deputy Director

Upon receipt of a recommendation from the CTO concerning an applicant, the deputy director shall complete Part IV of form DCR 0127 with their signature indicating approval or disapproval and return the forms to the CTO.

2. CTO

Upon receipt of forms DCR 0126 and 0127 from the deputy director, the CTO shall:

a) Forward the forms to the Department's Personnel Management Office with instructions for filing the documents in the applicant's personnel file.

b) Notify the applicant's supervisor in writing of the results of the investigation.

c) Notify the CTA in writing if an applicant has been found to be a fugitive from justice or to have been convicted of a felony or serious misdemeanor.

d) For those applicants who have received approval, apply to the CTA for an access code by completing the Honolulu Police Department form for an addition to the security list (attachment C) and forward the form with completed copies of Department forms DCR 0126 and 0127 attached, to the CTA.

d. Training

The CTA shall conduct all necessary training for proper use of terminal equipment. Upon successful completion of the training course, the CTA will provide the applicant with documentation indicating satisfactory completion of the course.

The applicant shall forward a copy of this documentation through their supervisor, and the CTO to the Department Personnel Management Office with instructions for filing the document in their personnel file.

.2 Physical Security

a. Computer Site

1. All computers with the capability of accessing NCIC information shall be located in a room or area which can be locked. The room shall remain locked when not in use by authorized personnel. Only authorized personnel shall be allowed in the area.

2. The supervisor of the area shall establish a system for the issue and control of keys to the area so that only authorized personnel shall have access to the terminal site.

b. Visitors

All visitors to the site shall be accompanied by an authorized person at all times.

.3 Technical Security

a. Terminal Use

1. Operators shall use the terminal only for those purposes for which they are authorized.

2. The terminal shall be turned off when not in use. It shall never be left on for any length of time when the operator is not there.

b. Access (User Authentication)

Authentication is the security measure designed to verify the identity of the user and establish their eligibility to receive NCIC information.

Authentication procedures are outlined in the NCIC Operations Manual. Only authorized persons shall have access to this manual.

The CTO shall control the receipt of and distribution to all departmental terminal users of authentication procedures from the CTA.

c. Lodging

All NCIC transactions and III transactions (both criminal history inquiry and criminal record request) originating from terminal devices that access the NCIC through the State system shall be maintained on an automated log. The procedures for logging as outlined in the NCIC Operations Manual shall be followed.

.4 Dissemination and Retention of NCIC Information

The data stored in the NCIC is documented criminal justice information which must be protected to ensure correct, legal, and efficient dissemination and use. An individual receiving a request for criminal justice information shall be responsible for ensuring that the person requesting the information is authorized to receive the data.

a. Dissemination

Copies of III data obtained from terminal devices shall be classified as confidential and labeled accordingly when being forwarded to an individual requesting the information. A dissemination log shall be maintained by the transmitting authority. The safeguards for confidential information as outlined in Department policy ADM.05.01, Access Control to Department Confidential Information, shall be followed.

b. Retention

Records of III data shall be maintained in a secure area. The provisions of Department policy ADM.05.01 shall apply. Such storage of records

shall be maintained for extended periods only when the III records are key elements for the integrity/utility of the case files/criminal record files where they are retained.

c. Destruction

When retention of III records is no longer required, they shall be destroyed by shredding or other secure manner as to preclude unauthorized access or use.

.5 Entering Records by the Department

a. Data Entry

Any authorized user in the Department who enters records into the system shall perform a second-party check of the data to ensure that the entry is complete and accurate. This second-party check shall be entered into the computer as part of the record in accordance with procedures outlined in the NCIC Operations Manual.

b. Record Validation

The CTA shall be advised to transmit all validation requests to the CTO. The CTO shall be responsible for:

1. Coordinating the validation check within the Department.

2. Ensuring a thorough attempt has been made in checking all sources of additional data.

3. Completing the validation report and forwarding the report to the CTA within 3 weeks of the request.

.6 Audits

The Department's security system and operational procedures for handling and accessing NCIC information may be audited at any time by the CTA to ensure compliance with NCIC policy and regulations. In addition, NCIC staff may conduct an on-site audit to ensure compliance with their regulations.

Department employees shall cooperate fully with the auditors during these inspections. All recommendations made by the auditors shall be fully complied with.

.7 Policy Violations

The data stored in NCIC is sensitive and shall be treated accordingly. An unauthorized request, use, or receipt of NCIC material may result in criminal proceedings. An employee violating any provisions of this policy shall be disciplined in accordance with the employee's collective bargaining agreement and/or Title 14, State of Hawaii Personnel Administrative Rules.

6.0 CONTROLLING AUTHORITY

A Control Terminal Operator (CTO) position shall be established in the Inspections and Investigations Office (IIO) who shall be responsible for the management of all equipment accessing NCIC information. The management responsibilities of the CTO shall include:

.1 Setting access priorities when necessary.

.2 Ensuring all personnel who utilize terminals have passed a criminal history background check and are properly trained in system access prior to authorizing their use of the terminal.

.3 Ensuring all terminal users and sites comply with the security provisions of this policy.

.4 Developing policy and procedures as needed for the personnel selection, personnel supervision, and the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit III record information.

.5 Ensuring that a minimum number of terminals necessary to complete the work are employed throughout the Department.

.6 Conducting periodic site inspections (at least annually) for compliance with the provisions of this policy.

.7 Assist the CTA in training Department personnel in the proper procedures for accessing NCIC information.

.8 Function as the central authority for the Department is coordinating all departmental NCIC matters with the CTA.

APPROVAL RECOMMENDED:

JAN 0 1 2024

Deputy Director for Administration Date

APPROVAL RECOMMENDED:

JAN 0 1 2024

Deputy Director for Corrections Date

APPROVED:

JAN 0 1 2024

DIRECTOR Date

ATTACHMENT A

STATE OF HAWAII
DEPARTMENT OF PUBLIC SAFETY

FINGERPRINT REPORT

PART I - REQUEST FOR FINGERPRINTING
(To be completed by the applicant)

Date:_____

Applicant:_____ Security No.:_____
Last Name First Name Middle Initial

Date of Birth:_____ Place of Birth:_____ Sex:_____

Any Alias(es) /Former Name(s) :_____

Address:_____

Classification Title:_____ Department: PSD

****

PART II - FINGERPRINTING DATA
(To be completed by the fingerprinting officer and person to be employed)

[redacted]on Fingerprinted:_____
(Signature)

Fingerprinting officer:_____
(Signature)

Fingerprinting agency:_____ Date:_____

****

PART III - FILE SEARCH DATA
(To be completed by the Department of Public Safety IS Office)

Report: SEE ATTACHED

Date:_____ By:_____

****

PART IV - DETERMINATION OF SUITABILITY

Applicant named above is:

☐ Suitable ----- Appointment approved_____

☐ Unsuitable -- Appointment disapproved_____

[redacted]_____

Date:_____ By:_____

PSD 0127 (1/94)

ATTACHMENT B

STATE OF HAWAII
DEPARTMENT OF PUBLIC SAFETY

CONFIDENTIAL
(When completed)

PART I
CRIMINAL DATA CHECK
INTERNAL USE ONLY PSD - IS

NAME:_____ POSITION:_____ CASE NO:_____

NCIC CHECK RESULTS:

STATE CRIMINAL CHECK RESULTS:

HPD ACTIVITY:

NAME OF INVESTIGATOR:_____
Type or Print Last Name First Name Middle Initial

SIGNATURE OF INVESTIGATOR:_____

****

PART II
EMPLOYER INFORMATION

Employer Results:

Employer Results:

Employer Results:

Employer Results:

Employer Results:

INVESTIGATOR COMPLETING JOB INFORMATION:_____
(Signature)

(When using this form for background investigation results, please attach it to form PSD 0127.
Please explain all codes used in results section of this form.)

PSD 0126 (1/94)

NOT CONFIDENTIAL

ATTACHMENT C

TOP SECRET: Additions/Deletions/Changes to Agency Security List

From Agency:

Agency Signature: Date:

HPD/R&D Comp. Security Liaison: Date:

HPD/R&D RMS Security Liaison: RCD ☐ Out ☐

ADDITIONS: Name (Last, First, M.I.) and Position Title/Rank	Profile Description (Give name and ACID of person with similar access)	Effective Date

DELETIONS: Name	ACID	Effective Date

CHANGES: ACID	Original Name	Changed Name	New Profile	Effective Date

Request Completed:

_____

DDS Authorized Signature Date

LE/3125, SA/3667, GY/3754
(R&D) I: TSADCAGC.SAD (REV 1/27/93)

NOT CONFIDENTIAL