N-DEx System User Participation Requirements Checklist

V1.0

Policy Requirements

The Federal Bureau of Investigation's (FBI's) *Criminal Justice Information Services (CJIS) Security Policy v5.6* and the *National Data Exchange (N-DEx) Policy and Operating Manual v4.0* are the referencing documents for all policy and security requirements for N-DEx System Participation. Policy requirements for N-DEx System participation may be stricter; however, at a minimum, adherence to all CJIS policy and security requirements, as defined in the *CJIS Security Policy v5.6* and the *N-DEx Policy and Operating Manual v4.0*, are necessary.

1. CJIS SECURITY POLICY v5.6

The *CJIS Security Policy v5.6*[1] provides Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to any FBI CJIS Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

> ***Section 5: POLICY AND IMPLEMENTATION***
> *The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.*
>
> *While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.*
>
> *Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:*
>
> ***5.1 Policy Area 1: Information Exchange Agreements***
>
> ***5.2 Policy Area 2: Security Awareness Training***
>
> ***5.3 Policy Area 3: Incident Response***
>
> ***5.4 Policy Area 4: Auditing and Accountability***
>
> ***5.5 Policy Area 5: Access Control***
>
> ***5.6 Policy Area 6: Identification and Authentication***
>
> ***5.7 Policy Area 7: Configuration Management***
>
> ***5.8 Policy Area 8: Media Protection***
>
> ***5.9 Policy Area 9: Physical Protection***

[1] <https://www.fbi.gov/file-repository/cjis-security-policy-v5_6_20170605.pdf/view>

5.10 Policy Area 10: System and Communications Protection and Information Integrity

5.11 Policy Area 11: Formal Audits

5.12 Policy Area 12: Personnel Security

5.13 Policy Area 13: Mobile Devices

2. N-DEx POLICY AND OPERATING MANUAL v4.0

Scope of N-DEx System policy: *The N-DEx Policy and Operating Manual v4.0*[2] *applies to all entities accessing data via N-DEx (i.e. both warehoused data and federated data sources). N-DEx information shall be used only for the purpose indicated by the Use Code and used consistently with the coordination required by the Advanced Permission Requirement (confirming the terms of N-DEx information use). Any subsequent use of N-DEx information inconsistent with the original Use Code or the previously conducted Advanced Permission Requirement requires re-satisfaction of the Advanced Permission Requirement.*

1.2 Operational Framework

- *1.2.2 Participating agencies and users must adhere to the CJIS Security Policy.*
- *1.2.6 N-DEx will not contain criminal intelligence data as defined by Title 28, Code of Federal Regulations (C.F.R.), Part 23.*

1.3 Data Use

- *1.3.6 Use Code Requirement: The FBI's CJIS Division is required to maintain an audit trail of each search request and returned result of N-DEx data. Therefore, every N-DEx search request must include a Use Code identifying why the search was performed.*
  - *The following Use Codes are considered acceptable when searching N-DEx:*
    - *1.3.6.1 Administrative Use Code "A": Must be used when N-DEx is utilized by a record-owning agency or submitter/aggregator to retrieve and display N-DEx contributed records in association with performing the agency's data administration/management duty. Responses for this purpose shall not be disseminated for any other reason and are limited to the record-owning agency portion of N-DEx records.*
    - *1.3.6.2 Criminal Justice Use Code "C": Must be used when N-DEx is utilized for official duties in connection with the administration of criminal justice as the term is defined in 28 Code of Federal Regulations (CFR) § 20.3 (2011).*
    - *1.3.6.3 Criminal Justice Employment Use Code "J": Must be used when N-DEx is utilized to conduct criminal justice employment background checks.*
      In order to use N-DEx to conduct criminal justice employment background checks, the agency must adhere to the following notice and consent, redress and audit requirements. (See N-DEx Policy Manual for additional Requirements.)
- *1.3.7 Search Reason Requirement: While the Use Code provides some lead information, it only provides a minimal audit trail. Therefore, all N-DEx users are required to provide the reason for every search request. This will ensure N-DEx searches are conducted for authorized uses and Use Codes are correctly applied. The Search reason shall include information, (such as, but not limited to, incident number, arrest transaction number, booking number, project name, routine activity description, and January 26, 2016 Page 12 if applicable the individual recipient/agency the search was made "on behalf of", etc.), to assist the user in accounting for appropriate system*

[2] <https://www.fbi.gov/file-repository/policy-and-operating-manual.pdf/view>

use for each transaction. Interstate Identification Index searches via N-DEx shall clearly identify the individual recipient/agency the search was made "on behalf of." The identification shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one-year retention period.

- *1.3.9 Advanced Permission Requirement: Terms of N-DEx information use must be obtained from the record-owning agency prior to reliance or action upon, or secondary dissemination. N-DEx information may only be relied or acted upon, or secondarily disseminated within the limitations specified by the record-owning agency. Reliance or action upon, or secondary dissemination of N-DEx information beyond the original terms requires further permission from the record owning agency.*
- *1.3.10 Verification Requirement: N-DEx information must be verified with the record-owning agency for completeness, timeliness, accuracy, and relevancy prior to reliance upon, action, or secondary dissemination.*

2.2 Security

- *2.2.1 Security standards are documented in the CJIS Security Policy v5.6.*

3. N-DEx DATA ACCESS AGREEMENT REQUIREMENT

The N-DEx Data Access Agreement fulfills the N-DEx Policy and Operating Manual policy section 2.4.2, requiring the following of the CJIS Systems Agency (CSA): *Prior to searching data via N-DEx, CSAs shall ensure, directly or through local delegation, that users are trained on N-DEx policy matters, emphasizing data use rules.*

The N-DEx Program Office implemented the N-DEx Data Access Agreement, which requires users to review, provide confirmation, and authenticate they comprehend the policies and rules required prior to searching data via the N-DEx System. This Data Access Agreement must be implemented for both user access methods - the N-DEx Portal and web service. The agreement shall contain language derived from the CJIS Security Policy and N-DEx Policy and Operating Manual, emphasizing data use rules. The N-DEx Data Access Agreement assures CJIS Systems Officers (CSOs) and regional system managers of users' comprehension of N-DEx System Policy.

The agreement screen, see Figure 1, appears within the N-DEx System portal on a yearly basis, when the user first logs into the N-DEx System. The affirmation of this agreement ensures system users are aware and agree to current policy matters. Additionally, the implementation requires the user to confirm, via check boxes, and authenticate, by clicking the "I AFFIRM" button, their understanding, and acceptance of the policies contained within the N-DEx Data Access Agreement. Upon user affirmation within the N-DEx System, the system captures the date within the N-DEx Training Management functionality listed under the N-DEx Data Access Agreement course. The CSO or Training Administrator may review which users have agreed to the N-DEx Data Access Agreement by accessing the "User Training Report."

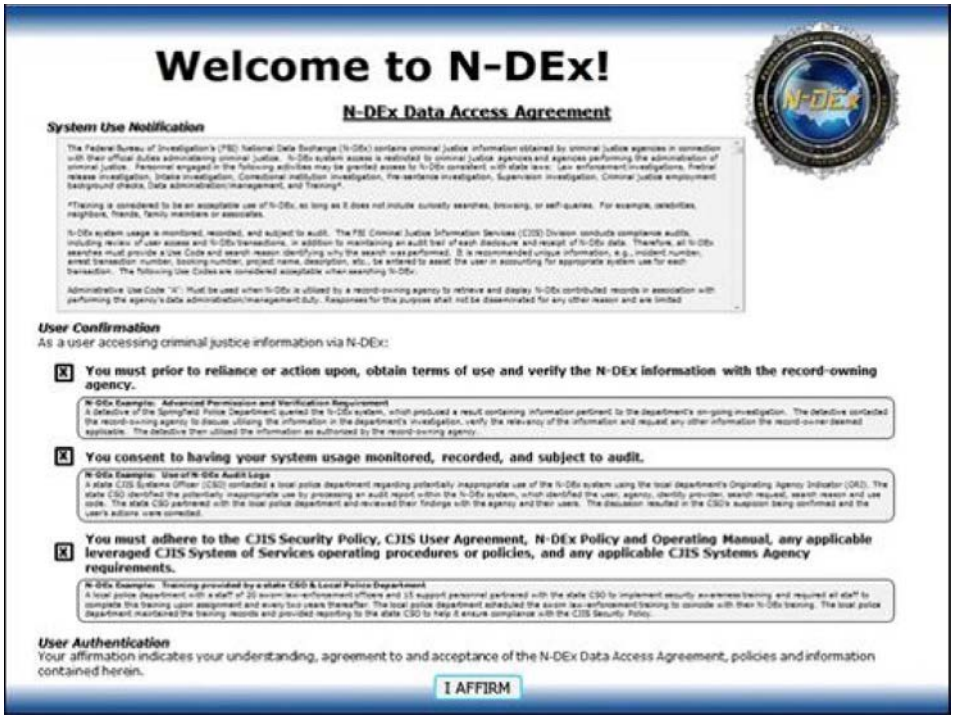

Figure 1 - N-DEx Data Access Agreement Screen

The N-DEx Program Office provides the same language and collaborates with the systems having a web service connection to the N-DEx System to ensure they implement this agreement and appropriately capture their users' affirmation.

The agreement language is provided below:

N-DEx Data Access Agreement

System Use Notification

The Federal Bureau of Investigation's (FBI) National Data Exchange (N-DEx) contains criminal justice information obtained by criminal justice agencies in connection with their official duties administering criminal justice. N-DEx System access is restricted to criminal justice agencies and agencies performing the administration of criminal justice. Personnel engaged in the following activities may be granted access to N-DEx consistent with state laws: Law enforcement investigations, Pretrial release investigation, Intake investigation, Correctional institution investigation, Pre-sentence investigation, Supervision investigation, Criminal justice employment background checks, Data administration/management, and Training.*

**Training is considered to be an acceptable use of N-DEx, so long as it does not include curiosity searches, browsing, or self-queries. For example, celebrities, neighbors, friends, family members or associates.*

N-DEx System usage is monitored, recorded, and subject to audit. The FBI Criminal Justice Information Services (CJIS) Division conducts compliance audits, including review of user access and N-DEx transactions, in addition to maintaining an audit trail of each disclosure and receipt of N-DEx data. Therefore, all N-DEx searches must provide a Use Code and search reason identifying why the search was performed. It is recommended unique information, e.g., incident number, arrest transaction number, booking number, project name, description, etc., be entered to assist the user in accounting for appropriate

system use for each transaction. The following Use Codes are considered acceptable when searching N-DEx:

- *Administrative Use Code "A": Must be used when N-DEx is utilized by a record-owning agency to retrieve and display N-DEx contributed records in association with performing the agency's data administration/management duty. Responses for this purpose shall not be disseminated for any other reason and are limited to the record-owning agency portion of N-DEx records.*

- *Criminal Justice Use Code "C": Must be used when N-DEx is utilized for official duties in connection with the administration of criminal justice as the term is defined in 28 Code of Federal Regulations (CFR) § 20.3 (2011).*

- *Criminal Justice Employment Use Code "J": Must be used when N-DEx is utilized to conduct criminal justice employment background checks or the screening of employees of other agencies over which the criminal justice agency maintains management control. See the N-DEx Policy and Operating Manual for additional requirements regarding Use Code "J."*

Prior to reliance or action upon, or secondary dissemination, a user must obtain terms of use and verify the completeness, timeliness, accuracy, and relevancy of N-DEx information with the record-owning agency. "Reliance upon" or "action upon" specifically includes the use or inclusion in the publication or preparation of charts, presentations, official files, analytical products, or other documentation, to include, use in the judicial, legal, administrative, or other criminal justice process, etc. Unauthorized use of the system and its data is prohibited and may be subject to criminal and/or civil penalties

User Confirmation
As a user accessing criminal justice information via N-DEx:

✓ ***You must prior to reliance or action upon, obtain terms of use and verify the N-DEx information with the record-owning agency.***

N-DEx Example: Advanced Permission and Verification Requirement
A detective queried the N-DEx System, which produced a result containing information pertinent to the department's on-going investigation. The detective contacted the record-owning agency to discuss utilizing the information in the department's investigation, verify the relevancy of the information, and request any other information the record-owner deemed applicable. The detective then utilized the information as authorized by the record-owning agency.

✓ ***You consent to having your system usage monitored, recorded, and subject to audit.***

N-DEx Example: Use of N-DEx Audit Logs
A state CJIS Systems Officer (CSO) contacted a local police department regarding potentially inappropriate use of the N-DEx System using the local department's Originating Agency Indicator (ORI). The state CSO identified the potentially inappropriate use by processing an audit report within the N-DEx System, which identified the user, agency, identity provider, search request, search reason and use code. The state CSO partnered with the local police department and reviewed their findings with the agency and their users. The discussion resulted in the CSO's suspicion being confirmed and the user's actions were corrected.

✓ ***You must adhere to the CJIS Security Policy, CJIS User Agreement, N-DEx Policy and Operating Manual, any applicable leveraged CJIS System of Services operating procedures or policies, and any applicable CJIS Systems Agency requirements.***

N-DEx Example: Training provided by a state CSO & Local Police Department
A local police department with a staff of 20 sworn law-enforcement officers and 15 support personnel partnered with the state CSO to implement security awareness training and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their N-DEx training. The local police department maintained the training records and provided reporting to the state CSO to help it ensure compliance with the CJIS Security Policy.

User Authentication

Your affirmation indicates your understanding, agreement to and acceptance of the N-DEx Data Access Agreement, policies, and information contained herein.

I AFFIRM

4. User Assertion Requirements
When searching and retrieving data from the N-DEx System, the partner system must provide the following identification (ID) information in the user assertion:

- Identity Provider ID
- User ID
- Last Name
- First Name
- Employer ORI

In addition, the partner system must provide the use code of the request and search reason in each search and retrieval request message sent to the N-DEx System. An example is provided below:

```
<lexs:DomainAttribute>
        <lexs:AttributeName>SearchReason</lexs:AttributeName>
        <lexs:AttributeValue>test</lexs:AttributeValue>
        <lexs:Domain>N-DEx</lexs:Domain>
    </lexs:DomainAttribute>

    <lexs:DomainAttribute>
        <lexs:AttributeName>PurposeCode</lexs:AttributeName>
        <lexs:AttributeValue>C</lexs:AttributeValue>
        <lexs:Domain>N-DEx</lexs:Domain>
    </lexs:DomainAttribute>
```