Policy Name:	Identification and Authentication
Policy Number:	36
Agency Name:	Westbrook Police Department
Effective Date:	08/11/2026
Revision Date:	
FBI CJIS Security Policy Section:	5.6 Identification and Authentication (IA)

PURPOSE:

To ensure that only properly identified and authenticated users and devices are granted access to Information Technology (IT) resources in compliance with IT security policies, standards, and procedures.

POLICY:

This policy is applicable to all departments and users of IT resources and assets of **Westbrook Police Department**.

1. IDENTIFICATION AND AUTHENTICATION
   Westbrook Police Department shall:

   a. Uniquely identify and authenticate **Westbrook Police Department** users and associate that unique identification with processes acting on behalf of **Westbrook Police Department** users.

   b. Implement multifactor authentication for network access to privileged accounts.

   c. Implement multifactor authentication for network access to non-privileged accounts.

   d. Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

   e. Accept and electronically verify Personal Identity Verification (PIV) credentials.

2. DEVICE IDENTIFICATION AND AUTHENTICATION
   Westbrook Police Department shall:

   a. Uniquely identify and authenticate **Westbrook Police Department**-managed devices before establishing network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset.

3. IDENTIFIER MANAGEMENT
   Westbrook Police Department shall manage system identifiers by:

a. Receiving authorization from **Westbrook Police Department** personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier.

b. Selecting an identifier that identifies an individual, group, role, service, or device.

c. Assigning the identifier to the intended individual, group, role, service, or device.

d. Preventing reuse of identifiers for one year.

e. Manage individual identifiers by uniquely identifying each individual as agency or nonagency.

4. AUTHENTICATOR MANAGEMENT
Westbrook Police Department shall manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator.

b. Establishing initial authenticator content for authenticators defined by **Westbrook Police Department**.

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use.

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

e. Changing default authenticators prior to first use.

f. Change/refresh authenticators annually or when there is evidence of authenticator compromise.

g. Protecting authenticator content from unauthorized disclosure and modification.

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators.

i. Changing authenticators for group/role accounts when membership to those account changes.

j. AAL2 Specific Requirements.

k. Ensure authentication occurs by the use of either a multi-factor authenticator or a combination of two single-factor authenticators:

l. If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator.

m. Cryptographic authenticators used at AAL2 SHALL use approved cryptography.

n. At least one authenticator used at AAL2 SHALL be replay resistant.

o. Communication between the claimant and verifier SHALL be via an authenticated protected channel.

p. Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.

q. Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.

r. If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.

s. If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be met.

t. Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.

u. Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.

v. The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJISSECPOL.

w. The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.

x. If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.

y. Memorized Secret Authenticators and Verifiers:

    a. Maintain a list of commonly-used, expected, or compromised passwords and update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly.
    b. Require immediate selection of a new password upon account recovery.

c. Allow user selection of long passwords and passphrases, including spaces and all printable characters.
d. Employ automated tools to assist the user in selecting strong password authenticators.
e. Enforce the following composition and complexity rules when agencies elect to follow basic password standards:
    i. Not be a proper name.
    ii. Not be the same as the Userid.
    iii. Expire within a maximum of 90 calendar days.
    iv. Not be identical to the previous ten (10) passwords.
    v. Not be displayed when entered.
f. If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.
g. If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.
h. Truncation of the secret SHALL NOT be performed.
i. Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.
j. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.
k. When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly used, expected, or compromised.
l. If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret.
m. If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.
n. If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.
o. Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.
p. Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.
q. The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
r. The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
s. Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.
t. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.
u. The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.
v. Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator.

w. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length.
x. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.
y. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets.

z. Look-Up Secret Authenticators and Verifiers:
    a. CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.
    b. Look-up secrets SHALL have at least 20 bits of entropy.
    c. If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 'n' 17 through 25.
    d. Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.
    e. A given secret from an authenticator SHALL be used successfully only once.
    f. If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.
    g. Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.
    h. If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function.
    i. If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.
    j. If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.
    k. If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret.
    l. If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.
    m. The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.
    n. The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

aa. Out-of-Band Authenticators and Verifiers:
    a. The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.
    b. Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).
    c. Methods that do not prove possession of a specific device, such as voice-over-IP (VoIP) or email, SHALL NOT be used for out-of-band authentication.
    d. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.

e. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.
f. If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).
g. If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.
h. If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.
i. The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.
j. Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.
k. If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.
l. If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator.
m. If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.
n. The authentication SHALL be considered invalid if not completed within 10 minutes.
o. Verifiers SHALL accept a given authentication secret only once during the validity period.
p. The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.
q. The verifier SHALL generate random authentication secrets using an approved random bit generator.
r. If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

s. If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.
t. If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25).
u. If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.
v. If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.
w. If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.
x. If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.

bb. OTP Authenticators and Verifiers:
a. The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.
b. The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.
c. OTP authenticators — particularly software-based OTP generators —SHALL NOT facilitate the cloning of the secret key onto multiple devices.
d. The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.
e. If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes.
f. The OTP value associated with a given nonce SHALL be accepted only once.
g. The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.
h. If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.
i. The verifier SHALL use approved encryption when collecting the OTP.
j. The verifier SHALL use an authenticated protected channel when collecting the OTP.
k. If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.
l. Verifiers SHALL accept a given time-based OTP only once during the validity period.
m. If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

n. If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.
o. If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a).
p. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).
q. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.
r. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.
s. If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.
t. In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13).

cc. Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based):
a. If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.
b. If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.
c. If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices.
d. If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).
e. If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.
f. If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.
g. If the authenticator is hardware-based, approved cryptography SHALL be used.
h. Cryptographic keys stored by the verifier SHALL be protected against modification.
i. If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.
j. The challenge nonce SHALL be at least 64 bits in length.
k. The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).
l. The verification operation SHALL use approved cryptography.
m. If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.
n. If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6

decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a).

o. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).

p. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.

q. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.

5. AUTHENTICATOR FEEDBACK
Westbrook Police Department shall:

a. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

6. CRYPTOGRAPHIC MODULE AUTHENTICATION
Westbrook Police Department shall:

a. Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

7. IDENTIFICATION AND AUTHENTICATION
Westbrook Police Department shall:

a. Uniquely identify and authenticate non-**Westbrook Police Department** users or processes acting on behalf of non-**Westbrook Police Department** users.

b. Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies.

c. Accept only external authenticators that are NIST-compliant; and document and maintain a list of accepted external authenticators.

d. Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect.

8. RE-AUTHENTICATION
Westbrook Police Department shall:

a. Require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours.

9. RE-AUTHENTICATION
Westbrook Police Department shall:

a. Identify proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.

b. Resolve user identities to a unique individual.

c. Collect, validate, and verify identity evidence.

d. Require evidence of individual identification be presented to the registration authority.

e. Require that the presented identity evidence be validated and verified through agency-defined resolution, validation, and verification methods.

ROLES AND RESPONSIBLITIES:
Local Agency Security Officer: Ensure that policies and procedures required by the FBI CJIS Security Policy are developed and maintained. Ensure that policies and procedures are disseminated and operationalized.

Westbrook Police Department Information Technology Staff: Develop, document, and disseminate to: to authorized personnel:

Agency-level identification and authentication policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls.

Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures.

Review and update the current identification and authentication:

1. Policy annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI; and
2. Procedures annually and following any physical, environmental, or security related incidents involving CJI or systems used to process, store, or transmit CJI.

Westbrook Police Department Personnel: All **Westbrook Police Department** personnel will understand what constitutes identification and authentication.

COMPLIANCE:

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

REFERENCE:

National Institute of Standards and Technology (NIST)

_____

CLEO or Agency Director

Date Issued:	08/11/2026
Date Reviewed:	08/11/2026