From: Violeta Navarro

To: All ACCESS Users

Date: October 27, 2022

Subject: New Template Procedure - CJIS User Account Validation Policy

Hello,

As stated in a previous email we have added a new CJIS User Account Validation Policy template procedure to our ACCESS Webpage. This procedure requirement is *not* new to the CJISSECPOL however when the FBI audited our state over the summer our state was found out of compliance. As a result, the WSP will start auditing for this procedure starting in January 2023 during our technical security audits.

Below is information from the email sent on 9-9-2022.

3. **Identification/User ID**: Ensure all account management, identification policies, and procedures are implemented on system accounts accessing CJI. (*This was a finding during the previous cycle.*)
    a. Refer to CJIS Security Policy 5.5.1 – Account Management
    b. A procedure is required. A template is available on the FBI website (coming soon to the ACCESS webpage)
    c. We will start reviewing this procedure during our IT audits starting in 2023

Below is the requirement from the CJISSECPOL. The FBI requires validation of accounts at least annually.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJI.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

If you have any questions please let me know.

Thanks,

Violeta Navarro
Information Security Officer
ACCESS Section
Washington State Patrol
Office: 360-534-2161 VoIP: 16161
Mobile: 360-485-9807
ACCESS Webpage