CHAPTER 7

INFORMATION SYSTEMS ACCOUNT MANAGEMENT POLICY

REVISED OCTOBER 2025

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 7

INFORMATION SYSTEMS ACCOUNT MANAGEMENT POLICY

1. PURPOSE. The purpose of this policy is to establish a standard for the administration of information system accounts that facilitate access or changes to CHP data. An account, at minimum, consists of a user ID and a password. Supplying account information will usually grant access to some set of services and resources.

2. SCOPE. This policy is applicable to those responsible for the management of user accounts and account holders with access to shared information or access to network devices. Such information can be held within a database, application, network configuration file, or network file space. This policy applies to all departmental information system accounts.

3. POLICY.

a. Accountability. The Department shall control and maintain individual employee and/or nondepartmental user account access to CHP computer/information systems resources through the assignment of rights and/or permissions for each of the Department's computer and information system resources.

b. Authentication. Authentication is the process of verifying the identity of the user utilizing controlled information. Users are identified and authenticated by establishing what they know, such as their user ID and password; what they have, such as a CHP network asset; and, in some cases, what they are, such as biometrics (e.g., physical, behavioral, and cognitive).

c. The Department requires users to be properly identified and authenticated before being allowed to access information systems. Verifying the identity of users is critical to ensure authorized access to system resources and establish accountability. Identification, such as a user's ID, distinguishes one user from another on the network.

d. Commanders' Responsibility. Commanders shall ensure:

(1) Access requested is commensurate with each employee's job duties and responsibilities, and a CHP 101, Appropriate Use of Automated Information & Systems Statement, is completed and approved as required (refer to Chapter 2, General Network Security and Administration, paragraph 2., of this manual).

(a) User Transfer. If there is a business requirement to transfer a user, a commander, or their designee, shall create an Account Management Request in ServiceNow (https://chp.service-now.com/esc) to change the account location and the user's access.

(b) Transfer Ownership of Files. If there is a business requirement to transfer ownership of files, a commander, or their designee, shall create an Incident Request in ServiceNow (https://chp.service-now.com/esc) to have all essential data transferred prior to the user's account being transferred or deleted.

(2) Account access is discontinued when no longer warranted.

e. Employee and/or Nondepartmental User Responsibility. All CHP employees and/or nondepartmental users who have computer and/or network access are responsible for protecting the Department's IT assets. This includes ensuring the security and privacy of individual records and record subjects. Employees who are granted administrative access rights shall be aware those privileges come with the additional responsibility of ensuring the information is accessed and/or viewed only by individuals with both a right to know and a need to know. Misuse of computing, networking, or automated information resources may result in loss of computing privileges and may be cause for disciplinary action and/or prosecution under applicable state or federal statutes.

4. ACCOUNT ISSUANCE.

a. Network Access Account. Upon receipt of an approved Access Request Form via ServiceNow, Technology Infrastructure Section (TIS) shall issue an individual unique account to each person authorized to have access to the CHP network and/or information resource(s).

(1) Basic User Network Account. Each employee utilizing CHP technology equipment to perform their job functions will be issued one basic network account. This account will include access to a personal drive, Department and command shared drives, e-mail, and basic Internet access.

(a) Commanders or their designees shall ensure the appropriate Access Request Form is submitted via ServiceNow for each employee with authorized access to appropriate computer software and information systems resources commensurate with each employee's job duties and responsibilities. Requests to copy another user's profile will be denied.

(2) Administrative Network Account. If a user requires administrative permissions to perform their duties, a separate administrative account will be issued for those purposes only. No account with elevated permissions shall be used to perform routine network access or activities not requiring such permissions. For security purposes, the administrative network account will not have access to the Internet or e-mail resources.

(a) Supervisors shall ensure the completion of the appropriate Access Request Form in ServiceNow for each employee with authorized access to appropriate computer and information systems resources commensurate with each employee's job duties and responsibilities.

(b) When establishing accounts, standard security principles of "least required access" to perform a function shall be followed. An administrative network account shall not be issued when a basic user network account is sufficient.

(3) Application and/or Resource Account. The command or Office of Primary Interest (OPI) responsible for an application and/or resource (e.g., Project Tracking Log, Allocated Resources Management System, and Capitol Garage Access System) shall issue a unique account to each person authorized to access the application and/or resource.

(a) Depending on the application and/or resource access required, supervisors shall ensure the completion and submission of the appropriate Access Request Form in ServiceNow for authorizing access to appropriate computer and information systems resources commensurate with each employee's job duties and responsibilities.

(4) E-Mail Account. Each permanent employee (uniformed and nonuniformed) will be issued a Department e-mail account. Nondepartmental employees will not be issued an e-mail account unless justified through the chain of command and approved by the Information Security Officer (ISO).

5. MANAGING ACCOUNTS. Account audits, reviews, and change notifications shall be performed quarterly to ensure access and account privileges are commensurate with job function, need to know, and employment status.

a. Mandatory Network Account Audits. On a quarterly basis, audits will be performed on randomly selected commands and Departmentwide stale network accounts. Commands who received a network account audit and/or stale account notification shall submit their response(s) to the ISO by the date established within the communication received.

b. Command-Initiated Account Review. A command or OPI may initiate an account review by submitting a request through the chain of command to the ISO for a list of users with access to their network command files and system access and/or privileges. Commands who have requested an account review shall submit their response(s) to the ISO by the date established within the communication received.

c. Network Account Access Change Notification. Commanders or their designees are responsible for immediate notification to the IT Support Unit, by submitting an Account Management Form in ServiceNow, to disable/revoke any computer or information system access upon a user's separation from the Department or when continued access is no longer required.

d. Application and/or Resource Account Access Change Notification. The command or OPI responsible for an application and/or resource is accountable for the prompt deactivation of accounts upon command notification of a user's separation from the Department or when continued access is no longer required. This includes accounts of transferred individuals to ensure changes in access privileges are appropriate for the change in job function or location.

6. PROCEDURES.

a. Information Technology Request. The appropriate Access Request Form in ServiceNow shall be used to request access for all employee and/or nondepartmental user accounts for computer and information systems resources and account access privileges.

(1) Information technology requests not requiring Information Technology Section (ITS), TIS, Information Management Division (IMD), or ISO approval should be submitted using the appropriate Access Request Form in ServiceNow. This includes, but is not limited to, the following requests to access:

(a) Computer Aided Dispatch.

(b) Web Access (e.g., e-mail).

(c) Allocated Resource Management System.

(d) Departmental standard and custom applications (e.g., Statewide Automated Citation System, Project Tracking Log, Statewide Integrated Traffic Records Management, and Microsoft Office Suite products).

(2) Information technology requests requiring ITS, TIS, IMD, and/or ISO approval should be submitted using the appropriate Access Request Form in ServiceNow. This includes, but is not limited to, the following requests to access:

(a) Nonstandard software (purchased or open source).

(b) Specialized or enhanced Internet.

(c) Computer, network, or Database Administrator privileges and/or rights.

(d) Virtual Private Network.

b. Frequency.

(1) The appropriate Access Request Form in ServiceNow shall be completed when:

(a) Establishing individual network accounts, permissions, and/or application and/or resource access for employee and/or nondepartmental users.

(b) A change is required for individual network accounts, permissions, and application and/or resource access of employee and/or nondepartmental users.

1 All established rights and permissions extended to an employee and/or nondepartmental user account shall be removed if the account is transferred to another command. Each employee shall submit a new request upon transfer to a new command commensurate with the change in job duties and responsibilities

c. Retention.

(1) All employee IT requests are maintained within ServiceNow.

(2) Sponsoring commands shall be responsible for maintaining an appropriate file for nondepartmental users. All nondepartmental user IT requests are maintained within ServiceNow.

d. Fingerprinting and Background Check. Employees and nondepartmental users shall not be granted access to confidential and/or sensitive information prior to the completion of fingerprinting and a background check consistent with the required level of access.

e. Additional Departmental Forms. Depending on the application and/or resource access being requested, the command or OPI may require additional departmental form(s).

7. DEFINITIONS AND TERMS.

a. Account. A series of rights or permissions granted to an individual which permits access to a network and/or information system.

b. Computer and Information System Resources. Computer or computing system and/or application used by users to complete job-related tasks efficiently.

c. Nondepartmental User. A contractor, consultant, Explorer, retired annuitant, senior volunteer, student assistant, or any individual not under the direct employment of the CHP.