
Alameda-Contra Costa Transit District

Administrative Regulation No. 440B: Information Security

Issuing Officer: General Manager
Date of Adoption: 3/22/17
Most Recent Amendment: 2/1/2023
See Also: 217, 440, 440A, 440C, 440D

Subject Category: Section 400, Operations
Subsection: Information Systems
Control Department(s): Innovation and Technology

I. PURPOSE

The purpose of this regulation is to communicate the guidelines for properly safeguarding District information stored on electronic computer systems.

II. PERSONS AFFECTED

All users of the District's computers or network infrastructure.

III. DEFINITIONS

"Physical theft" Theft of a laptop, phone, CD, DVD, flash drive, or any other item.

"Sensitive Information" includes all data, in its original and duplicate form, which contains personal information, passwords, protected health information, customer record information, cardholder data, confidential personal data, pending litigation, matters addressed in Closed Session by the Board of Directors, or information that is deemed to be confidential or is otherwise exempt from disclosure under state law.

"Unauthorized Disclosure" means the intentional or unintentional revealing of sensitive information to people, whether inside or outside of AC Transit, who do not have a need to know that information.

"User" is anyone using District computing resources including but not limited to employees, contractors, consultants, limited-term employees, interns, Board Officers and Board Members.

IV. REGULATION

A. General

1. All users have a responsibility to safeguard AC Transit information from unintended disclosure.
2. Risks: The following are some examples of the risks associated with improper safeguarding of information:
 - a. Identity theft.
 - b. Unwanted access to personal information such as medical records, drug test results, etc.
 - c. Stolen credit card or bank account information.
 - d. Legal liability for improper disclosure.

B. Passwords Requirements

1. Passwords to all systems capable of supporting them are to meet the following criteria:
 - a. Minimum password length: 12 characters. No limit to Maximum password length.
 - b. Password complexity is required. Passwords will require at least 1 upper case, 1 numeric character, and 1 special character.
 - c. A password must be used for a minimum of 3 days before the user can change it again.
 - d. Passwords shall be changed every 365 days or when there is evidence or a strong suspicion that it is no longer secure. Accounts with Admin privileges in IT will be changed every 90 days.
 - e. Password policy history is 10 passwords to prevent the old passwords from being reused.
 - f. Password notification for expiring passwords is 14 days.
 - g. Passwords shall not be left in voicemail or emailed.
 - h. Domain accounts shall automatically lockout for ten minutes after five consecutive failed login attempts. After five lockouts, users must reset the password.

C. User Accounts

1. User accounts are not to be shared. Each user account represents a unique relationship with an individual. Permission to access information is granted to the individual not the job function.
2. Users requiring remote network access shall be required to use multi-factor authentication.
3. User accounts are to be granted only when necessary to carry out a job function.
4. All applications are to have defined procedures and documentation for user account creation and termination, including approving authority, roles, and permission levels.
5. All applications must have provisions to log out users after a period of inactivity.
6. All applications that maintain sensitive information must be auditable.
7. IT is required to have Administrator Access or “Admin” permissions to all District Applications for regulatory and cyber insurance compliance as well as maintenance.
8. All applications must support single-sign-on (SSO) and multifactor-authentication (MFA). Legacy applications that do not meet these requirements must be upgraded to support the technology for regulatory and cyber insurance compliance.

D. Permission Levels and Roles

1. All applications shall have permissions to access information based on roles.
2. IT staff shall work with users to define application roles and the access permissions assigned to that role.
3. Roles are to have the minimum access necessary for employees to carry out their job function.
4. User activity shall be logged to allow auditing of access to ensure adherence to best security practices and respond to security breaches.
5. The District reserves the right to modify or disable (or both) any user’s access any time.

E. Safeguarding Sensitive Information

1. While almost all information is to be safeguarded against unintended disclosure, personal and credit card information is particularly sensitive, as is material related to potential or pending litigation and matters to be addressed in Closed Session by the Board of Directors.
2. In order to protect Sensitive Information, the following steps are to be taken:
 - a. Sensitive Information is to be identified and inventoried.
 - b. Sensitive Information is to remain within the application (such as PeopleSoft). Such data is not to be saved on a user's local hard drive, flash drive, unprotected network share, or any other media.
 - c. Copying or transmitting Sensitive Information to non-AC Transit devices or destinations is forbidden except in specific circumstances approved in writing by the Chief Information Officer.
 - d. AC Transit devices capable of holding Sensitive Information must be erased before being removed from District premises for repair or disposal.
 - e. Theft or loss of AC Transit devices must be reported immediately.
 - f. Mobile devices issued by the District and any personal mobile device capable of accessing District data must be locked and passcode protected while not in use.

F. Contractor/ Vendor Responsibilities

1. This section applies to procurements and contracts. AC Transit acknowledges that information is sometimes shared with or placed in the custody of third-party vendors/contractors in the regular course of business. All vendors/contractors engaged in information stewardship must sign the Contractor Confidentiality and Integrity Statement, attached.

G. Network Security

1. Devices not owned and controlled by AC Transit are not allowed to connect to the District's network except via the remote terminal servers provided by the Department of Innovation and Technology or the District's guest Wi-Fi network.
2. Users are not allowed to use personal email accounts to conduct District business. Access to a personal email account from District equipment is not allowed.

H. Training

1. AC Transit shall provide cybersecurity awareness training for all employees.
2. All District Users with a valid AC Transit email address shall be required to complete annual cybersecurity awareness training provided by the District. Initial training shall be completed during the onboarding process and annually thereafter.

V. RESPONSIBILITIES

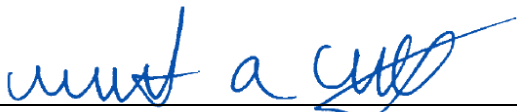
It is the responsibility of all District computer system Users to understand and comply with this regulation.

An employee found to have violated this regulation may be subject to disciplinary action, up to and including termination.

VI. ATTACHMENTS

A. Contractor Confidentiality and Integrity Statement

Approved by:



Michael A. Hursh, General Manager
Alameda-Contra Costa Transit District

Attachment A

Contractor Confidentiality and Integrity Statement

AC Transit's Department of Innovation and Technology is responsible for safeguarding the integrity and confidentiality of data in the District computer files regardless of the source of the data or medium on which they are stored. All data generated from the original source data shall remain property of AC Transit (e.g. reports, metrics and benchmarks). The control of the disclosure of data shall be retained by AC Transit.

I/we, as a representative of _____, understand that I/we act as an extension of AC Transit's Department of Innovation and Technology and therefore I/we are responsible for safeguarding District data included within the scope of services of contract _____.

I/we will not use, disclose, or modify District data without the written authorization of AC Transit. I/we agree to take all necessary precautions to prevent unauthorized use, disclosure, or modification of District data.

I/we will alert AC Transit immediately of any situation in which any data under my/our responsibility has or may have been accessed, disclosed, or modified without authorization.

Penalty for unauthorized use, disclosure or modification may result in the District finding my company in violation of the contract and may mean prosecution under applicable state or federal law.

I, the Undersigned, hereby affirm that I have read and agree to abide by the terms above.

Contractor Signature: _____

Date: _____

Contractor Name: _____