SR 20-202
Att.1.

Alameda-Contra Costa Transit District

Administrative Regulation No. 440B: Information Security

Issuing Officer: General Manager **Date of Adoption:** 3/22/17 **Most Recent Amendment:** N/A **See Also:** 217, 440, 440A, 440C, 440D	**Subject Category:** Section 400, Operations **Subsection:** Information Systems **Control Department(s):** Information Services

I. PURPOSE

The purpose of this regulation is to provide 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

"Malware", short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to or control over computer systems, or display unwanted advertising.

"Phishing" is a fraudulent activity where criminals seek access to secure information by posing as another, legitimate entity.

"Ransomware" is the use of file encryption software to prevent a user from accessing their own files and then demanding money, usually in Bitcoin, to unencrypt the files.

"Sensitive information" includes all data, in its original and duplicate form, which contains personal information, protected health information, customer record information, card holder data, confidential personal data, 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

Each employee, regardless of their job function, has a responsibility to safeguard AC Transit information from unintended disclosure.

Risks

The following are some examples of the risks associated with improper safeguarding of information:

- Identity theft.
- Unwanted access to personal information such as medical records, drug test results, etc.
- Stolen credit card or bank account information.
- Legal liability for improper disclosure.

Threats

Common external threats include:

- Brute Force or Dictionary attacks: A program attempts to crack your password by systematically using common words or character combinations until the correct one is used.
- Phishing: An attacker impersonating another entity to entice you to give up your password. This can occur via a phone call, an e-mail, or visiting a website.
- Ransomware: The use of file encryption software to prevent a user from accessing their own files and then demanding money, usually in Bitcoin, to unencrypt the files.
- Physical theft: Theft of a laptop, phone, CD, DVD, flash drive, or any other device with information on it.

However, most threats are internal and can include:

- Weak permissions: granting too much access to an employee.
- Improper storage of information: it may be convenient to save information to a spreadsheet on an employee's computer to work on but that information is now exposed to any number of threats.
- Weak audit trails: inadequate tracking of file access.
- Poor disposal practices: improper disposal of information or devices containing information such as printouts, hard drives and DVDs.

B. Passwords / Password Phrase Requirements

Passwords to all systems capable of supporting them are to meet the following criteria.

- Password complexity is less important than length.
  - Minimum password length: 20 characters.
  - Must not contain the user's first or last name.
- Passwords shall be changed every two years or when there is evidence or a strong suspicion that it is no longer secure.
- Users are encouraged to create passwords using password phrases. For example: *ilovetoeatatricksdeli*
- Manual password resets performed by Information Services (I.S.) staff will be relayed directly to the individual. Passwords will not be left in voicemail or emailed.
- Domain accounts will automatically lockout for five minutes after every five failed login attempts. After five lockouts they will require I.S. staff assistance to reset.

C. User Accounts

User accounts that manage information 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.

Users in critical positions requiring remote network access will be required to use multi-factor authentication – two or more methods of user authentication.

User accounts are to be granted only when necessary to carry out a job function.

All applications are to have defined procedures and documentation for user account creation including approving authority, roles, and permission levels.

All applications are to have defined procedures and documentation for user account termination.

All applications must have provisions to log out users after a period of inactivity.

All applications that maintain sensitive information must be auditable.

D. Permission Levels and Roles

All applications shall have permissions to access information based on roles.

I.S. staff shall work with users to define application roles and the access permissions assigned to that role.

Roles are to have the minimum access necessary for employees to carry out their job function.

Roles and the permissions assigned to them are to be audited annually.

District reserves the right to modify or disable (or both) employee's access any time the employee violates the terms and conditions outlined herein, or such violation is reported.

E. Safeguarding Sensitive Information

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.

In order to protect information, AC Transit retains control over the location of that information. Once AC Transit identifies where sensitive information is located, copying that information to other, less secure locations undermines any security measures AC Transit undertakes. To avoid this situation the following steps are to be taken:

a. Sensitive information is to be identified and inventoried, including:
   - System\Server\Database the information is stored on, and
   - Location of any backups of sensitive information.
b. Sensitive information is to remain within the application (such as PeopleSoft) until it is properly disclosed. Such data is not to be saved on an employee’s local hard drive, flash drive, unprotected network shares, 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. Do not copy or download sensitive information to your home computer or to a web file sharing service in order to work remotely. Sensitive information must be used only in District systems or on District-owned devices. It may not be sent or accessed via email or other electronic means (e.g., FTP) on non-District devices.
d. AC Transit devices capable of holding sensitive information must have it 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

AC Transit acknowledges that, during the course of business, information is sometimes shared with or placed in the custody of third party vendors. All vendors engaged in information stewardship must sign the Contractor Confidentiality and Integrity Statement which states that control of the disclosure of information shall be retained by AC Transit.

The statement includes:

- The vendor acts as an extension of AC Transit’s I.S. department and is therefore responsible for safeguarding District data included within the scope of services of contract.
- The vendor will not use, disclose, or modify District data without the written authorization of AC Transit.
- The vendor agrees to take all necessary precautions to prevent unauthorized use, disclosure, or modification of District data.
- The vendor will alert AC Transit immediately of any situation in which any data under the vendor’s responsibility has or may have been accessed, disclosed, or modified without authorization.

G. Network Security

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 I.S. department or the District’s guest WiFi network.

They may connect to externally-hosted District resources such as email with proper user authentication, with the understanding that downloading District information may make them subject to legal search and disclosure.

Under no circumstances are unauthorized networking devices including network interface cards, access points, routers, and switches allowed to connect to AC Transit’s network.

H. Training

AC Transit provides self-directed and auditable training for all employees on safeguarding information. Available training topics will include at least:

- Email and Messaging
- Phishing awareness
- Malware
- Ransomware
- Password security
- Data Security
- Mobile Device Security
- Safe Internet Browsing
- Social Networking Risks
- Personally Identifiable Information
- Payment Card Industry Data Security Standard (PCI-DSS) Compliance (for those staff that handle credit card information)

All district users with a valid AC Transit email address will be required to complete annual End User Security Awareness Training provided by the District and then to successfully complete a brief security quiz. Initial training will 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 Information Services department is responsible for safeguarding the integrity and confidentiality of data in 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 Information Services department 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 persecution 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: ___________________________