

AC TRANSIT DISTRICT
Board of Directors
Executive Summary

GM Memo No. 09-145

Meeting Date: June 10, 2009

Committees:

Planning Committee
External Affairs Committee
Rider Complaint Committee
Board of Directors

Finance and Audit Committee
Operations Committee
Paratransit Committee
Financing Corporation

SUBJECT: Possible Adoption of a Comprehensive Data Security Program similar to the one now required by the new Massachusetts Regulations

RECOMMENDED ACTION:

Information Only Briefing Item Recommended Motion

Fiscal Impact:

None at this current time, however could be minimal depending on method and tools used moving forward.

Background/Discussion:

Overview

This GM Memo addresses the possible adoption of a comprehensive data security program similar to the one now required by the new Massachusetts regulations. Similar to California's SB-1386, the Massachusetts law requires businesses to provide prompt notice of security breaches related to personal non public information. Personal information is defined as a person's name together with his/her social security number, driver's license number, financial/credit card numbers, etc. As a follow-up, Massachusetts more recently issued comprehensive regulations related to the law that requires businesses to implement and maintain a comprehensive information security program. Additionally, regulations also detail required controls related to data access, transmission and protection (via encryption).

Applicability

Current California and Massachusetts law applies specifically to "personal information". However, it is fairly logical and prudent that the implementation of such policies and procedures include as much data, private or not, as possible. In fact, all encompassing security can be implemented, monitored and maintained with less effort than better

BOARD ACTION: **Approved as Recommended** [] **Other** []
 Approved with Modification(s) []

The above order was passed on:

Linda A. Nemeroff, District Secretary
By _____

defined, granular security. An example of such would be the encryption of an entire server rather than specified folders. In this light, it is the goal of Information Services to meet the intent of California (and Massachusetts) laws on a wider scale beyond that of personal information.

Information Systems Standards

Attached is a draft of the Information Systems Standards document. This document addresses, in more detail, many of the issues raised by the newer, stricter data security laws. Topics covered include, but are not limited to:

- Identification and classification of data
- Proper authentication of users
- Appropriate access controls
- Methods of assigning passwords
- Secure transmission and transfer of data
- Encryption of portable data

Work continues on the document to further define methods, systems and procedures to secure systems and data as well as to provide auditable processes and documentation for the purpose of enhanced data security.

Prior Relevant Board Actions/Policies:

None

Attachments:

Information Systems Standards

Approved by: Rick Fernandez, General Manager
Blake W. Pelletier, Chief Technology Officer

Prepared by: Glenn Massaro, Director of I.T.

Date Prepared: May 28, 2009



Information Systems Standards

DRAFT

**Confidential Information
Redacted for Security Reasons**

Standards Overview	2
Acknowledgement	2
Terminology.....	2
Network Use and Security	3
Computer Network Orientation	3
Creating a secure password.....	5
Internet Usage	9
Email and Messaging.....	10
Usage.....	10
Email and Data Confidentiality	11
Email Etiquette.....	11
Data Confidentiality.....	13
Overview.....	13
Information Classification and Labeling	13
Information and Media Disposal	14
Storing and Accessing Information	14
Transmitting Nonpublic Information.....	15
Encryption.....	15
Detailed Policy Provisions.....	16
Management and Administration.....	16

Standards Overview

Alameda Contra Costa Transit District (AC Transit) provides access to computing equipment, internal network and systems as well as the vast information resources of the Internet to help you do your job faster and smarter, and be a well-informed business citizen. The facilities to provide that access represent a considerable commitment of District resources for telecommunications, networking, software, storage, etc. This standards document is designed to help you understand our expectations for the use of those resources and to help you use those resources wisely.

In addition to detailed policy provisions in this document you will find several narratives written in simple, non-technical fashion. These are aimed at providing a better understanding of the issues and expectations from a day to day business level with less emphasis on “technical jargon”. Hopefully, these will provide a clear understanding of our network, its capabilities and our expectations for you.

Finally, these standards are in place to protect employees as well as the District itself. Inappropriate use of network computers and systems exposes us to risks including viruses, hacking, compromise of systems and private data and, ultimately, legal issues.

Acknowledgement

All employees granted access to the AC Transit District network, it's applications and systems will be provided with a written copy of these standards and will be required to sign the AC Transit District Information System Standards Acknowledgement form (see last page of this document).

Terminology

Certain terms in this standards document should be understood expansively to include related concepts. AC Transit District may also be referred to as AC Transit as well as “the District”.

Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the so-called HTML files read in an Internet browser, any file meant to be accessed by a word processing or desk-top publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools.

Graphics includes photographs, pictures, animations, movies, or drawings.

Display includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

Network Use and Security

AC Transit District's resources are to be used for District business-related purposes only subject to a limited exception for necessary personal situations, such as family emergencies, communications from a school or child care facility at which one's children are located, communications to reschedule personal appointments due to conflicts with work assignments or other critical non-AC Transit District related communications which must occur at the work place due to an emergency or time sensitive matter. AC Transit District recognizes that it cannot list every type of permitted personal communication that qualifies for an exception and expects all employees and Third Parties to use sound judgment when deciding if a personal communication qualifies for exception. Management reserves the right to inspect any/all data, files, communications passing through and/or stored on AC Transit District systems.

Computer Network Orientation

Network Workstation Logon


You will be required to logon to the network from your computer workstation each day to access your applications and network resources.

- When your computer is booted up you press CTRL-ALT-DEL to initiate the login process.
- Accept the Confidentiality Agreement by clicking OK
- Enter your User Name: First initial and last name i.e. JSMITH for Joe Smith.
- Enter your password: The password will be case sensitive.
- The Domain field for your network account is currently set to one of the following: [REDACTED]. However, work is underway to move all users to the [REDACTED] domain.

Password Policy

To maintain high security standards and meet industry best practices guidelines, the following password policy parameters are required for the Network Workstation Logon password.

- Minimum Password Length: At least [REDACTED] length.
- Password Makeup: Must have [REDACTED]
- Passwords must not be the same or similar to a previous password used.
- Password Expiration: The system will prompt you to change your password every [REDACTED] days.

- 
- Screen Saver Password Lock: After 30 minutes of inactivity on your workstation, your workstation will automatically go to a screen saver and lock your workstation with your password. You will need to enter CTRL-ALT-DEL and enter in your password to unlock your workstation.

Desktop Icons

After you are logged on you will have a minimum set of standard icons on your desktop that will include the following:

- Internet Explorer - Application for Web Browsing on the Internet.
- Citrix Program Neighborhood – Contains applications like that run in the Citrix environment.
- My Computer - Access to other network drives where shared data can be accessed.
- My Documents - Storage place for your personal files and folders which is on your personal network U: drive (see the next section, Data Storage and Shared Access, for additional information).

Depending on your needs, you may also have additional application icons available to you.

Data Storage and Shared Data Access

There are two types of general file and folder data you may want to store and access.

- Personal Data is your own private data and can be stored and accessed within your "My Documents" folder on your desktop. This folder is also known as your U: drive or your Home Share. Everyone's U: drive (My Documents) is unique to them and others cannot access your personal U: drive. This location for data storage is automatically backed up to the server daily and is the safest storage area for your personal data. It is highly recommended that you do not store data locally on the C: drive of your computer.
- Shared Data is data you want to share with others on the network. This can be shared within certain groups or publicly District wide. It is stored on network drives that are accessed through the "My Computer" icon on your desktop. The current list of network drives that you have available to you is based on your department and access rights. Everyone will have at least the S: drive as this is the Public storage area that all District users can access.
- The following is a list of network drives and how they are assigned:
 - ■ - This drive contains information that is shared between users within departments. Information placed here may be seen by other members of your department and is not as private and confidential as your personal drive (see the next bullet, Drive U:).
 - ■ - Your own personal storage space that is not shared with anyone. This is the place to store confidential sensitive data.
 - ■ - This drive contains applications typically used at AC Transit. This drive is secured and used by Information Services staff to load applications and

perform troubleshooting on PCs. Note: some users may have this drive mapped elsewhere such as those that use Lotus 1-2-3

Printing

All District users can have access to the various network printers located throughout the facility to print any business communication or application printing that is necessary.

Initially, users have been setup to access the network printer closest to their workstation.

Each network printer has a label with identifying information on it indicating it's location and/or department. Access to additional or alternate printers can be setup as needed and as approved by the management team. As always, please call the Help Desk at extension 7170 to start this process if necessary.

For those that have access to multiple printers, a default printer can be selected by going to Start / Settings / Printers & Faxes, right-click on the printer you want as the default and select 'Set as Default' option.

Some users may have local printers directly attached to their workstation computers on their desks. These printers can only be accessed from the workstation computer they are attached to. Local printers may not be shared without approval due to the load they place on the network as well as the load they place on printers that are not designed for more than single person use.

Email

Outlook is the application used for the District's email access. Outlook can also be used to keep your calendar, contacts, tasks, and other notes. Outlook can be used to send/receive email both from internal staff members as well as to anyone with an external Internet email address.

Creating a secure password

Securing your access to AC Transit District's system and data is essential and protects you, the District and, most importantly, our customers from information theft or tampering. While the Password Policy section, above, outlines good network password policy, it doesn't address selecting a solid, memorable password. The following information from Microsoft addresses the issue of creating a secure password that's easy to remember with little effort on your part. It is presented for your use and reference:

Your passwords are the keys you use to access personal information that you've stored on your computer and in your online accounts. If criminals or other malicious users steal this information, they can use your name to open new credit card accounts, apply for a mortgage, or pose as you in online transactions. In many cases you would not notice these attacks until

it was too late. Fortunately, it is not hard to create strong passwords and keep them well protected.

What makes a strong password?

To an attacker, a strong password should appear to be a random string of characters. The following criteria can help your passwords do so:

- Make it lengthy. Each character that you add to your password increases the protection that it provides many times over. Your passwords should be 8 or more characters in length; 14 characters or longer is ideal.
- Many systems also support use of the space bar in passwords, so you can create a phrase made of many words (a "pass phrase"). A pass phrase is often easier to remember than a simple password, as well as longer and harder to guess.
- Combine letters, numbers, and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Other important specifics include:
 - The fewer types of characters in your password, the longer it must be. A 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard. If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection. An ideal password combines both length and different types of symbols.
 - Use the entire keyboard, not just the most common characters. Symbols typed by holding down the "Shift" key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard, and any symbols unique to your language.
 - Use words and phrases that are easy for you to remember, but difficult for others to guess.

Create a strong, memorable password in 5 steps

Use these steps to develop a strong password:

- Think of a sentence that you can remember. This will be the basis of your strong password or pass phrase. Use a memorable sentence, such as "My son Aiden is three years old."
- Check if the computer or online system supports the pass phrase directly. If you can use a pass phrase (with spaces between characters) on your computer or online system, do so.
- If the computer or online system does not support pass phrases, convert it to a password. Take the first letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "msaityo".
- Add complexity by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden's name, or substituting the word "three" for the number 3. There are many possible substitutions, and the longer the sentence, the

more complex your password can be. Your pass phrase might become "My SoN Ayd3N is 3 yeeRs old." If the computer or online system will not support a pass phrase, use the same technique on the shorter password. This might yield a password like "MsAy3yo".

- Finally, substitute some special characters. You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i\$ 3 yeeR\$ old" or a password (using the first letter of each word) "M\$8ni3y0".

Password strategies to avoid

Some common methods used to create passwords are easy to guess by criminals. To avoid weak, easy-to-guess passwords:

- Avoid sequences or repeated characters. "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.
- Avoid using only look-alike substitutions of numbers or symbols. Criminals and other malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to replace an 'i' with a '1' or an 'a' with '@' as in "M1cr0\$0ft" or "P@ssw0rd". But these substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case, to improve the strength of your password.
- Avoid your login name. Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. This is one of the first things criminals will try.
- Avoid dictionary words in any language. Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions. This includes all sorts of profanity and any word you would not say in front of your children.
- Use more than one password everywhere. If any one of the computers or online systems using this password is compromised, all of your other information protected by that password should be considered compromised as well. It is critical to use different passwords for different systems.
- Avoid using online storage. If malicious users find these passwords stored online or on a networked computer, they have access to all your information.

Keep your passwords secret

Treat your passwords and pass phrases with as much care as the information that they protect.

- Don't reveal them to others. Keep your passwords hidden from friends or family members (especially children) that could pass them on to other less trustworthy individuals. Passwords that you need to share with others, such as the password to your online Districting account that you might share with your spouse, are the only exceptions.

- Protect any recorded passwords. Be careful where you store the passwords that you record or write down. Do not leave these records of your passwords anywhere that you would not leave the information that they protect.
- Never provide your password over e-mail or based on an e-mail request. Any e-mail that requests your password or requests that you go to a Web site to verify your password is almost certainly a fraud. This includes requests from a trusted District or individual. E-mail can be intercepted in transit, and e-mail that requests information might not be from the sender it claims. Internet "phishing" scams use fraudulent e-mail messages to entice you into revealing your user names and passwords, steal your identity, and more. Learn more about phishing scams and how to deal with online fraud.
- Change your passwords regularly. This can help keep criminals and other malicious users unaware. The strength of your password will help keep it good for a longer time. A password that is shorter than 8 characters should be considered only good for a week or so, while a password that is 14 characters or longer (and follows the other rules outlined above) can be good for several years.
- Do not type passwords on computers that you do not control. Computers such as those in Internet cafés, computer labs, shared systems, kiosk systems, conferences, and airport lounges should be considered unsafe for any personal use other than anonymous Internet browsing. Do not use these computers to check online e-mail, chat rooms, District balances, business mail, or any other account that requires a user name and password. Criminals can purchase keystroke logging devices for very little money and they take only a few moments to install. These devices let malicious users harvest all the information typed on a computer from across the Internet—your passwords and pass phrases are worth as much as the information that they protect.

What to do if your password is stolen

Be sure to monitor all the information you protect with your passwords, such as your monthly financial statements, credit reports, online shopping accounts, and so on. Strong, memorable passwords can help protect you against fraud and identity theft, but there are no guarantees. No matter how strong your password is, if someone breaks into the system that stores it, they will have your password. If you notice any suspicious activity that could indicate that someone has accessed your information, notify authorities as quickly as you can. Get more information on what to do if you think your identity has been stolen or you've been similarly defrauded.

Internet Usage

While we've set forth explicit requirements for Internet usage below, we'd like to start by describing our Internet usage philosophy. First and foremost, the Internet for this District is a business tool, provided to you at significant cost. That means we expect you to use your Internet access primarily for business-related purposes, i.e., to communicate with customers and suppliers, to research relevant topics and obtain useful business information. We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings. To be absolutely clear on this point, all existing District policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of District resources, sexual harassment, information and data security, and confidentiality.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the District and expose the District to significant legal liabilities. The chats, news groups and email of the Internet give each individual Internet user an immense and unprecedented reach to propagate District messages and tell our business story. Because of that power we must take special care to maintain the clarity, consistency and integrity of the District's image and posture. Anything any one employee writes in the course of acting for the District on the Internet can be taken as representing the District's posture. That is why we expect you to forgo a measure of your individual freedom when you participate in chats or news groups on District business, as outlined below.

While our direct connection to the Internet offers a cornucopia of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features like file transfers. The overriding principle is that security is to be everyone's first concern. An Internet user can be held accountable for any breaches of security or confidentiality.

Email and Messaging

Usage

Electronic mail or email is provided to facilitate the business of AC Transit District. AC Transit email systems are intended for District business, not for personal communication or other inappropriate activities. Occasional personal use of email is permitted (see “Network Use and Security” section, above). The email and other information systems are not to be used in a way that may be disruptive, offensive to others, or harmful to morale.

Any transmission or use of email that contains ethnic slurs, racial epithets, or any message that may be construed as harassment or offensive to others based on their race, national origin, sex, sexual orientation, age, disability, religious, or political beliefs is prohibited and could result in appropriate disciplinary action, up to and including termination.

The email system also should not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other personal matters unrelated to your job.

For privacy reasons, employees should not attempt to gain access to another employee’s files or email. However, AC Transit reserves the right to enter an employee's email files. AC Transit may regularly monitor email messages, and employees are reminded there is no privacy in the use of AC Transit information systems, including email systems. AC Transit reserves the right to access and monitor these systems without notice.

All authorized users are assigned the use of one unique email account or address. Individual accountability must be in effect at all times. If there is a business requirement to share a mailbox, Microsoft Exchange has the ability to grant permission to view another user’s inbox. Only AC Transit personnel are allowed to be members of internal mail distribution lists. Non-AC Transit users are not allowed to be members of such lists. Microsoft Outlook is the only approved email client (with the exception of the Telephone Information Center using Microsoft Outlook Express).

The use of non-AC Transit District communication systems (e.g., Internet-based email systems including but not limited to AOL, Yahoo, MSN, etc.) by employees is strongly discouraged. Use of Internet-based email systems as well as downloading attachments from these systems to AC Transit systems could expose AC Transit to increased risk and harmful situations such as virus or worm outbreaks, to the installation of a Trojan horse program. Additionally, information stored on Internet-based email systems is not secure and is sometimes scanned for content and keywords to determine which advertisements to display on your browser.

Blanket or automatic forwarding of messages to parties or mailboxes outside AC Transit District is prohibited. This includes automatic forwarding from one account to another and/or AC Transit District email to personal, and non-AC Transit District email addresses.

Use of Instant Messaging applications is limited to the system and client approved by the District for business use only. There are limited exceptions as described earlier for personal

use. (see “Network Use and Security” section, above). Other Instant Messaging systems and clients including, but not limited to ICQ, HotMail are not allowed under any circumstances.

Email and Data Confidentiality

Email is not private! It’s the electronic equivalent of sending a postcard through the mail. The email, once it leaves AC Transit District bounces around the Internet and makes many stops at (the equivalent of) electronic post offices where it can be read, tampered with or destroyed. Email may be fine for scheduling an appointment or asking someone to give you a call but it is NOT suitable for transmitting PRIVATE, CONFIDENTIAL data. You wouldn’t want your social security number or checking account number sent to you via a postcard, would you?

In order to protect AC Transit District customer information and to maintain regulatory compliance, unencrypted transmission of confidential customer information is not to be transmitted via email. Unauthorized transmission of such information including but not exclusive to: account numbers, social security numbers, credit information, and customer identification information is not allowed under any circumstances. Please refer to the “Data Confidentiality” section, below, for more information.

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, users of electronic communications should exercise caution when forwarding messages. AC Transit District’s confidential information must not be forwarded to any outside party without the approval of a manager.

Email Etiquette

Email is everywhere. We use it to chat with our relatives and friends, we submit questions to vendors, we reply to customers (WITHOUT violating rules of data confidentiality) and, at the top of the list, we use email as a means of communicating with our business associates to facilitate higher levels of productivity. Professionalism in communicating with peers and clients via email is just as important as it is with person to person, written and telephone communication. With that in mind, here are some tips for using email effectively and politely:

- Be concise and to the point and clearly summarize the contents of your email in the subject line.
- Avoid using all caps – it’s the electronic equivalent of shouting.
- Be sure to answer ALL questions to eliminate the frustration and wasted time of multiple emails when all it should have taken was one!
- Check your grammar and punctuation. Use your spell-checker!
- Respond promptly.
- Include previous emails when replying so the recipient can refer back and/or get a better sense for the conversation thus far.
- Don’t send large files with your emails (such as photos) unless they are needed.

- Read your email before sending it. Give it a quick run through to be sure you've corrected all grammatical and punctuation errors. Also, this is another chance to rephrase or clarify something.
- Watch your tone. Remember, you don't have the benefit of face to face communication with email. Your facial or vocal cues that would suggest humor or sarcasm are not available via email and may cause your message to be taken incorrectly. Be polite; terseness can be misinterpreted. Don't forget to use "please" and "thank you".
- Avoid using URGENT or IMPORTANT in your subject line. Reserve these words for use only when the message is truly important or urgent. Overuse will dull the recipient to their presence in your emails. Similarly, don't overuse the bold and italics options unless emphasis is really required.
- Watch your content. Don't forward chain letters. Do not send personal emails using your AC Transit District email, including jokes or photos or other inappropriate or possibly offensive material.
- Don't post your email address on Internet sites or other public parts of the Internet. The result will be a deluge of spam!
- Never email while angry. If you do, don't hit the send key until waiting a bit and then rereading your email and making appropriate corrections. Once the email is sent there's no going back.
- Never send PRIVATE, CONFIDENTIAL data via email.

Data Confidentiality

Overview

AC Transit District must appropriately safeguard all nonpublic customer information, as well as, other confidential information. AC Transit is obligated to protect the security and confidentiality of customers' nonpublic personal information.

Customer Information is defined as any record containing nonpublic personal information (NPI) about a consumer who obtains a product or service to be used primarily for personal, family, or household purposes.

This includes paper, electronic or other form, which is handled or maintained by or on behalf of AC Transit or its affiliates. Examples include but are not limited to: social security numbers, account and policy numbers, credit card account numbers, date and/or location of birth, account balances, payment histories, credit ratings, income histories, driver's license information, and tax return information.

AC Transit policies, standards, procedures and guidelines have been established to address administrative, technical, and physical safeguards to:

- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records.
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Each department must assume responsibility for ensuring that adequate safeguards are in place within its area of responsibility.

Information Classification and Labeling

Not all information requires the same level of protection. The level of protection applied to information must be commensurate with its classification to ensure appropriate handling and disclosure. All information must be identified (i.e. labeled) and classified according to its level of confidentiality and business need-to-know. The classifications are:

- Public
- Confidential and Proprietary
- Restricted

All information is considered “Confidential and Proprietary” by default. Information which has not been classified is to be treated as “Confidential and Proprietary”. All AC Transit-related information, whether in digital or hardcopy form, must be labeled with its information classification.

Any document or report created by an employee or Third Parties that contain nonpublic information must be marked with the appropriate classification. The classification must be clearly marked using highlighting, bolding, or asterisks to increase visibility. For example:

AC TRANSIT DISTRICT – CONFIDENTIAL AND PROPRIETARY

Information System Standards Rev 1.0

AC Transit District Confidential & Proprietary, not for distribution

6/4/2009

Page 13

Any document or report created by employees or Third Parties that contain confidential information must have the appropriate control statements added. Control statements describe special handling of documents. The control statements should be added to each page (header or footer) along with the classification category (e.g. Confidential). The statements must be clearly marked using highlighting, bolding, or asterisks to increase their visibility. Examples of control statements are:

AC TRANSIT DISTRICT CONFIDENTIAL - MODIFICATION OR REPRODUCTION IS PROHIBITED

AC TRANSIT DISTRICT RESTRICTED - NOT FOR DISTRIBUTION

All electronic media (DVDs, CDs, tapes, diskettes, etc.) should be externally labeled to identify contents and avoid mishandling. Media containing confidential information must have an external label with the information classification and should be stored in a physically secure fireproof (approved for media) location when not in use.

Information and Media Disposal

When nonpublic documents are to be destroyed, destruction must occur either by shredding the document or placing it in a locked shred bin.

Electronic media such as floppies, backup tapes, removable drives, and hard drives must be securely wiped (overwritten with “1”s and “0”s) before being disposed of to ensure that the information is not readable. Every sector of the media must be wiped to prevent the data from ever being recovered. Formatting alone is insufficient for securely and permanently erasing the data. See your manager to request assistance with accomplishing this task.

Additionally, all media and storage devices that are unable to be securely erased must be disposed of in a specially labeled media shred bin.

Storing and Accessing Information

Each employee is provided with a personal directory that is located on a server in a secure server room or data center. Nonpublic information must be stored in that personal directory or other designated directory located on an AC Transit server. Nonpublic information must not be stored on your desktop.

Information may not be removed from AC Transit District to be used or edited at another location unless specifically authorized by management. The use of floppies, CDs, DVDs and/or USB memory devices all fall under this policy. Management must identify and mitigate risks of data loss or theft during transport and use on foreign systems before granting authorization.

The use of laptops is currently monitored and approved on a case by case basis at AC Transit District. Prior to the granting the use of any laptop, AC Transit District will determine the nature of data to be stored on the laptop and mandate the use of encryption software to secure any and all customer non-public information and/or data sensitive or material to the business of the District. Use of encryption software as well as “rules of engagement” for data and

laptop storage, transport and use must be determined and disseminated before the use of laptops on or with data taken from the AC Transit District network.

When not in use, all nonpublic information and computer storage media must be put away before leaving the immediate work area unless the work area is secured and designated only for processing nonpublic information. A secure location is a locked cabinet, an individual locked office, or safe.

Where possible, nonpublic conversations should be conducted in person in a private location. Exercise caution when discussing confidential information in public places, open areas, lobbies, on wireless devices, such as cellular phones, or when leaving voicemail. Confidential conversations can be overheard, and voicemail is recorded and can be forwarded.

Transmitting Nonpublic Information

Nonpublic information must not be sent in email over the Internet unless it is encrypted, if available, or put into an attached document that is password protected and encrypted. The recipient of the email should then be provided the password over the phone. The purpose of this control is to provide additional protection in case the email is intercepted or inadvertently sent to someone other than the intended recipient.

All attempts should be made to eliminate or reduce the amount of nonpublic information in any email. For example, list only a partial account number versus the entire account number so that the email is no longer classified as Confidential.

When sending a fax containing confidential information, do not assume that the receiving fax machine is physically secure. It is the responsibility of the sender to ensure that the appropriate person is physically present to receive the fax at the time it is sent. When receiving a fax containing confidential information, it is the responsibility of the receiver to ensure that either the receiving fax machine is physically secure or that the receiver is physically present at the time the fax is sent.

All attempts should be made to eliminate or reduce the amount of confidential information on any faxed document. For example, list only a partial account number versus the entire account number so that the fax is no longer classified as Confidential.

Encryption

Data may need to be encrypted when in transmission, memory, or storage. The need for encryption is dependent on the classification of data. Information systems including email do not encrypt information by default. If confidential information must be sent by electronic communication systems, encryption or similar technologies to protect the data must be employed. Unless encryption is used, users should not send information over the Internet if they consider it to be confidential. Likewise, whenever AC Transit District Confidential data, and/or data that has been entrusted to AC Transit by a business partner, is to be sent over an un-trusted network, it too must be transmitted in an encrypted form.

Detailed Policy Provisions

Management and Administration

AC Transit District has software and systems in place that can monitor and record Internet usage (including email and other messaging traffic). We reserve the right to monitor usage at any time. No employee should have any expectation of privacy as to his or her Internet usage. Our managers may review Internet activity and analyze usage patterns to assure that District Internet resources are devoted to maintaining the highest levels of productivity.

We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

The display of any kind of sexually explicit image or document on any District system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.

We may block access from within our networks to any inappropriate sites that we know of. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

AC Transit District's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any District resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.

All data created and stored on any AC Transit District PC or network-attached device remains the property of AC Transit District.

No employee may use District facilities knowingly to download or distribute pirated software or data.

No employee may use the AC Transit District's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

No employee may use the AC Transit District's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Each employee using the Internet facilities of AC Transit District shall identify himself or herself honestly, accurately and completely (including one's District affiliation and function where appropriately requested) when participating in chats or news groups, or when setting up accounts on outside computer systems.

Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the District may speak/write in the name of the District to any news group or chat room. Other employees may participate in news groups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this District, the employee must refrain from any unauthorized political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the District of any commercial product or service not sold or serviced by this District, its subsidiaries or its affiliates. Only those managers and District officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the District may grant such authority to news group or chat room participants.

AC Transit District retains the copyright to any material posted to any forum, news group, chat or World Wide Web page by any employee in the course of his or her duties.

Employees are reminded that chats and news groups are public forums where it is inappropriate to reveal confidential District information, customer data, trade secrets, and any other material covered by existing District secrecy policies and procedures. Employees releasing protected information via a news group or chat – whether or not the release is inadvertent – will be subject to all penalties under in existing data security policies and procedures.

Use of AC Transit District Internet access facilities to commit infractions such as misuse of District assets or resources, sexual harassment, unauthorized public speaking and misappropriation or theft of intellectual property are also prohibited by general District policy, and will be sanctioned under the relevant provisions of the personnel handbook.

Since a wide variety of materials may be deemed offensive by colleagues, customers or suppliers, it is a violation of District policy to store, view, print or redistribute any document or graphic file that is not directly related to the user's job or the District's business activities.

Employees may use their Internet facilities for non-business research or browsing during meal time or other breaks, or outside of work hours, provided that all other usage policies are adhered to. Please note that use of streaming media (live or stored video, music, Internet Radio) is never allowed at anytime unless absolutely required for AC Transit business purposes. The use of such streaming media greatly impacts Internet performance for all users of the network and results in greater costs for the District. Please be a good neighbor to all of your coworkers by not impacting their work day via frivolous use of the Internet.

AC Transit District will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries and archives on individuals' Internet activities.

Employees with Internet access may download only software with direct business use, and must arrange to have such software properly licensed, registered and installed. Users may never install software on AC Transit District PC's or systems.

Any software or files downloaded via the Internet into the AC Transit District network become the property of the District. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

Employees with Internet access may not use District Internet facilities to download entertainment software or games, or to play games locally or against opponents over the Internet.

Employees with Internet access may not use District Internet facilities to download images or videos unless there is an explicit business-related use for the material.

Employees with Internet access may not upload any software licensed to the District or data owned or licensed by the District without explicit authorization from the manager responsible for the software or data.

User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. District policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites.

Forwarding (manually or automatically via software) of AC Transit District email to another non-AC Transit District email address is prohibited.

Instant messaging regardless of service and/or software client is limited.

Employees should schedule communications-intensive operations such as large file transfers, video downloads, mass emailing and the like for off-peak times (defined however that is appropriate for the particular District). Any file that is downloaded must be scanned for viruses before it is run or accessed.

Video and audio streaming and downloading technologies represent significant data traffic which can cause local network congestion. Video and audio downloading is prohibited unless specifically authorized by management as a part of AC Transit District business and/or education. When approved, such activities should be scheduled for off-peak times.

AC Transit District has installed a variety of firewalls, proxies, Internet address screening programs and other security systems to assure the safety and security of the District's networks. Any employee who attempts to disable, defeat or circumvent any District security facility will be subject to immediate dismissal.

Files containing sensitive District data as defined by existing corporate data standards that are transferred in any way across the Internet must be encrypted.

Computers that use their own modems to create independent data connections sidestep our network security mechanisms. An individual computer's private connection to any outside computer can be used by an attacker to compromise any District network to which that computer is attached. That is why any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from District's

internal networks. (Major on-line services such as CompuServe and America Online, and content providers such as Lexis-Nexis, can be accessed via firewall-protected Internet connections, making insecure direct dial-up connections generally unnecessary.) Only those Internet services and functions with documented business purposes for this District will be enabled at the Internet firewall.

AC Transit District Information System Standards Acknowledgement

I acknowledge that I have received a written copy of the Information System Standards for the AC Transit District. I have been given the opportunity to have any questions answered by management and/or their representatives.

I understand the terms of these standards and agree to abide by them. I realize that the District's security systems may monitor, record and store for management use my access to any/all network systems. Management may review electronic e-mail messages I send and receive, the Internet address of any site that I visit, and any network activity in which I transmit or receive any kind of file.

I understand that any violation of these standards may be subject to disciplinary action, up to and including termination of employment as well as possible criminal prosecution.

Name (Printed): _____

Signature: _____ Date: _____

Manager (Printed) _____

Signature: _____ Date: _____